

Unified Infrastructure Management - 20.3

Table of Contents

| | |
|--|-----------|
| Release Notes | 11 |
| UIM 20.3.3 | 11 |
| OC 20.3.2 Patch | 28 |
| UIM 20.3.1 | 32 |
| What's New | 36 |
| Release Comparison | 46 |
| Probes and Packages | 49 |
| Resolved Issues | 52 |
| Known Issues | 53 |
| International Support | 64 |
| Third-Party Software Agreements | 64 |
| CA Business Intelligence JasperReports Server with CA UIM Release Notes | 66 |
| Product Accessibility Features | 74 |
| Getting Started | 75 |
| Role-based Documentation | 75 |
| Evaluator..... | 78 |
| New User..... | 80 |
| Product Administrator..... | 81 |
| Monitoring Administrator..... | 82 |
| Operations Manager..... | 83 |
| IT Administrator..... | 83 |
| Developer..... | 84 |
| CA UIM Overview | 85 |
| CA UIM Architecture..... | 85 |
| CA UIM Components..... | 87 |
| CA UIM Key Features..... | 89 |
| Service and System Monitoring..... | 89 |
| CA UIM Reference Architecture | 90 |
| CA UIM Interfaces | 90 |
| Admin Console..... | 90 |
| Operator Console..... | 91 |
| Infrastructure Manager..... | 92 |
| RESTful Web Services..... | 92 |
| Videos | 93 |
| CA UIM Security | 93 |
| Additional Resources | 94 |

| | |
|--|------------|
| Accessing support.nimsoft.com..... | 95 |
| Installing..... | 96 |
| Pre-Installation Planning..... | 96 |
| Prepare Your Server Hardware..... | 97 |
| Configure Your Operating Systems..... | 100 |
| Install and Configure Your Database Software..... | 104 |
| Microsoft SQL Server..... | 105 |
| MySQL Server..... | 122 |
| Oracle..... | 124 |
| Pre-Installation Considerations..... | 142 |
| Configure Installation on IPv6 Environment..... | 142 |
| Password Policies..... | 148 |
| Firewall Port Reference..... | 149 |
| UIM Sizing Recommendations..... | 158 |
| Product Compatibility..... | 166 |
| Supported Install/Upgrade Paths..... | 166 |
| UIM Compatibility Matrix..... | 168 |
| CA UIM Probes Support Matrix..... | 174 |
| Install UIM Server..... | 174 |
| Installation Parameters..... | 179 |
| Installing in an Active/Passive Microsoft Cluster..... | 183 |
| Uninstalling UIM Server..... | 188 |
| Install Infrastructure Manager..... | 188 |
| Install Secondary Hubs..... | 189 |
| Deploy Secondary Hubs on Windows..... | 189 |
| Deploy Secondary Hubs and Robots on Linux..... | 190 |
| Configure the robot.cfg File..... | 194 |
| Install Operator Console (OC)..... | 195 |
| Configure Multiple OC Servers..... | 201 |
| Uninstall OC..... | 204 |
| Discover Systems to Monitor..... | 205 |
| Introduction..... | 205 |
| Discovery Components..... | 206 |
| Discovery Considerations..... | 207 |
| Prerequisites and Supported Platforms..... | 208 |
| Configuring Discovery..... | 209 |
| Discovery Probe Deployment..... | 210 |
| Configure Discovery Queues..... | 210 |
| Launch the Discovery Wizard..... | 213 |
| Create Authentication Profiles..... | 213 |

| | |
|---|------------|
| Define Scopes..... | 219 |
| Schedule Discovery..... | 222 |
| Run File-based Import..... | 222 |
| View Discovered Systems..... | 231 |
| Advanced Configuration..... | 232 |
| Run discovery_server on a Child Robot of the Primary Hub..... | 232 |
| Set Maximum Java Heap Size..... | 234 |
| Remove Master Devices through Discovery Server..... | 235 |
| Set the Probe Transaction Timeout Value..... | 236 |
| Remove Devices in OC..... | 237 |
| Deploy Robots..... | 239 |
| Install a Windows Robot..... | 240 |
| Install a Unix Robot..... | 241 |
| Install an IBM i Robot..... | 241 |
| Bulk Robot Deployment with an XML File..... | 243 |
| Deploy Robots in OC..... | 254 |
| Deploy Robots in Bulk with a Third-Party Tool and Native Installers..... | 256 |
| Install Multiple Robots on a Single Host..... | 260 |
| Optional Post-Installation Tasks..... | 262 |
| Configure Admin Console to Use a Proxy Server..... | 262 |
| Configure Email Address Login to OC..... | 262 |
| Configure HTTPS in Admin Console or OC (Self-Signed Certificate)..... | 263 |
| Configure HTTPS in Admin Console or OC (Authority-Signed Certificate)..... | 273 |
| Configure OC to Use SAML Single Sign-On..... | 281 |
| Enable Login with LDAP..... | 289 |
| Encrypt UIM Network Traffic with SSL..... | 294 |
| Set Up Access to Operator Console (OC) Using a DMZ..... | 295 |
| Restrict Computer-Level (IP) Access to the CA UIM Database..... | 299 |
| Deploy Your Monitoring Probes..... | 299 |
| Bulk Probe Deployment with an XML File..... | 309 |
| CA Business Intelligence with CA UIM..... | 310 |
| Installing and Upgrading CA Business Intelligence JasperReports Server with CA UIM..... | 315 |
| Install or Upgrade for a Bundled CA Business Intelligence JasperReports Server..... | 316 |
| Install or Upgrade for an External CA Business Intelligence JasperReports Server..... | 335 |
| Migrate from Bundled to External Configuration..... | 348 |
| Migrate Reports from Unified Reporter..... | 350 |
| Changing the JNDI Password for CABI Server..... | 352 |
| Reinstalling UIM Server..... | 354 |
| Additional Topics..... | 354 |
| Packages Signed with GPG-Enabled Keys..... | 354 |

| | |
|---|------------|
| Addressing CVE-2018-13820 and CVE-2018-13819 Vulnerabilities..... | 360 |
| Upgrading to Microsoft Visual C++ Redistributable for Visual Studio 2017..... | 361 |
| Addressing Jackson Vulnerabilities..... | 363 |
| Enhanced security.cfg..... | 364 |
| Adopting OpenJDK..... | 368 |
| Upgrading..... | 369 |
| Upgrade Step 1: Evaluate the Existing Environment..... | 369 |
| Upgrade Step 2: Prepare for the Upgrade..... | 371 |
| Upgrade Step 3: Deploy the Upgrade..... | 373 |
| Upgrade UIM Server..... | 373 |
| Secure Hub and Robot..... | 379 |
| (Optional) Upgrade the Infrastructure Manager..... | 442 |
| Upgrade the Hubs..... | 443 |
| Upgrade the Robots..... | 444 |
| Configure robot.cfg..... | 445 |
| Upgrade Operator Console..... | 446 |
| Upgrade a Multiple OC Configuration..... | 451 |
| Upgrade CA Business Intelligence with UIM..... | 454 |
| Upgrade Monitoring Configuration Service Templates..... | 454 |
| Upgrade Step 4: Perform Post-Upgrade Verification and Configuration..... | 455 |
| Roll Back to a Previous Version of UIM Server..... | 455 |
| Administering..... | 456 |
| Working with Admin Console..... | 456 |
| Admin Console Archive Concepts..... | 458 |
| Deploy Admin Console to a Secondary Hub..... | 459 |
| Log in to Admin Console..... | 460 |
| Manage Hub and Probe Licenses..... | 460 |
| Restart or Remove a Robot..... | 462 |
| Download, Update, or Import Packages..... | 462 |
| Deploy Packages..... | 463 |
| Configure a Probe..... | 464 |
| Activate, Deactivate, or Restart a Probe..... | 465 |
| View a Probe Log File..... | 466 |
| Manage Probe Security Settings..... | 466 |
| Use the Probe Utility..... | 467 |
| Manage Bus Users..... | 468 |
| Admin Console ACL Permissions Reference..... | 469 |
| Working with Infrastructure Manager..... | 470 |
| General Probe Management in Infrastructure Manager..... | 470 |

| | |
|---|------------|
| Manage Robots in Infrastructure Manager..... | 476 |
| Locate or Move a Robot..... | 477 |
| Connect a Passive Robot to a Hub..... | 478 |
| Add or Modify Users in Infrastructure Manager..... | 478 |
| Manage Licenses for Components in Infrastructure Manager..... | 479 |
| Using Account Admin..... | 480 |
| Change a User Password in the Account Admin..... | 480 |
| Add or Modify Users with Account Admin..... | 481 |
| Types of Users..... | 486 |
| ACL Permissions List..... | 486 |
| Permissions Reference for OC Features..... | 492 |
| Start, Stop, or Uninstall a Robot (Command Line)..... | 493 |
| Hub Information..... | 496 |
| Move the UIM Database (MS SQL Server)..... | 497 |
| Run Probe Commands from a Command Prompt..... | 497 |
| Set Up Automated Usage Metering and Billing..... | 499 |
| Robot Commands for the IBM System i Computer..... | 500 |
| Enable Sub-Tenancy..... | 500 |
| Configure Telemetry for the PLA Model..... | 511 |
| Operator Console (OC) Host Header Validation..... | 515 |
| Auditing in UIM Interfaces..... | 516 |
| White Labeling in Operator Console..... | 517 |
| Change Your Password..... | 519 |
| Back Up the Licensing Information..... | 521 |
| Configuring and Viewing Monitoring Data..... | 522 |
| OC Prerequisites..... | 531 |
| Run Discovery in OC..... | 532 |
| Use Application Discovery..... | 538 |
| Manage Groups..... | 546 |
| View Interface Data..... | 562 |
| Manage Alarms..... | 564 |
| View Your Dashboards..... | 578 |
| MCS Dashboards..... | 581 |
| Create a New Custom Dashboard View..... | 585 |
| View Your Reports..... | 587 |
| View Your Inventory..... | 592 |
| Using Setup Wizard..... | 599 |
| Working with the Metrics Palette..... | 601 |
| Manage Alarms with Centralized Alarm Policies..... | 612 |
| Alarm Message Variables..... | 636 |

| | |
|--|------------|
| Alarm Policy Troubleshooting..... | 637 |
| Admin Console in OC..... | 639 |
| Deprecated Portlets..... | 640 |
| Operator Console Endpoints..... | 642 |
| Monitor Technologies Using RESTMon..... | 644 |
| The Settings View..... | 644 |
| The Dashboard Designer..... | 644 |
| Migrate Dashboards from the Legacy Dashboard Designer portlet..... | 654 |
| Add a Dashboard Widget..... | 655 |
| Create and Assign the Data Source for a Widget..... | 671 |
| Set the Properties for a Widget..... | 679 |
| Change a Dashboard Widget on the Canvas..... | 685 |
| Change the Appearance of a Dashboard Widget..... | 688 |
| Restrict Dashboard Navigation..... | 690 |
| Monitoring Configuration Service..... | 692 |
| Manage Monitoring Using MCS Profile Types..... | 706 |
| Enable Read-Only Access to MCS Profiles..... | 723 |
| How to Copy and Apply Profiles in MCS..... | 725 |
| The SLM View..... | 729 |
| SLM Interface Reference..... | 735 |
| Create a New Service Level Agreement..... | 740 |
| Create an SLA Using the Wizard..... | 753 |
| Create a QoS Monitoring Profile..... | 755 |
| Send SQL Queries to the UIM Database..... | 756 |
| SLM Data Management..... | 757 |
| View and Export Quality of Service (QoS) Data..... | 762 |
| The SLA Reports..... | 764 |
| Working with Report Scheduler..... | 768 |
| The SNMP Device Self-Certification..... | 776 |
| Dashboards..... | 776 |
| AD Server Unified Dashboard..... | 778 |
| Apache Unified Dashboard..... | 780 |
| AWS Auto Scaling Unified Dashboard..... | 781 |
| AWS Billing Unified Dashboard..... | 784 |
| AWS DynamoDB Unified Dashboard..... | 784 |
| AWS EC2 Unified Dashboard..... | 788 |
| AWS ElastiCache Unified Dashboard..... | 789 |
| AWS ELB Unified Dashboard..... | 791 |
| AWS RDS Unified Dashboard..... | 793 |
| AWS Route 53 Unified Dashboard..... | 795 |

| | |
|---|-----|
| AWS S3 Unified Dashboard..... | 796 |
| AWS SNS Unified Dashboard..... | 797 |
| AWS SQS Unified Dashboard..... | 797 |
| AWS Unified Dashboard..... | 799 |
| Cassandra Unified Dashboard..... | 805 |
| Cisco CBQoS Unified Dashboard..... | 808 |
| Cisco UCM Unified Dashboard..... | 811 |
| Cisco Unified Dashboard..... | 813 |
| CloudStack Unified Dashboard..... | 815 |
| Datacenter Unified Dashboard..... | 819 |
| DB2 Unified Dashboard..... | 821 |
| Docker Unified Dashboard..... | 823 |
| EMC Celerra Unified Dashboard..... | 825 |
| EMC Clariion Unified Dashboard..... | 827 |
| EMC VMAX Unified Dashboard..... | 829 |
| EMC VPLEX Unified Dashboard..... | 832 |
| Hadoop Unified Dashboard..... | 834 |
| Hitachi Unified Dashboard..... | 837 |
| HP 3Par Unified Dashboard..... | 839 |
| Hyper-V Unified Dashboard..... | 842 |
| IBM_SVC Unified Dashboard..... | 843 |
| IBM DS4K Unified Dashboard..... | 846 |
| IBM DS Next Unified Dashboard..... | 850 |
| IBMVM Unified Dashboard..... | 853 |
| IIS Unified Dashboard..... | 856 |
| Cisco IP SLA Unified Dashboard..... | 857 |
| JBoss Unified Dashboard..... | 863 |
| Lync_Monitor Unified Dashboard..... | 864 |
| Microsoft Azure Unified Dashboard..... | 867 |
| MongoDB Unified Dashboard..... | 869 |
| MS Exchange 2007 Unified Dashboard..... | 871 |
| MS Exchange 2010 Unified Dashboard..... | 875 |
| MS Exchange 2013 Unified Dashboard..... | 880 |
| MS SharePoint Server Unified Dashboard..... | 884 |
| MS SQL Server Unified Dashboard..... | 889 |
| NETAPP ONTAP Unified Dashboard..... | 891 |
| Network Unified Dashboard..... | 896 |
| Nutanix Clusters Unified Dashboard..... | 898 |
| Nutanix Containers Unified Dashboard..... | 899 |
| Nutanix Disks Unified Dashboard..... | 900 |

| | |
|--|-------------|
| Nutanix Hosts Unified Dashboard..... | 901 |
| Nutanix Storage Pools Unified Dashboard..... | 902 |
| Nutanix VMs Unified Dashboard..... | 904 |
| OpenStack Unified Dashboard..... | 905 |
| Oracle RAC Unified Dashboard..... | 910 |
| Oracle Unified Dashboard..... | 913 |
| Power Unified Dashboard..... | 914 |
| Processes Unified Dashboard..... | 916 |
| PureStorage All-Flash Array Unified Dashboard..... | 916 |
| Router-Switch Unified Dashboard..... | 920 |
| SAP_Basis DB2 Database Unified Dashboard..... | 925 |
| SAP_Basis HANA Database Unified Dashboard..... | 926 |
| SAP_Basis NetWeaver Unified Dashboard..... | 929 |
| SAP_Basis Oracle Database Unified Dashboard..... | 931 |
| SAP_Basis Unified Dashboard..... | 933 |
| Server Unified Dashboard..... | 937 |
| Storage Unified Dashboard..... | 938 |
| Vblock Unified Dashboard..... | 942 |
| VCloud Unified Dashboard..... | 949 |
| VNX Unified Dashboard..... | 952 |
| Weblogic Unified Dashboard..... | 953 |
| Websphere MQ Unified Dashboard..... | 954 |
| Websphere Unified Dashboard..... | 958 |
| XenServer Unified Dashboard..... | 958 |
| Integrating Other Products..... | 961 |
| Integrate CA Application Delivery Analysis..... | 962 |
| Integrate CA Automic..... | 963 |
| Integrate CA Network Flow Analysis..... | 973 |
| Integrate CA Service Desk..... | 973 |
| Integrate CA Service Operations Insight..... | 973 |
| Integrate CA SiteMinder..... | 974 |
| Integrate DX NetOps Spectrum..... | 978 |
| Log Analytics..... | 979 |
| Working with Development Tools..... | 988 |
| The NimAlarm Utility..... | 989 |
| Create Custom Scripts for Application Discovery..... | 992 |
| Troubleshooting..... | 1005 |
| Troubleshooting Admin Console..... | 1005 |
| Troubleshooting Alarm Console..... | 1006 |

| | |
|---|-------------|
| Troubleshooting Dashboards..... | 1006 |
| Troubleshooting Infrastructure Manager..... | 1008 |
| Troubleshooting Operator Console..... | 1013 |
| Troubleshooting SiteMinder Configuration..... | 1021 |
| Troubleshooting Discovery and the Discovery Wizard..... | 1021 |
| Troubleshooting the Service Desk Adapter..... | 1022 |
| Troubleshooting Alarm Views..... | 1023 |
| Troubleshooting UIM Server Installation or Upgrade..... | 1023 |
| Troubleshooting Additional Scenarios..... | 1028 |
| Troubleshooting Monitoring Configuration Service (MCS)..... | 1038 |
| Documentation Legal Notice..... | 1039 |

Release Notes

The CA Unified Infrastructure Management (CA UIM) Release Notes provide the latest information about new features, enhancements to existing features, resolved issues, international support, known issues, and third-party software agreements for CA UIM.

The CA UIM Release Notes only include probes that are installed or upgraded when you run either the CA UIM Server or OC installers. Some examples include:

- data_engine
- baseline_engine
- nas
- wasp

The Release Notes for individual monitoring probes are available on the [Probes Documentation Space](#).

NOTE

More information:

UIM 20.3.3

As part of the regular release cycle for updating Unified Infrastructure Management (UIM), we are pleased to announce the UIM 20.3.3 release. This release includes new and enhanced features, resolved issues, and so on.

The following features and enhancements are included in 20.3.3:

Metrics Palette Enhancements

The following enhancements have been made to the Metrics palette. These enhancements further improve the usability of the palette:

- Define and save the metrics view.
This eases the process of accessing the views. Otherwise, you would be required to select the metrics every time you want to access the specific metrics view for a device/group.
- Rename, copy, or delete the metrics view.
This helps you make the necessary updates to the views based on the changes in your scenarios.
- Export the metrics view.
This helps you save or share the views in the supported formats.
- Publish the metrics view at the private, account, or public level.
This ensures that only authorized users can access the required views.
- Set a specific metrics view as a default view.
This ensures that the same view is displayed in the UI whenever you navigate to the Metrics palette for that entity.
- Configure the custom time period.
This allows you to view the historical metrics data based on your defined custom duration.

For more information, see the [Working with the Metrics Palette](#) article.

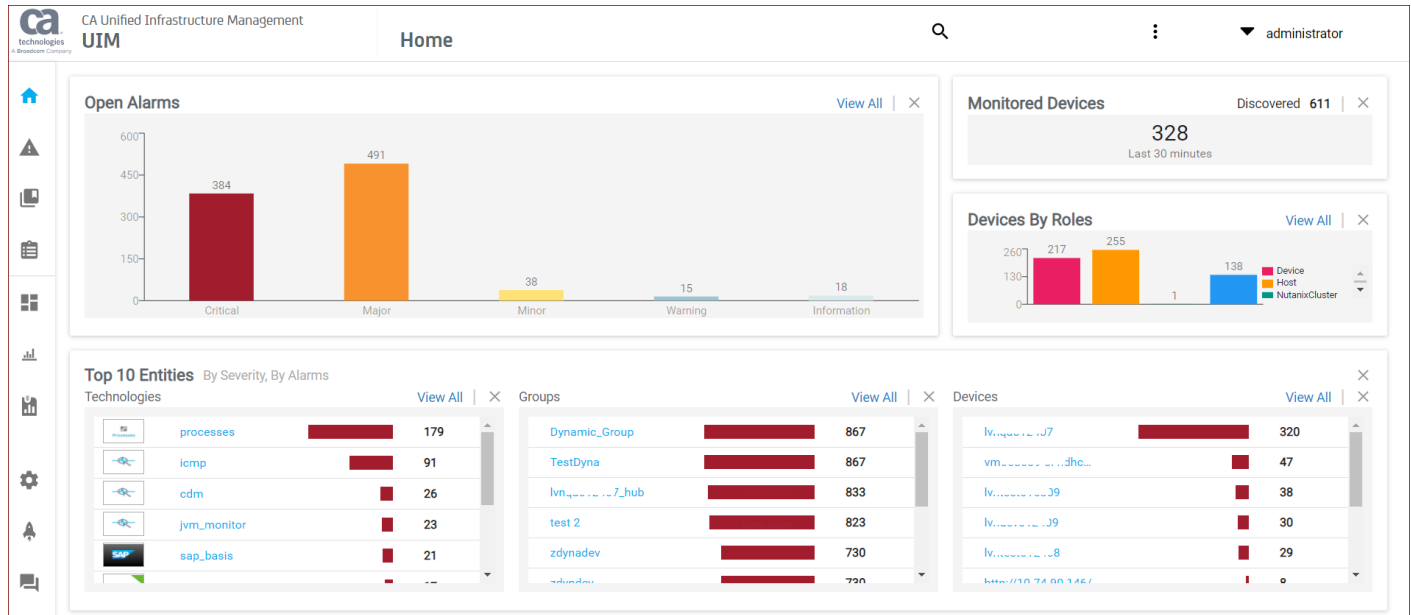
Removing CABI Dependency (Native Operator Console)

This release of UIM removes dependency on CA Business Intelligence (CABI) for rendering the following OC web pages. These pages are now rendered by using HTML5:

- **Home page**

The Home page lets you:

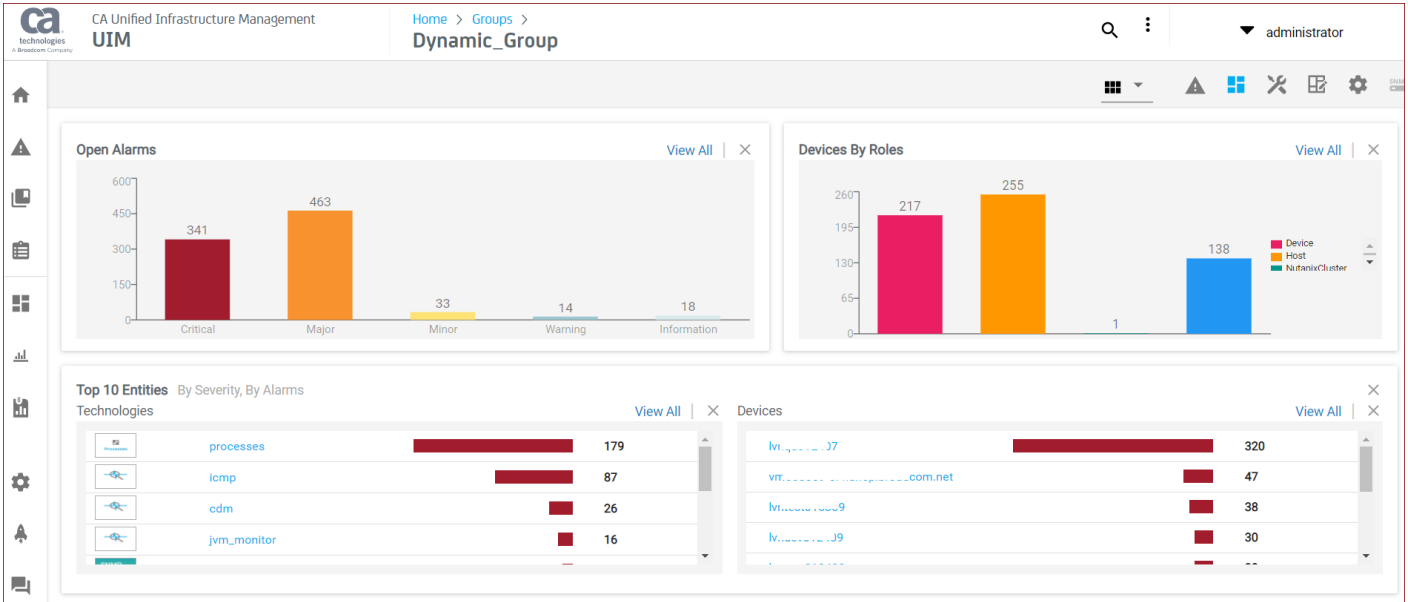
- View the open alarms, monitored devices, segregation of devices by role, and top ten entities for monitoring technologies, groups, and devices in your environment.
- Customize the Home page view (using the three-dot menu) to show or hide specific tiles.
- Click the respective View All link or the specific entity to navigate to the detailed view.
- Remove a tile from the view by clicking X on the respective tile.



- **Group view page**

The Group view page lets you:

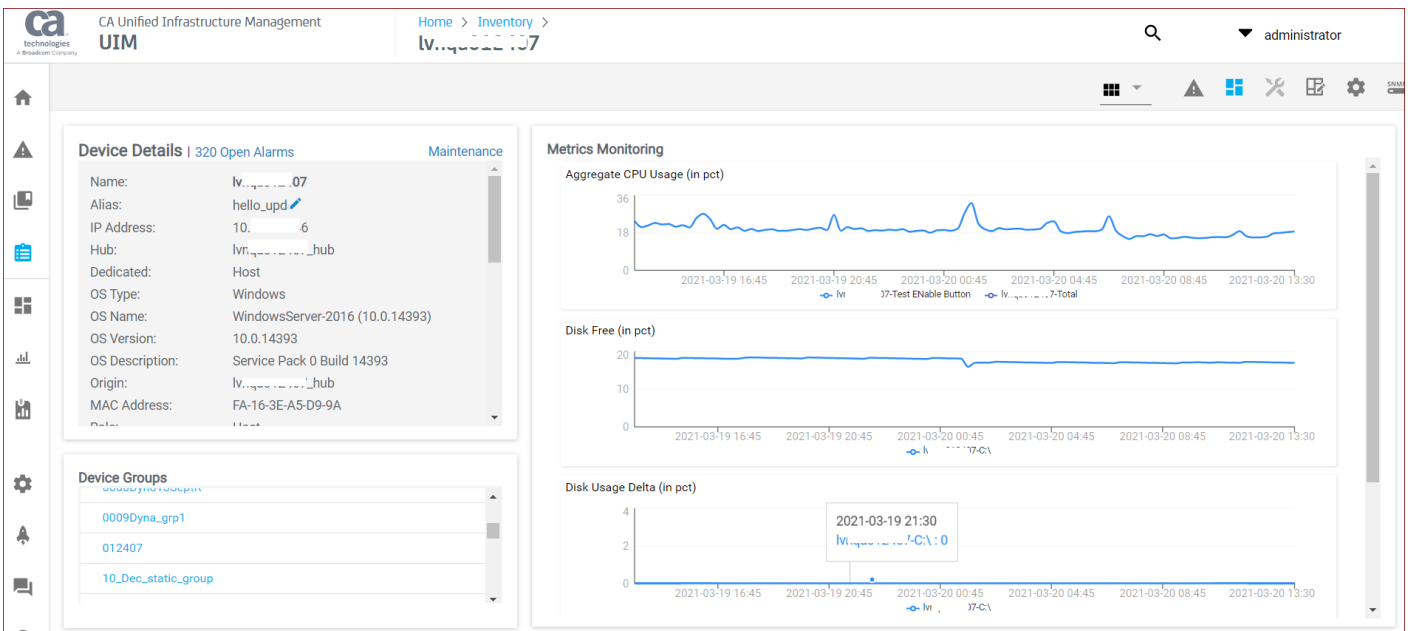
- View the open alarms, segregation of devices by roles, and top entities for sub-groups/monitoring technologies, and devices related to your group.
- Use the properly created URL to directly access the specific group dashboard view: `http://<OC_Server>/operatorconsole_portlet/groups/0/<Group_ID>/dashboard`
- Customize the view (using the three-dot menu) to show or hide specific tiles.
- Click the respective View All link or the specific entity to navigate to the detailed view.
- Remove a tile from the view by clicking X on the respective tile.



• **Device view page**

The Device view page lets you:

- View the details about the device, groups related to the device, count of open alarms, and metrics monitoring charts (metric views) related to the selected device.
- Put the device in the maintenance schedule by using the in-context Maintenance link on the Device Details tile.
- Edit the device alias by using the edit icon (pencil) next to the alias name on the Device Details tile.
- Use the properly created URL to directly access the specific device dashboard view: `http://<OC_Server>/operatorconsole_portlet/computer_systems/<CI_ID>/dashboard`
- Click the specific group entity link to navigate to the detailed view.
- Click the open alarms count to access the associated list of alarms.

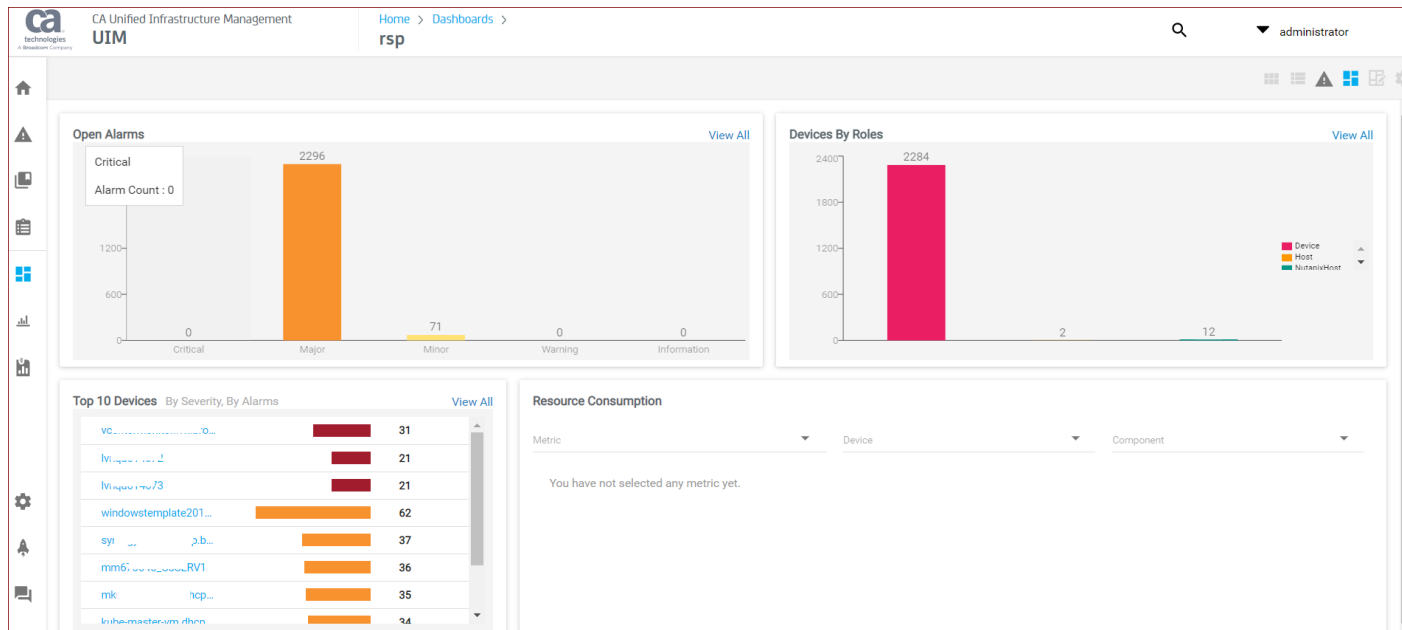


• **Monitored Technologies (probes) view page**

The Monitoring Technologies view lets you:

- Access the dashboard views rendered by using HTML5 for the monitoring technologies like cdm, processes, rsp, and so on.
- View the information like open alarms, devices by roles, and top devices.
- Click the respective View All link or the specific entity to navigate to the detailed view.

The following example screenshot shows the dashboard view (for cdm) that is rendered by using HTML5 in UIM 20.3.3.



Custom and Out-of-the-Box dashboards and reports are still rendered using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered using HTML5. This gives improved performance and actionable views for users to navigate and triage.

For more information, see the [Configuring and Viewing Monitoring Data](#) article.

NOTE

If you change the Zoom level in your browser, then you must reload the OC so that all the widgets in these native OC screens can be loaded properly. This behavior is applicable only for the above-mentioned OC screens.

Availability of Report Scheduler

This release of UIM provides the Report Scheduler functionality that helps you schedule Metric views (Performance metrics) or Service Level Agreement (SLA) reports to run at specified times. With the availability of this functionality, you can now share the reports for viewing and comparing the performance metrics for the various monitored devices, SLAs in terms of the alarms, metrics, and QoS with your stakeholders for the compliance purpose on the predefined schedules. The reports can be delivered as a PDF through email or FTP, or can be stored on a server. Furthermore, you can create, edit, delete, copy, and run jobs for the reports.

For more information, see the [Working with Report Scheduler](#) article.

Packages Signed with GPG-Enabled Keys

This release of UIM provides the .rpm and .deb packages that are signed with the GNU Privacy Guard (GPG)-enabled keys. With this enhanced security mechanism, the integrity and authenticity of the packages are maintained. This helps you verify that the packages that you are using for installation are the same that you have downloaded from the Support

site. You can, therefore, be assured that no modifications have occurred in the packages after they were signed, thereby providing the quality and security assurance of the delivered packages.

The following packages have been signed with the GPG-enabled keys:

- nimsoft-robot.i386.rpm
- nimsoft-robot.x86_64.rpm
- nimsoft-robot+debian_amd64.deb
- nimsoft-robot+ubuntu_amd64.deb

For more information, see the [Packages Signed with GPG-Enabled Keys](#) article.

Secure Transmission of Certificates

With newer security issues coming up every single day, organizations understand the importance of products having robust security mechanism. This release of UIM has further enhanced its security by enabling the seamless transfer of the certificates *from a hub to a robot* over a secure channel.

Now, you no longer need to manually drag-and-drop the certificates from a hub to a robot when using the secure bus. The complete process is automatically done without any intervention, which ensures that the communication is secure and the data is not tampered with.

For more information, see the [Secure Transmission of Certificates](#) article.

Ability to Change the Password

As an account contact user, you can now change your own password. If the "Change Password" ACL is enabled for an account, then the associated account contact users can change their own password. This reduces the chances of your password getting compromised.

The option (Change Password) to change the password is available in the top-right area of the OC UI (under the logged-in user name). After you click the Change Password option, you can enter and save your new password.

For more information, see the [Change Your Password](#) article.

Alarm Console Enhancements

The following enhancements have been made to the Alarm console:

- Provides the arrival date information for an alarm. The Arrival Date column is now available in the Alarm console. With this, you can sort the information based on the arrival date of the alarm, allowing you to always view the latest updates.
- Displays the date format based on the browser locale.
- Updates the Alarms UI to show the configured annotations in the Alarm Details section in OC.
- Provides the ability to access a specific alarm by using the alarm ID as a filter. For example, `http://<OC_server>/operatorconsole_portlet/uim-alarms?alarmId=MA123456-76568`
- Provides the ability to access the alarms for a specific host by using the host name as a filter. For example, `http://<OC_server>/operatorconsole_portlet/uim-alarms?hostname=am102345`
- Provides the Hide Invisible and Include Invisible options for alarms in the Alarm console. The Hide Invisible option hides the alarms that are marked as invisible from the list. The Include Invisible option shows all the alarms: alarms marked as invisible and also the alarms *not* marked as invisible.
- Added the ability to display alarms in the Alarm console based on the alarm filter conditions in the Dashboard Designer view. You can create the alarm filter in the Dashboard Designer view. When you access that alarm filter in the created dashboard, you are then redirected to the Alarm console. The Alarm console displays the appropriate alarms based on the defined filter conditions; it does not display other alarms.

For more information, see the [Manage Alarms](#) article.

Asynchronous Distribution of Probes

UIM 20.3.3 now introduces the asynchronous behavior for probe distribution mechanism, which ensures more robust and resilient deployments. This ability also helps you avoid intermittent time-out or communication issues with the deployment of the larger probes. Previously, while deploying the larger packages, distsrv and ADE were facing time-out issues, which was causing unsuccessful deployment of such packages.

This functionality supports backward compatibility. For example, if you have an older robot, then the deployment happens based on the earlier (synchronous) behavior.

Creating New Custom Dashboard Views

You can now create new custom dashboard views using CA Business Intelligence (CABI) and add them to the OC Dashboards page. This ability helps you address situations where you want to create customized views of your dashboards depending on your needs. Therefore, in UIM 20.3.3, you can create these views in two ways: by using CABI or by using the already existing Dashboard Designer functionality.

For more information, see the [Create a New Custom Dashboard View](#) article.

Data Maintenance Stored Procedures Enhancement

For Microsoft SQL Server 2016 (or higher), the existing data maintenance stored procedures have been enhanced to enable the truncation of partitions directly from the table. This enhancement eases the data maintenance process. For example, it eliminates the need of creating temporary tables, creating indexes, switching the partition data to the temporary tables, and then truncating the data.

For Microsoft SQL Server 2012 or 2014, the existing stored procedures would continue to work as they were working earlier. That is, the new behavior is not applicable for these versions.

For more information, see the [data_engine](#) probe documentation.

discovery_server Enhancement

The `discovery_server` probe has been enhanced in this release. A new parameter (`using_datomic`) has been introduced. This flag is intended to make the `discovery_server` probe function without having `udm_manager`. In this release of 20.3.3, the default value of this flag is true and users can set it to false if they want to stop using `udm_manager` or Datomic. You can set this parameter by using the raw configuration or by updating the `discovery_server.cfg` file (under `setup/udm/`). The `discovery_server` probe then does not try to perform any Datomic transactions, and all the data is stored in the relational database.

This flag mainly impacts the way how device interfaces are processed within `discovery_server`. When using `udm_manager` or Datomic, the device interfaces information is stored in Datomic first and then ported to the relational database. When `udm_manager` is disabled and `discovery_server` is configured with `using_datomic = false`, then the device interfaces information is stored only in the relational database. No data is propagated to Datomic. So, if there are any other probes that read information from Datomic, you must run `discovery_server` with `using_datomic = true`, which means enabling `udm_manager`.

NOTE

If you are integrating with DX NetOps Spectrum or Network Flow Analysis (NFA), then we recommend that you allow `discovery_server` to continue using the `udm_manager` probe.

For more information, see the [discovery_server](#) probe documentation.

Group Management Enhancements

The following enhancements have been made to the groups:

- Added the ability to move groups along with devices from one container group to another. This helps you logically organize your groups.
- Added the new group ACL permissions (OC Group Add, OC Group Edit, OC Group Delete) to provide the create, edit, and delete group permissions to the appropriate users. This ensures that only required users are allowed to perform the relevant operations.

For more information, see the [Manage Groups](#) article.

Group View and Alarm View Optimization

The response time in the Alarm view and the Group view in the OC UI has been further optimized for better user experience and ease of working. For example, with the implementation of the lazy loading in the Group tree view, you no longer experience any lag while accessing the information.

Improved Implementation of the Alarm Policy and MCS ACL Permissions

With this release, the implementation of the ACL permissions for the alarm policy and MCS has been improved. Now, when you disable the Policy Management ACL permission for the alarm policy, the associated users no longer see the option to add, update, or delete an alarm policy. Similarly, when the OC Monitoring Configuration Service and OC Edit Monitoring Templates ACL permissions are disabled for MCS, the Monitoring Config gear icon is not enabled for the related users.

Monitoring Configuration Service (MCS) Enhancements

The following new parameters are now available in the MCS configuration:

- `txn_timeout`: This parameter lets you configure the transaction time-out. This configuration, therefore, helps you roll back the transaction if any exception occurs during the transaction process. The transaction time-out is configured so that if any exception occurs, the transaction is rolled back. It is available in the setup section of the MCS configuration. The default value is 1020. For example, `txn_timeout = 1020`.
- `audit_enabled`: This parameter lets you enable or disable the auditing in MCS. For example, if you want to stop the auditing only in MCS, you can disable this parameter. It is available in the timed section of the MCS configuration. By default, the value is set to true. For example, `audit_enabled = true`.
- `number_of_processing_devices`: This parameter lets you specify the number of devices (which are in the modified or new state) to be processed for the monitoring purpose. It is available in the timed section of the MCS configuration. The default value is 1000. For example, `number_of_processing_devices = 1000`.

For more information, see the [mon_config_service](#) probe documentation.

Persist Maintenance Schedules in the nas Probe

The nas probe now lets you persist the maintenance schedules even when the `maintenance_mode` probe is not reachable from nas. Also, while trying to reconnect, the previous schedules are not deleted and the alarms can be filtered even if the `maintenance_mode` probe is unavailable.

A new parameter `maint_sched_discard` is available that lets you decide whether you want to discard the maintenance schedule. You can specify the value as `yes` or `no`. The value `no` implies that the maintenance schedule is retained.

For more information, see the [nas](#) probe documentation.

Deprecating the ace Probe

The ace (Automatic Configuration Engine) probe has been deprecated in UIM 20.3.3. When you upgrade from a previous version of UIM to UIM 20.3.3, the already existing ace probe is removed from the probes and the installed packages lists after the upgrade. The probe package, however, remains in the local archive.

Platform Support

- UIM now supports Microsoft SQL Server 2019.
- Robot 9.33/9.33S supports Ubuntu 20.01 LTS (Intel 64-bit).

Resolved Issues

The following are the resolved issues in UIM 20.3.3:

- **Operator Console**
 - Fixed an issue where duplicate devices were displaying when users were editing a static group in OC 20.3.2. While editing static groups, users could see the duplicate devices in the device selection area of the edit group dialog.

Out of the two entries, one entry was selected and the other was unselected. If users were selecting an unselected device, they were receiving an exception in that case.

- Fixed an issue where exporting SLA to PDF was truncating the QoS constraint list of SLOs in UIM 20.3.1. In SLA Reports, when users were exporting the SLA to the PDF format, the SLA and SLO information was exporting to the PDF. However, the list of QoS constraints configured in the SLO was not exporting completely.
- Fixed an issue where the change password option for the account users added manually to the Account Admin was not available in UIM 20.3.0. Users were not able to change the password using OC.
- Fixed in an issue where the percentage (%) was not getting displayed in the Dashboard Designer when users were clicking the show units. (Support Case: 32416005)
- Fixed an issue where the customized dashboard layout was not working after upgrading to 20.3.2. (Support Case: 32442952)
- Fixed an issue where the PDF export was not working in Dashboard Designer. (Support Case: 32420957)
- Fixed an issue where the images were not loading in the dashboard in 20.3.2. When users were creating a dashboard, uploading an image to it, and publishing the dashboard, they were not able to view the images. An empty box was displaying in place of the image. (Support Case: 32438021)
- Fixed an issue where the published custom dashboards were not opening. When users were accessing the custom dashboard through OC, the custom dashboard was not redirecting to the HTTPS link. Therefore, the dashboards were not opening. (Support Case: 32455058)
- Fixed an issue where users were getting 401 and 500 data access errors in 20.3.2 while using OC. If an LDAP user was mapped to multiple accounts and logged into OC 20.3.2, the user was unable to access the web pages and was receiving the data access errors. (Support Case: 32439786)
- Fixed an issue where resetting of the maintenance schedule for the create/edit process was happening when multiple users were accessing the maintenance schedules. (Support Case: 32452624)
- Fixed an issue where the information in the Member Group table was not rendering properly in the Group Details view in OC. (Support Cases: 32452448 and 32450811)
- Fixed an issue where while generating the SLA report from the SLM view, the PDF was generating only the first page of the report. It was not generating the remaining pages. (Support Case: 32513503)
- Fixed an issue where the new dialog was flashing (appearing/disappearing) while creating a new maintenance schedule or editing an existing schedule. (Support Case: 32452613)
- Fixed an issue where while performing an update to the member hosts in a maintenance item, the update host choice was resetting to the original value. (Support Case: 32387923)
- Fixed an issue where the Admin Console link from the Settings page in OC was not working. (Support Case: 32443932)
- Fixed an issue where LDAP users were not able to view the dashboards published to No account. They could view only those dashboards that were published to Public. (Support Case: 32440968)
- Fixed an issue where users were unable to download, edit, or copy the SLA report. When users were navigating to SLA in OC to download the report, the OC UI was not responding. (Support Case: 32456125)
- Fixed an issue where the last modified date for the alarms was not available in the Alarm view. (Support Case: 32466952)
- Fixed an issue where the single source selection in Metric Viewer was not working in those scenarios where the multi-source was available. This issue was being observed with all the probes QoS that had the multi-source available. For example, when they were selecting "disk usage - Percentage", they were seeing all the file systems.

- When they were trying to select the "disk usage" metric, select the three dots next to that metric, and then select the specific file system, they were still getting a graph with all the file systems. (Support Case: 32543888)
- Fixed an issue where the metrics view graph was showing a continuous line even when the system status was down. (Support Case: 32540906)
 - Fixed an issue where users were unable to change the parent group of static or dynamic groups. (Support Case: 32534974)
 - Fixed an issue where users were receiving the invalid dashboard report PDF through the email. When users were configuring a schedule on the dashboard to send the report through email, they were receiving the email with an invalid PDF. (Support Case: 32535203)
 - Fixed an issue where the scheduled dashboard and generate dashboard were showing the logon screen. (Support Case: 32502458)
 - Fixed an issue where users were not able to set the compliance value in decimals while creating a monthly SLA report in OC. (Support Cases: 32432656 and 32442628)
 - Fixed an issue where some of the URL actions in the Alarms page stopped working after upgrading to 20.3.1. Users were getting the error as `<Error><Message>The requested resource does not`

support http method 'GET'.</Message></Error> . And, those URLs were doing the GET operation instead of the POST operation. (Support Case: 32415022)

- Fixed an issue where users were getting errors when they were trying to export SLA reports to PDF. (Support Case: 32432717)
- Fixed an issue where users were unable to accept or assign alarms. When users were trying to assign alarms to some other users with email addresses, OC was displaying the Request failed with a status code 406 message. (Support Case: 32388293)
- Fixed an issue where the delete option for some of the SLOs was not working. This issue was occurring in those scenarios where SLOs were having exclusion period with the notes. If users were trying to delete such SLOs, they were not able to do that. (Support Case: 32411716)
- Fixed an issue where while creating the dashboard using the Dashboard Designer, the circle widget was not showing up properly in the canvas. (Support Case: 32452612)
- Fixed an issue where the selected device under a group was not getting highlighted. When users were navigating to the Groups view and selecting a device under a specific group, the UI was not highlighting the selected device. (Support Case: 32511189)
- Fixed an issue where sorting of the accounts list was not working when users were trying to create groups and maintenance schedules in OC. (Support Case: 32529776)
- Fixed an issue where the maximum aggregation was not working in the list widget in Dashboard Designer. (Support Case: 32460053)
- Fixed an issue where users were unable to view the general alarm policies with the Policy Basic ACL. Users with the "MCS Read-Only Access" ACL and the "Policy Basic" ACL could view the MCS profiles and a specific alarm policy, but they could not view the list of all the alarm policies. (Support Case: 32412802)
- Fixed an issue where users were unable to update a parent of a static or a dynamic group. This issue was occurring after users upgraded to 20.3.2. (Support Case: 32511259)
- Fixed an issue where when users were creating the Application Discovery Script MCS profile, the profile was not appearing in the list of the profiles for the group. When users were trying to create the profile again, they were receiving the error that the profile was already available. (Support Case: 32450249)
- Fixed an issue where users were facing issues with the sort order in SLM while configuring QoS constraints. When users were adding the new QoS in an SLO, the source list was not sorting alphabetically. (Support Case: 32502206)
- Fixed an issue where one account user could see the other origin names of a robot. (Support Case: 32504369)
- Fixed an issue where users were facing issues while editing a weekly maintenance schedule that had multiple days selected in the Starting field. After creating a weekly schedule with multiple starting days, when users were trying to edit this schedule, the starting days were not getting selected. (Support Case: 32461052)
- Fixed an issue where no targets were appearing when users were looking for targets using the QOS_e2e_Execution on a VM in the SLM. (Support Case: 32385684)
- Fixed an issue where users were unable to create SLA for the server CDM data. (Support Case: 32485423)
- Fixed an issue where the alarm policy deleted by the admin user was still visible in the OC UI. (Support Case: 32498397)
- Fixed an issue where the Operator Console /main.js and accountadmin/ were displaying the dummy values. In UIM 20.3.3, these dummy values have been removed. (Support Case: 32521709)
- Fixed an issue where the Enable Callback Proxy for MCS in the configuration service options was not working. (Support Case: 32398528)
- Fixed an issue where the alarms generated from an MCS profile were displaying the host name and the alarms generated from an alarm policy were displaying the IP address in the Alarm view (Device Name column). (Support Case: 32382212)
- Fixed an issue where the status was not getting updated in the Group tree view (left pane) when alarms were raised or acknowledged. The status was getting updated only after refreshing the browser. (Support Case: 32528576)
- Fixed an issue where users were not able to drill down the Citrix XenDesktop dashlets in the OC UI. (Support Case: 32374724)
- Fixed an issue where users were able to dissociate a device from the Inventory view and also select the maintenance button even when they did not have the Edit Maintenance ACL permission. Now, after fixing this issue,

- they cannot dissociate a device from the Inventory view and the maintenance button is also disabled for such users. (Support Case: 32438209)
- Fixed an issue where the policy_management queue was not getting processed and the queue color was yellow. (Support Case: 32463333)
 - Fixed an issue where the sorting of the Group members in the Name column was not happening properly. When users were trying to sort the data in the Name column, the sorting was not happening alphabetically. The sorting was case-sensitive and the uppercase names were getting listed before the lowercase names. (Support Case: 32529786)
 - Fixed an issue where some of the hubs in the Admin Console were not displaying properly. Also, users were not able to retrieve the robot information for such hubs. (Support Case: 32445829)
 - Fixed an issue where no option in OC was working when users were trying to access the SLM functionality. (Support Case: 32463430)
 - Fixed an issue where the time for the maintenance schedule was getting changed to the 24-hour format with AM (for example, 17:00 AM). Also, the starting data was resetting to the default value (for example, dd-mm-yyyy). This was happening when users were saving the maintenance schedule. (Support Case: 32407130)
 - Fixed an issue where the Interface groups were not displaying the utilization data after upgrading to 20.3. (Support Case: 32445423)
 - Fixed an issue where users were getting the Data Access Error in the OC reports after they upgraded to 20.3.2. (Support Case: 32455050)
 - Fixed an issue where the OC installer was selecting the main hub as the server for installation. This issues was occurring when users were trying to upgrade to 20.3.0. (Support Case: 32501074)
 - Fixed an issue where users were receiving the "no metrics found" error when they were trying to create an alarm policy on an existing group. The metrics was available, but users were getting the no metrics error message. (Support Case: 32517066)
 - Fixed an issue where alarm policies were not working. They were in the ERROR_RECOVERY or PENDING_RECOVERY state. (Support Case: 32488591)
 - Fixed an issue where users were facing the problems while creating an alarm policy using the long RegEx string that had more than 256 characters. (Support Case: 32492535)
 - Fixed an issue where users were getting the "Error Adding Scopes | Invalid Discovery Agent" error when they were trying to add the scope in the Discovery wizard. (Support Cases: 32513593, 32533191, 32426281, and 32506530)
 - Fixed an issue where users were not able to set the alarms coming from the spectrumgtw probe to the invisible state in the Alarm console. When they were trying to do so, the visibility state of such alarms was not changing. The Alarm console was still showing the state as true and the alarm was not getting removed from the list of the displayed alarms. (Support Case: 32497750)

- **CABI**

- Fixed an issue where users were unable to download or export the reports. For example, when they created customized CPU reports in the CABI dashboard, they could not perform the export or download. (Support Case: 32478274)
- Fixed an issue where users were unable to deploy the cabi 4.30 probe in UIM 20.3.0 environment. The CABI log was showing the *usersync errors*. (Support Case: 32518022)
- Fixed an issue where users were facing Data Access Error in the OC reports after upgrading to 20.3.2. (Support Case: 32455050)
- Fixed an issue where CABI 4.30 was not working after disabling TLS v1.0 and TLS v1.1 on the Microsoft SQL Server. (Support Case: 32485217)
- Fixed an issue where scheduled reports were timing-out or failing to complete. Users started observing this behavior after they upgraded to CABI 4.30. (Support Case: 32469192)
- Fixed an issue where users were observing performance issues with CABI when they were generating the reports. (Support Case: 32505644)
- Fixed an issue where Operator Console in the HTTPS mode was not loading. (Support Case: 32365132)
- Fixed an issue where users were facing CABI issues and they were unable to connect to JasperServer. (Support Case: 32446652)
- Fixed an issue where users were unable to install CABI in a newly upgraded 20.3 environment. When they were trying to install the bundled CABI on a standalone robot reporting to the primary hub, they were receiving the error. (Support Case: 32446543)
- Fixed an issue where the Device/Group Trend/At A Glance reports in the /public/ca/uim/reports/library/health location were not aware of the origin. (Support Case: 32439177)
- Fixed an issue where users were getting the Data Access Error in the dashboard home page after upgrading to 20.3.0. (Support Case: 32511235)
- Fixed an issue where users were unable to see the data in the CABI report (UIM Single QOS Topic). (Support Case: 32453770)
- Fixed an issue where values in reports were not showing in percentage. For example, when users configured the adhoc reports for Disk Utilization in percentage (%), the value in reports was not showing up in percentage. (Support Case: 32468506)
- Fixed an issue where the CABI bundled installation was completing successfully, but the cabi probe was failing to start. (Support Case: 32437153)
- Fixed an issue where users were unable to fetch the data for more than three months in CABI. (Support Case: 32450088)
- Fixed an issue where only limited time range options were available in the CABI reports. For example, there was no option to run a report for the previous month or to select a custom time range when running a report. (Support Case: 32510132)
- Fixed an issue where users were unable to view the CABI page in the OC UI. (Support Case: 32473595)
- Fixed an issue where the CABI Home Dashboard was not displaying the dashboards correctly. (Support Case: 32456241)
- Fixed an issue where the Schedule menu within OC, *Reports* was not displaying the Edit option correctly. (Support Case: 32447941)
- Fixed an issue where the dashboards were not loading when the users were accessing them directly from the CABI server. The users were getting the waiting (hourglass) symbol. (Support Case: 32485752)
- Fixed an issue where users were not able to open the reports page from the OC UI. The users were receiving the 500 error. (Support Case: 32497978)
- Fixed an issue where the Availability reports were not showing any groups or devices in CABI. (Support Case: 32512294)
- Fixed an issue where the users were receiving the JKS key error when they were trying to import the reports. This issue was occurring in the case of the bundled CABI. (Support Case: 32455022)
- Fixed an issue where users were facing issues while installing the cabi 4.30 version in their UIM environment. (Support Case: 32424521)
- Fixed an issue where users were receiving Data Access Error when they were trying to access the Reports page in OC. (Support Case: 32458239)
- Fixed an issue where CABI was not working with TLS v1.2 when UIM was using Microsoft SQL Server as the database. (Support Case: 32442685)
- Fixed an issue where users were getting Data Access Error when they were opening the OC Home page. (Support Case: 32470294)
- Fixed an issue where users were not able to download the robot_update_9.32.zip package. They needed this

- **data_engine**
 - (9.20 HF5) Fixed an issue where data_engine was not processing all the qos_processor-enriched metrics after the restart.
 - (9.20 HF5) Fixed an issue where after updating the origin through qos_processor, data_engine was unable to store the related metrics.
 - Fixed an issue where users were unable to upgrade to 20.3.0. The upgrade was getting stuck at 40%. (Support Case: 32473364)
- **discovery_server**
 - Fixed an issue where the availability data was not reflecting in the UI. The data was present, but it was not showing up in the UI. (Support Case: 32450276)
 - Fixed an issue where the group_info queue was re-establishing itself (returning) after a reboot, which was causing the probe_discovery queue to back up. (Support Case: 32492426)
- **ems**
 - Fixed an issue where the ems probe was always in the process of getting restarted. (Support Case: 32464287)
- **hub**
 - (9.32 HF2 and 9.32 SHF2) Fixed an issue where users were able to see the cleartext passwords in the hub.log file when they were logging in using the Admin Console. (Support Case: 32475607)
 - Fixed an issue where the primary hub was restarting after every few minutes. The logs from controller and hub were not showing any relevant information about the issue. (Support Case: 32498752)
 - Fixed an issue where users were getting errors when they were trying to create tunnels on a hub. (Support Case: 32488645)
 - Fixed an issue where the enhanced security.cfg configurations were not propagating to one of the hubs in the environment. (Support Case: 32509796)
 - Fixed an issue where the AD/LDAP login through IM was failing. The hub was able to connect to the AD/LDAP server and fetch the group/user list, but the login was still failing. (Support Case: 32424406)
- **maintenance_mode**
 - Fixed an issue where the maintenance schedules were not starting at the correct time. These schedules were starting after 1-2 hours of the correct start time. (Support Case: 32493641)
 - (20.30 HF1) Fixed an issue where the maintenance schedule for the Nth day of a month was not working. The schedule was not starting on the scheduled date and time and was remaining inactive. This was happening when the user time zone or the target schedule time zone and the server time zone were different.
 - (20.10 HF1) Fixed an issue where the alarms were getting generated during the maintenance schedule.
 - (9.20 HF5) Fixed an issue where the maintenance schedules were not working. (Support Case: 32160419)
- **mon_config_service**
 - (20.31 HF1) Fixed an issue where updates on the UIM profiles were not always triggering the probe restart. (Support Case: 32283937)
 - (20.31 HF1) Fixed an issue where monitoring profiles were not always getting assigned to the server. (Support Case: 32327952)

NOTE

The 20.31 HF1 hotfix introduces a new key (number_of_processing_devices) in the mon_config_service.cfg file (under the timed section). The default value is 1000. This value is

configurable. You can change the value based on the number of devices in the inventory that you are monitoring.

- (20.31 HF2) Fixed an issue where the MCS profiles were getting created too slowly. (Support Case: 32440705)
 - Fixed an issue where the UIM provisioning information and the profile name were not matching with the profile variable field. This issue was being observed for the Network Connectivity (Enhanced) profile. (Support Case: 32443342)
 - Fixed an issue where the MCS query was making the SQL transaction log full after every 2-3 days. (Support Case: 32462061)
 - Fixed an issue where for several "disabled" profiles, the expected template or probe versions within the MCS backend tables were actually missing within the UIM probe/package archive. This was resulting in the profiles being disabled as MCS/ADE was unable to locate the required versions for the monitoring configuration deployment. Also, the MCS profiles were not deploying and the MCS logs were showing *maximum number of profiles*. (Support Cases: 32481934 and 32469928)
 - Fixed an issue where the default alarm policies were not getting created after upgrading from UIM 9.2.0 to UIM 20.3.1. For example, when users were creating a new profile using MCS and the processes (enhanced) template on a device, the default alarm policy "CA default policy" was not getting created. (Support Cases: 32425602 and 32475405)
 - Fixed an issue where MCS was creating the profiles at an extremely slow pace. (Support Case: 32440705)
 - Fixed an issue where the MCS template deployment for nic_monitor was failing. The MCS log was not showing up any entries of uploading the new template. It was still referring to the older version. (Support Case: 32445566)
 - Fixed an issue where users were unable to use OC after they upgraded to 20.3.2. They were observing that the performance was too slow. (Support Case: 32467330)
 - Fixed an issue where the probe deployment was getting referred for most of the robots. The MCS deployment dashboard was also showing that the profiles were still in the pending state. (Support Case: 32470045)
- **mon_config_service_cli**
 - (20.31 HF1) Fixed an issue where updates on the UIM profiles were not always triggering the probe restart. (Support Case: 32283937)
 - (20.31 HF1) Fixed an issue where the monitoring profiles were not always getting assigned to the server. (Support Case: 32327952)
 - (20.31 HF2) Fixed an issue where the MCS profiles were getting created too slowly. (Support Case: 32440705)
 - **mon_config_service_ws**
 - (20.31 HF1) Fixed an issue where updates on the UIM profiles were not always triggering the probe restart. (Support Case: 32283937)
 - (20.31 HF1) Fixed an issue where the monitoring profiles were not always getting assigned to the server. (Support Case: 32327952)
 - (20.31 HF2) Fixed an issue where the MCS profiles were getting created too slowly. (Support Case: 32440705)
 - **mon_config_service_recon**
 - (20.31 HF1) Fixed an issue where updates on the UIM profiles were not always triggering the probe restart. (Support Case: 32283937)
 - (20.31 HF1) Fixed an issue where the monitoring profiles were not always getting assigned to the server. (Support Case: 32327952)
 - (20.31 HF2) Fixed an issue where the MCS profiles were getting created too slowly. (Support Case: 32440705)
 - **nas**
 - Fixed an issue where, in UIM 20.3.0 (nas 9.31), when the parenthesis "(" or ")" was used in the Auto-Operator (AO) message matching criteria (RegEx), all alarms were matching. However, only alarms matching the alarm text should had been identified. This issue was occurring because starting from nas 9.31 RegEx is being used instead of the

pattern matching to match the alarms. This represents a change regarding the previous pattern matching behavior. Also, ensure that the RegEx defined in nas for any AO rule or pre-processing rule must be validated and must not include any RegEx complication error. For more information, see the [KB Article](#). (Support Case: 32302660)

- Fixed an issue where pre-processing rules were not working as expected in nas. (Support Case: 32476942)

- **prediction_engine**

- Fixed an issue where the prediction_engine probe was not starting. Users were receiving the "max restart reached" error. (Support Case: 32475437)
- Fixed an issue related to the vulnerability in the probe. (Support Case: 32501164)

- **robot**

- (9.32 HF1 and 9.32 SHF1) Fixed an issue where robots were not falling back to their primary hub and were staying connected to their secondary hub, until the secondary hub was switched off. This behavior was being observed in those scenarios where both the proxy_mode and strict_ip_binding were enabled for the robot. (Support Case: 32302280)
- Fixed an issue where the Windows blue screen (BSOD) was coming up during the reboot that was caused by controller.exe. Upon rebooting a system, during or immediately after the reboot process, users were observing a Windows crash event. (Support Case: 32467624)
- Fixed an issue where the UIM Server installing was failing while upgrading from 20.1.0 to 20.3.0. The installation was unable to communicate with the controller probe in the allotted time. (Support Case: 32446423)
- Fixed an issue where duplicate robots were getting reported in the OC UI, but the Admin Console was showing only one robot. (Support Case: 32450799)

- **uimapi**

- Fixed an issue where the /uimapi/hubs/{domain}/{hub}/robots endpoint was not returning the probes information in the return statement. This issue was occurring in the uimapi 20.30 version. (Support Case: 32490205)
- Fixed an issue where the GET /hubs/{domain}/{hub}/robots endpoint was returning the error `No element found for key pkg_version`. (Support Cases: 32191365 and 32193303)
- (20.32 HF2) Fixed an issue where the alarm acknowledgement was taking very long time when using uimapi. This was happening because the PUT /alarms/{alarmid}/ack API of uimapi was taking too long to complete. (Support Case: 32543378)
- (20.32 HF1) Provided the uimapi endpoint that helps encrypt the password while updating the probe configuration for the XenDesktop probe.

Download Artifacts

The UIM 20.3.3 artifacts (OC installer, UIM Server installer, and GPG Key File) are available at [UIM Hotfix Index](#).

High-Level Deployment Process

This section provides a high-level deployment process that helps you quickly get started with this release.

1. Review the [upgrade path](#).
2. Run the 20.3.3 server installer.
3. Upgrade the robots on the OC and the CABI computers to the latest version released with 20.3.3.
4. Run the OC 20.3.3 installer.
5. Upgrade the other hubs to the latest version released with 20.3.3. For more information, see the [Upgrade the Hubs](#) article.
6. Upgrade the other robots to the latest version released with 20.3.3. For more information, see the [Upgrade the Robots](#) article.

Probes and Packages

This section lists the probes and packages that are updated in UIM 20.3.3.

| Component | Version |
|-----------------------------|------------|
| automated_deployment_engine | 20.31 |
| cdm | 6.60 |
| cm_data_import | 20.33 |
| data_engine | 20.31 |
| discovery_agent | 20.33 |
| discovery_server | 20.33 |
| distsrv | 9.33 |
| ems | 10.25 |
| hdb | 9.33S |
| hub | 9.33 |
| hub_secure | 9.33S |
| hub_adapter | 9.33S |
| maintenance_mode | 20.31 |
| mon_config_service | 20.33 |
| nas | 9.32 |
| rsp | 5.50 |
| spooler | 9.33/9.33S |
| sla_engine | 20.11 |
| udm_manager | 20.33 |
| usage_metering | 9.28 |
| wasp | 20.33 |
| attr_publisher | 9.33 |
| java_jre | 2.06 |
| mcsuiapp_portlet | 1.39 |
| nisapi_wasp | 20.33 |
| policy_management_ws | 0.27 |
| robot_aix | 9.33 |
| robot_deb | 9.33 |
| robot_exe | 9.33 |
| robot_hpux | 9.33 |
| robot_update | 9.33 |
| robot_update_secure | 9.33S |
| robot_rpm | 9.33 |
| robot_sol | 9.33 |
| uimhome | 20.33 |
| uimapi | 20.33 |
| ump_accountadmin | 20.33 |

| Component | Version |
|----------------------|---------|
| uim_reportscheduler | 20.33 |
| ump_cabi | 4.23 |
| ump_dashboard | 20.33 |
| ump_operatorconsole | 2.10 |
| ump_slm | 20.33 |
| vs2017_vcrist_x64 | 1.02 |
| vs2017_vcrist_x86 | 1.02 |
| wasp_alarmviewer_api | 2.17 |
| wasp_service_wrapper | 20.33 |

Known Issues

The following are the newly found known issues in UIM 20.3.3:

- **[UIM 20.3.3] Interface Groups Not Displaying in the Dashboard Overview Page**
The Interface groups are not showing up in the dashboard overview page. For example, the Top 10 Entities (Sub Groups) view does not display in the Interface groups.
- **[UIM 20.3.3] Creation Time and Date Alarm Filter Not Working Correctly**
In the Alarm console, when users are trying to use the "Creation time & date" alarm filter with the current date, the filter is not working properly. Additionally, the column name and its date value is not displaying correctly in the Advanced Filters area.
- **[UIM 20.3.3] Session Time-out Not Working in Groups View**
While working in the Groups view in OC, the session time-out does not happen even if the time-out value is configured properly. The session continues to work irrespective of the fact that the user is idle in the Groups view.

Third-Party Software Agreements

For a list of third-party software agreements that are added in UIM 20.3.3, download the attached file "[tpsrs_uim_2033.zip](#)".

OC 20.3.2 Patch

This document provides information about the Operator Console (OC) 20.3.2 patch. OC 20.3.2 is a cumulative patch on top of OC 20.3.0 and OC 20.3.1 with upgrade supported from both the versions.

Enhanced Features

This patch includes the following enhancements:

Enhanced Group Management

The group management functionality in OC has been further enhanced to ease the group creation, edit, and management process in UIM:

- You can now define filters while creating static groups.
 - This ability lets you fetch a list of devices at the time of creating a static group. You can then browse the list to identify and add the required devices to the static group. Previously, the ability to define filters was available only for the dynamic groups.
- Complete end-to-end group creation and edit functionality is now available through the single UI dialog.

- You no longer need to move across different screens to perform create or edit operations. For example, previously, the process of creating static groups was spread across multiple UI screens. Now, you can achieve the same functionality using the single screen.
- Similarly, when you try to edit a group, you can find all the options to edit a group at the same place (Actions menu (three dots), Edit group). For example, the following options are now consolidated and are available as part of the edit group dialog:
 - Modify the filter criteria.
 - Add devices to a static group.
 - Remove devices from a static group.
 - Update the group name or description.
 - Change the account information.
 Previously, these options were scattered across different locations in the UI.

For more information, see the [Manage Groups](#) article.

Enhanced Monitoring Configuration Service (MCS) UI

The following enhancements have been made to the MCS UI in OC:

- The Actions column on the Profiles page now logically organizes different actions that you can perform on the created profiles. The available actions are copy a profile, delete a profile, and view the profile details:
 - The copy profile icon is now logically grouped under the Actions column along with the new icons (delete profile and profile details).
 - The delete profile icon lets you delete a created profile directly from the Profiles page. You no longer need to navigate to the specific profile page to delete it.
 - The details icon lets you view the profile details information. The detailed information helps you determine if a configuration profile was successfully applied to target devices.
- At the time of creating a profile, you can now view the template version. The version of the template is displayed as a separate column (Template Version).
- In addition to the existing Profiles tab and the Alarm Policies tab, a new tab (MCS Deployment Overview) is now added to the UI. This tab provides an in-context linking of the profiles to MCS Deployment Dashboard. You can access this tab through the same Monitoring Config icon (gear icon) that you use to access the Profiles and Alarm Policies tabs.
- The Profiles page now contains additional columns, Profile Id and Derived from Group, to provide the relevant information.

For more information, see the [Manage Monitoring Using MCS Profile Types](#) article.

Enhanced Session Management

UIM now provides the following token parameters in the `wasp.cfg` file that help administrators efficiently manage the user sessions:

- **`oc.jwt.expiryInSecs`** Allows administrators to specify the appropriate interval (in seconds) after which the session of the inactive users is expired. After the expiry of the session, when the users try to perform any action in the OC UI, they receive a session timeout expiry message along with the login link.
- **`oc.jwt.refreshInterval`** Allows administrators to configure the refresh interval (in seconds). Based on the specified interval, the session is appropriately refreshed if the user is active in the UI. Ensure that the value of the refresh interval is lower than the session expiry (`oc.jwt.expiryInSecs`) value.

NOTE

OC users can add the `keep-alive=true` parameter to the OC URL to continue working in the UI without any interruption. For example, `http://<OC_server>/operatorconsole_portlet/standalone_login.jsp?keep-alive=true`.

View List of Maintenance Schedules for Devices

You can now access the list of maintenance schedules from the device view. When you select a device through the Inventory view, you can see all the maintenance schedules that include the selected device. To access the list, click the Information icon (Name column) for the selected device, and select the Maintenance tab. You can then access the following information:

- Name of the maintenance schedule that contains the device.
- Status (Active or Inactive) of the maintenance schedule that contains the device.
- An option to remove the device from the maintenance schedule. When you click the minus icon (Disassociate column), the device is removed from the maintenance schedule. The corresponding row is also removed from the table.

For more information, see the "View Maintenance Schedule for Devices" section in the [View Your Inventory](#) article.

Prerequisites

Verify that your existing environment is using 20.3.0 or 20.3.1.

Deployment

You can upgrade from:

- OC 20.3.0 to OC 20.3.2
- OC 20.3.1 to OC 20.3.2

Follow these steps:

1. Download the OC 20.3.2 patch installer from [UIM Hotfix Index](#).
2. Run the OC 20.3.2 patch installer on the primary hub and specify the OC server during the upgrade.
3. [Download](#) the MCS 20.31 HF1 (or higher) package bundle and deploy the MCS 20.31 HF1 (or higher) packages as follows:

NOTE

If you are upgrading from 20.3.0 to 20.3.2, you need to first upgrade the MCS 20.30 packages to [MCS 20.31](#) and then apply the MCS 20.31 HF1 (or higher) packages. For 20.3.1 to 20.3.2, directly apply the MCS 20.31 HF1 (or higher) packages.

- a. Deactivate the existing `mon_config_service` probe on the primary hub, deploy the `mon_config_service` 20.31 HF1 (or higher) package to the primary hub, and activate `mon_config_service`.
 - b. Deactivate the `wasp` probe on the OC robot, deploy the `mon_config_service_ws` 20.31 HF1 (or higher) package to the OC robot, and activate `wasp`. This step is required if you are using the MCS web services.
 - c. Deploy the `mon_config_service_recon` 20.31 HF1 (or higher) package to the primary hub and activate the probe after it gets created. This step is required if you want to use the MCS reconciliation functionality.
 - d. Deploy the `mon_config_service_cli` 20.31 HF1 (or higher) package to the primary hub. This step is required if you are using the MCS CLI functionality.
4. If your environment contains multiple OC instances, perform the following additional steps on your secondary OC servers:
 - Upgrade the packages listed in Step 2 of the [Configure a Secondary OC Server](#) section to the latest version that the OC 20.3.2 patch provides. You can find the latest packages in the local archive.
 - Execute Step 3b on the secondary OC robots.
 - Deploy the `ump_slm` 20.32 package to the secondary OC robots. The `ump_slm` 20.32 package is available in the local archive.

Resolved Issues

The following issues have been resolved in this patch release:

- Resolved an issue where users were facing problems while creating OC groups with the SQL type filter criteria. (Support Case: 32368990)
- Resolved an issue where users were not able to apply a duration of more than 12 hours while creating a maintenance schedule. (Support Cases: 32391126 and 32418953)
- Resolved an issue where when users were adding the maintenance schedule through the Swagger UI, the schedules added through the OC UI were disappearing. Additionally, even the Swagger-created schedule was not becoming visible in the UI.
However, if the Swagger-created schedule was deleted from the database, the schedules created through the UI were appearing again. (Support Cases: 32285971, 32329398, and 32391160)
- Resolved an issue where in the Alarm properties (expanded item on the tab overview), the policy name was displaying the ID instead of the name. (Support Case: 32387893)
- Resolved an issue where the time for the maintenance schedule was getting changed to the 24-hour format with AM (for example, 17:00 AM). (Support Case: 32407130)
- Resolved an issue related to the maintenance mode view. Now, with this patch, when a computer system is in the maintenance mode, the Inventory view does not show an alarm icon; instead, it displays the maintenance mode icon. Also, in the Groups tree view, the system in a group displays the maintenance mode icon instead of an alarm icon. (Support Cases: 32345467 and 32301665)
- Resolved an issue where OC session was not timing out. The session was remaining active even after being idle for 72 hours.
- Resolved an issue where the Bus users were observing occasional interchanging of the groups in the tree view. This was occurring when two different account users were creating the groups with the same name.
- Resolved an issue where an incorrect label “Interface Filters” was getting displayed in the UI when users were trying to edit a dynamic group. The dynamic group was created with the OR conditions in the group filter criteria.
- Resolved an issue where when the alarms were getting created as a result of an alarm policy in the alarms page of OC, the link to the alarm policy was not enabling for the newly created alarm policies.
- Resolved an issue where users were unable to view the summary of the maintenance schedule group at the device level. (Support Case: 32419077)
- Resolved an issue where the MCS Deployment Dashboard was not working; it was displaying the following error:

```
Data access error
The data required for this page is not currently available
```

(Support Cases: 32398161 and 32396442)
- Resolved an issue where the Dashboard was not filtering the data correctly; it was not considering the time-related filters. (Support Case: 32271065)
- Resolved an issue where the account contact users were not able to see the metrics in the created Dashboard. (Support Case: 32263741)

Known Issues

The following are the newly added known issues that are applicable for this patch release:

- **[OC 20.3.2] SAML SSO Not Forwarding Additional URL Request Parameters**
With SAML SSO, the session timeout configuration is considered, and every user request adheres to the centralized session time out configured in the `wasp.cfg` file. It does not allow the users to create the sessions that will never expire with the `keep-alive` flag set to `true` in the URL request parameter.
- **[OC 20.3.2] Duplicate Devices Are Displaying While Editing a Static Group**
While editing static groups, users can see duplicate devices in the device selection area of the edit group dialog. Out of the two entries, one entry is selected and the other is unselected. If users select an unselected device, they receive an exception in that case.

NOTE

This issue has been fixed in [UIM 20.3.3](#).

UIM 20.3.1

As part of the regular release cycle for updating Unified Infrastructure Management (UIM), we are pleased to announce the UIM 20.3.1 patch release. This release includes new and enhanced features, resolved issues, and so on.

New and Enhanced Features

The following features and enhancements have been included in 20.3.1:

Service Level Management

This release of UIM provides the Service Level Management (SLM) functionality. The SLM view is an interface to create service-level agreements (SLAs) and their component service-level objectives (SLOs) and quality of service (QoS) constraints. With this functionality, you can build powerful, extensible, and measurable agreements with clients. Once you define SLAs in the SLM view, data is recorded and compliance is computed automatically.

For more information about how to work with SLM, see the [SLM View](#) article.

SLA Reports

You can also view reports on SLA compliance in the SLA Reports interface and can export them for transmission to clients. The SLA Reports view displays performance information for service level agreements (SLAs) defined in the SLM.

For more information about SLA Reports, see the [SLA Reports](#) article.

Access Admin Console from OC

You can now access the Admin Console UI from Operator Console (OC). This ability provides a seamless access to the Admin Console UI without logging out of OC. The Admin Console application allows you to manage and maintain the hubs, robots, and probes on your system.

For more information about how to access Admin Console from OC, see the [Admin Console in OC](#) article.

Alarm Policy Enhancement

The alarm policy functionality has been enhanced in this release to provide a centralized threshold management for technologies that are monitored remotely. For remote probes, alarm policies are no longer tied with the robot, which implies that the same policies are not applied to all the devices that a remote probe manages.

You can define separate thresholds for different devices or groups that are monitored through the same remote probe. Therefore, for devices or groups that a remote probe manages, alarm policies are now applied only to those devices for which they were created. This ensures that alarms are generated only for the relevant devices, allowing you to manage your policies and alarms in a more efficient manner.

For more information, see the "Centralized Threshold Management for Technologies Monitored Remotely" section in the [Manage Alarms with Centralized Alarm Policies](#) article.

Copy MCS Profiles

You can now copy a device or a group profile (the source) and apply the copied profile to another device or group profile (the target). Monitoring Configuration Service (MCS) then analyzes the source against the target and performs the appropriate action. When you apply a profile at the group level, MCS applies this profile to all devices within the group.

For more information about how to copy and apply MCS profiles, see the [How to Copy and Apply MCS Profiles](#) article.

Delete a Device Using OC

UIM now lets you remove devices using the Operator Console (OC) Inventory view. The process gives you the ability to delete a device from inventory and prevent rediscovery, close alarms associated with the device, and delete stored QoS data for the device.

For more information about how to delete a device using OC, see the [Remove Devices in OC](#) article.

Deprecated Portlets

To view the complete list of deprecated portlets, see the [Deprecated Portlets](#) article.

Enable Read-Only Access to MCS Profiles

This release of UIM facilitates read-only access to the MCS profiles based on the role of a user. A new permission is now available that provides the read-only access to the user. Users with this permission can only view the MCS profiles; they cannot edit, create, or delete them. This ensures that only relevant users are allowed to perform the required operations on the profiles.

For more information about how to enable the read-only access to the MCS profiles, see the [Enable Read-Only Access to MCS Profiles](#) article.

Enhanced Telemetry for PLA Model

Telemetry is a foundational element of the Enterprise Software Portfolio License Agreement (PLA) model. The initial requirement of the Telemetry effort is to collect and report product-specific usage daily in support of the new consumption model. Broadcom uses its own endpoint to support the Enterprise Software Telemetry rollout. This endpoint provides a centralized platform for the collection and routing of usage data through various pre-built integrations and destinations.

For more information, see the [Configure Telemetry for the PLA Model](#) article.

Manage Discrepancies Between Expected and Existing MCS Configurations

The GA version of the `mon_config_service_recon` probe is now available that lets you administer the MCS configurations in your UIM environment. You can use this probe to detect and handle discrepancies between the expected configuration and the existing configuration that is deployed to the probes in your environment.

For more information about how to work with this probe, see the [mon_config_service_recon probe](#) documentation.

UIM Perl SDK Supports TLS 1.2

An updated version of the Perl SDK is now available. This version of the SDK supports Perl v5.32, which provides the TLS 1.2 support in the SDK while communicating with the UIM databases (Oracle and Microsoft SQL Server).

The Perl SDK now supports only the following UIM-supported platforms:

- Microsoft Windows x86_64
- Linux x86_64

For more information, see the Perl SDK section in the [Working with Development Tools](#) article.

Resolved Issues

The following issues have been resolved in this release:

- Resolved an issue where users were getting the data access error when they were trying to launch the MCS Dashboard from the OC UI (with MySQL as the database).
- Fixed an issue where while trying to create a ticket in ServiceNow from the Alarms view in OC, the ticket was not getting created. The Create Ticket option was available along with the alarms, but it was not allowing to create the tickets.
- Resolved an issue where when the same groups were created from two different account users, only one group was getting displayed in the tree view. However, the List and the Card views were displaying both the groups. This issue was occurring when the UIM 20.3.0 setup was using the Oracle database.
- Fixed an issue where the alarms table was displaying the "Error retrieving alarms" message instead of "No active alarms" even when all the alarms were acknowledged. This issue was occurring when the UIM 20.3.0 setup was using the Oracle database.
- Fixed an issue where moving a robot from one hub to another was not changing the origin in OC. The old hub was still shown as the origin of the robot even when the robot was moved to a new hub.
- Fixed an issue where after creating the "remote system monitoring" profile at the group level for non-robot devices, when users were trying to click the non-robot device and open the profile, they were receiving an error.
- Fixed an issue where the MCS profile names in the Remote and Cloud Monitoring option of the Setup Wizard (in OC) were not always visible. This behavior was occurring when the database was Oracle.
- Fixed an issue where the robot deployment configuration/status was missing for the robot deployment functionality in OC.
- Fixed an issue where switching from one group to another in the dashboards was not working properly in the tree view. The dashboards were showing the previous group details instead of a new group even when the users moved to the new group.
- Fixed an issue where the option to remove a device was not available in the Inventory view of OC.
- Fixed an issue where users were unable to create the Microsoft Windows Service (ntservices) "For-Each" group profile. When they tried to create it, the service name field remained in the disabled state. Therefore, the values were not becoming available for mapping the keys in the "For-Each" profile.
- Fixed an issue where users were unable to delete those device-level profiles that were created by the group-level profile. The delete option was not deleting the profiles.
- Fixed an issue where when the SQL_Response OLEDB legacy profile was created with "For Each Deployment Enable" = Yes, the group level profiles were getting migrated, but not the device-level profiles.
- Resolved an issue where the device-level profile migration was not working for the For-Each profile.
- Fixed an issue where the newly enabled metrics were not reflecting in the UI for the existing Apache MCS profile. They were remaining in the disabled state.
- Resolved an issue where the profiles were not getting created when users were trying to create a "For Each" profile in OC using the "{foreach-instance}" details.

Upgrade Patch Artifacts

The following artifacts are available as part of the UIM 20.3.1 patch:

| Artifact | Version Number | Download Location |
|--|----------------|--|
| OC Installers <ul style="list-style-type: none"> • installOC.exe (Windows) • installOC_linux.bin (Linux) | 20.3.1 | UIM Hotfix Index |
| Robot Packages <ul style="list-style-type: none"> • robot_update • robot_update_secure | 9.32 | Web Archive and UIM Hotfix Index |

| | | |
|--|---|--|
| MCS Packages (provided as mon_config_service bundle): <ul style="list-style-type: none"> mon_config_service mon_config_service_ws mon_config_service_recon mon_config_service_cli | 20.31 | UIM Hotfix Index |
| Perl and Perl SDK Packages <ul style="list-style-type: none"> Perl_LINUX_23_64 SDK_PERL | <ul style="list-style-type: none"> 5.32 (for Perl_LINUX_23_64) 20.30 (for SDK_PERL) | Web Archive and UIM Hotfix Index |
| PLA Telemetry <ul style="list-style-type: none"> uimesdplatelemetry | 1.07 | Web Archive and UIM Hotfix Index |
| UIMAPI Package <ul style="list-style-type: none"> uimapi | 20.31 | Web Archive and UIM Hotfix Index |

High-Level Upgrade/Deployment Process

For the UIM 20.3.1 upgrade, review the following points:

- Before you upgrade to UIM 20.3.1, verify that your existing environment is using UIM 20.3.0.
- The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch contains separate standalone artifacts that you need to deploy manually to upgrade the respective components to 20.3.1. Therefore, ensure that you deploy the latest packages (for example, robot_update, mon_config_service) that are available for 20.3.1.
- The UIM 20.3.1 patch also includes an upgrade installer for OC. You can run the OC upgrade installer to upgrade OC 20.3.0 to OC 20.3.1.
- Finally, after upgrading all the appropriate components, you can start using the features that the UIM 20.3.1 patch provides.

The recommended high-level steps to apply the patch artifacts are as follows:

1. Deploy robot 9.32 to the core robots (for example, hub, OC, CABI).
2. Run the OC 20.3.1 upgrade installer on the primary hub and specify the OC server during the upgrade.
3. Deploy the MCS 20.31 packages as follows:
 - a. Deactivate the existing mon_config_service probe on the primary hub, deploy the mon_config_service 20.31 package to the primary hub, and activate mon_config_service.
 - b. Deactivate the wasp probe on the OC robot, deploy the mon_config_service_ws 20.31 package to the OC robot, and activate wasp. This step is required if you are using the MCS web services.
 - c. Deploy the mon_config_service_recon 20.31 package to the primary hub and activate the probe after it gets created. This step is required if you want to use the MCS reconciliation functionality.
 - d. Deploy the mon_config_service_cli 20.31 package to the primary hub. This step is required if you are using the MCS CLI functionality.
4. Deploy the uimapi 20.31 package to the OC robot.
5. Deploy the other packages: uimesdplatelemetry (on UIM Server) and SDK_PERL (on any robot), if required.
6. If your environment contains multiple OC instances:
 - a. On your secondary OC servers, upgrade the relevant packages listed in Step 2 of the [Configure a Secondary OC Server](#) section to the 20.3.1 version. The 20.3.1 packages are available in the local archive.
 - b. Execute Step 3b (deploy mon_config_service_ws 20.31) and Step 4 (deploy uimapi 20.31) on the secondary OC robots.
 - c. Deploy the ump_slm 20.31 package to the secondary OC robots. The ump_slm 20.31 package is available in the local archive.

Known Issues

The following are the newly added known issues that are applicable for the 20.3.1 patch:

- **[UIM 20.3.1] Delayed Discovery Agent Status**
When a discovery is scheduled, it is taking some time to update the status in the UI. This behavior is occurring because when a discovery is scheduled on a discovery agent, the agent status is delayed by 1 minute due to the internal architecture. This causes the delay in the status. This can be treated as a known issue.
- **[UIM 20.3.1] Context Launch for DX NetOps Spectrum Alarms Not Available in OC**
For the DX NetOps Spectrum-UIM integration, the context launch for the DX NetOps Spectrum alarms is not available from the OC interface. This issue will be addressed soon.
- **[UIM 20.3.1] System-Generated Job Not Getting Created after Saving SLA**
When you save SLA, the system-generated job is not getting created if there is no change in the SLA form.
- **[UIM 20.3.1] Exporting SLA to PDF Truncates the QoS Constraint List of SLOs**
In SLA Reports, when you export the SLA to the PDF format, the SLA and SLO information is exported to the PDF. However, the list of QoS constraints configured in the SLO is not exported completely.
NOTE
This issue has been fixed in the [UIM 20.3.3](#) release.
- **[UIM 20.3.1] Incorrect Label “Interface Filters” Coming Up During Group Edit**
If a dynamic group is created with the OR conditions in the group filter criteria, then an incorrect label “Interface Filters” is getting displayed in the UI when you try to edit that group.
NOTE
This issue has been fixed as part of the [OC 20.3.2 patch](#) release.
- **[UIM 20.3.1] Interchanging of Group Names in Tree View**
When groups are created with the same name by two different account users, the Bus users will see the occasional interchanging of the groups in the tree view.
NOTE
This issue has been fixed as part of the [OC 20.3.2 patch](#) release.

To view the complete list of known issues that are applicable for this release, see the "UIM 20.3.1 Known Issues" section in the [Known Issues](#) article.

Third-Party Software Agreements

For a list of third-party software agreements that are newly added in UIM 20.3.1, download the attached file "[#unique_32](#)

NOTE

To view the complete list of third-party software agreements, see the [related TPSR article](#).

What's New

UIM 20.3.3 (March 2021)

This section outlines the new features and enhancements that are available in UIM 20.3.3.

- Metrics Palette Enhancements
- Removing CABI Dependency (Native Operator Console)
- Availability of Report Scheduler
- Packages Signed with GPG-Enabled Keys
- Secure Transmission of Certificates
- Ability to Change the Password
- Alarm Console Enhancements
- Asynchronous Distribution of Probes
- Creating New Custom Dashboard Views
- Data Maintenance Stored Procedures Enhancement
- discovery_server Enhancement
- Group Management Enhancements
- Group View and Alarm View Optimization
- Improved Implementation of the Alarm Policy and MCS ACL Permissions
- Monitoring Configuration Service (MCS) Enhancements
- Persist Maintenance Schedules in the nas Probe
- Deprecating the ace Probe
- Platform Support

For more information, see the [UIM 20.3.3](#) article.

OC 20.3.2 Patch (December 2020)

This section outlines the enhancements that are available in the OC 20.3.2 patch:

- Enhanced Group Management
- Enhanced Monitoring Configuration Service (MCS) UI
- Enhanced Session Management
- View List of Maintenance Schedules for Devices

For more information, see the [OC 20.3.2 Patch](#) article.

UIM 20.3.1 (November 2020)

This section outlines the new features and enhancements that are available in the UIM 20.3.1 patch.

- Service Level Management
- SLA Reports
- Access Admin Console in OC
- Alarm Policy Enhancement
- Copy MCS Profiles
- Delete a Device Using OC
- Deprecated Portlets
- Enable Read-Only Access to MCS Profiles
- Enhanced Telemetry for PLA Model
- Manage Discrepancies Between Expected and Existing MCS Configurations
- UIM Perl SDK Supports TLS 1.2

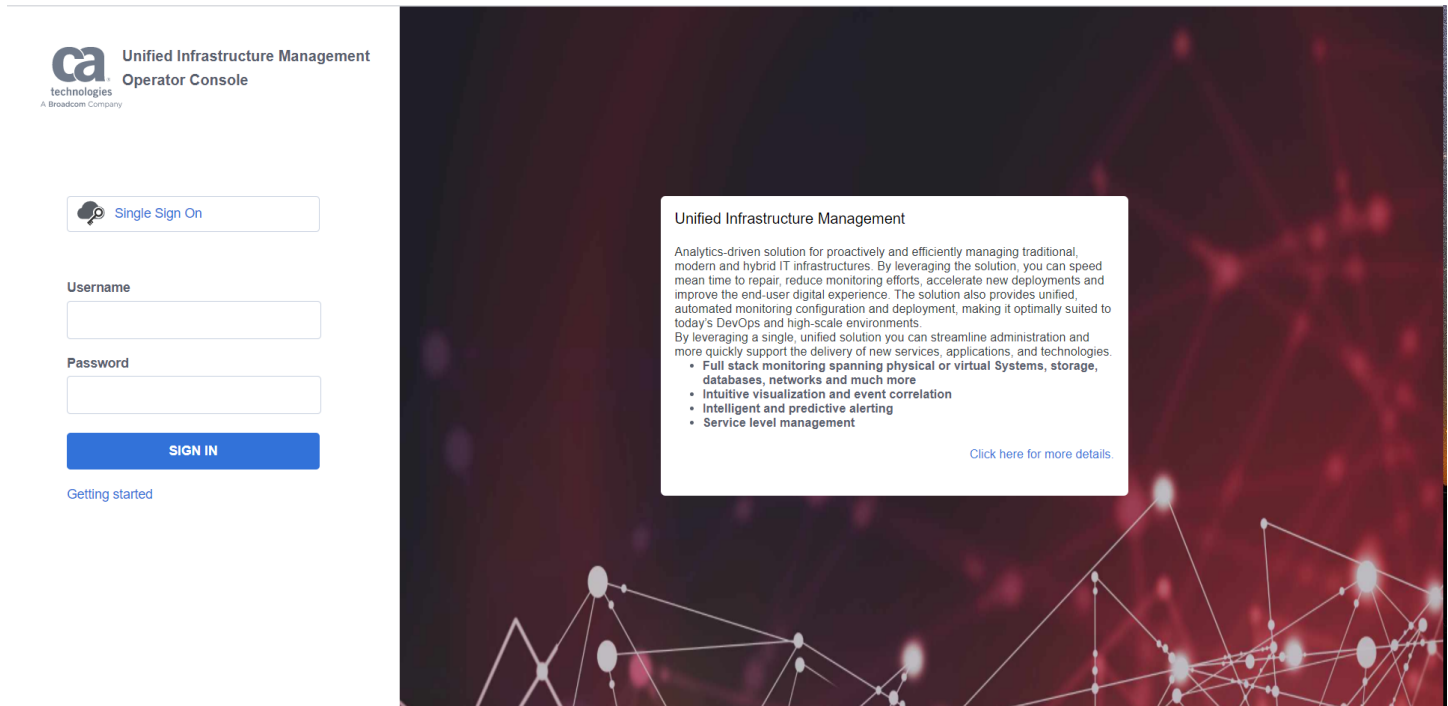
For more information about the new features, enhancements, resolved issues, and known issues, see the [UIM 20.3.1](#) article.

UIM 20.3.0 (September 2020)

This section outlines the new features and enhancements that are available in the UIM 20.3.0 release.

Zero Flash UIM

UIM 20.3.0 has removed the dependency on Adobe® Flash® Player. This release now provides an enhanced web-based user interface for both Operator and Administrator personas.



The enhanced user interface provides ease of use for both operators and administrators, like providing modern context-aware observability engagement layer for infrastructure management.

With the removal of Adobe Flash, the Unified management portal (UMP) that contained flash-based portlets has been deprecated. The Operator Console (OC) and Admin Console interfaces are now web-based.

Operator Console Enhancements

With UIM 20.3.0, the enhanced Operator Console supports most of the UMP functionality to meet the needs of the Operator and Administrator personas for infrastructure management.

Highlights of the newly added and enhanced features in the OC are as follows:

- View, manage, and act on alarms using the alarm console.

CA Unified Infrastructure Management UIM | Home > Alarms | administrator Logout

Filter Results 53 Show Historical

Alarm By Severity

Alarm By Probes

Top Alarming

| Host | Count |
|-----------------------------------|-------|
| w19robot21 | 16 |
| LVNLVCLM | 5 |
| vm668039vm1apm.dhcp.broadcom.net | 4 |
| vm668039vm2uim1.dhcp.broadcom.net | 4 |

| <input type="checkbox"/> | | Device Name | Actions | Alarm Type | Owner | Alarm Message | Duration | Count | Acknowledged... |
|--------------------------|--|--------------|---------|------------|------------|---|------------|-------|-----------------|
| <input type="checkbox"/> | | w19robot21 | ⋮ | MySQL | Unassigned | sample_profile-thread_cache_hi_rate. Perce... | 7 minutes | 8 | - |
| <input type="checkbox"/> | | LVNLVCLM | ⋮ | Nutanix | Unassigned | Controller VM 10.17.12.154 is not reachable ... | 34 minutes | 1 | - |
| <input type="checkbox"/> | | LVNLVCLM | ⋮ | Container | Unassigned | QOS_NUTANIX_AVERAGE_CONTAINER_LATE... | an hour | 17 | - |
| <input type="checkbox"/> | | LVNLVCLM | ⋮ | Container | Unassigned | QOS_NUTANIX_TOTAL_CONTAINER_USAGE ... | an hour | 17 | - |
| <input type="checkbox"/> | | LVNLVCLM | ⋮ | Container | Unassigned | QOS_NUTANIX_TOTAL_CONTAINER_CAPACI... | an hour | 17 | - |
| <input type="checkbox"/> | | LVNLVCLM | ⋮ | Container | Unassigned | QOS_NUTANIX_AVERAGE_CONTAINER_IOPS... | an hour | 17 | - |
| <input type="checkbox"/> | | w19robot21 | ⋮ | MySQL | Unassigned | sample_profile-stmts_rollback_commit_ratio... | an hour | 57 | - |
| <input type="checkbox"/> | | 10.17.12.150 | ⋮ | Nutanix | Unassigned | Features not permitted by Starter license are ... | an hour | 1 | - |
| <input type="checkbox"/> | | w19robot21 | ⋮ | SQL-Server | Unassigned | Profile sample_profile, instance lvmssql2016... | an hour | 1 | - |
| <input type="checkbox"/> | | w19robot21 | ⋮ | SQL-Server | Unassigned | Profile sample_profile, instance lvmssql2016... | an hour | 1 | - |

©2020 CA. All rights reserved.

- Use the enhanced inventory management in the context of groups and devices, along with maintenance scheduling.

CA Unified Infrastructure Management UIM | Home > Inventory | administrator Logout

Filter 338 2 minutes ago

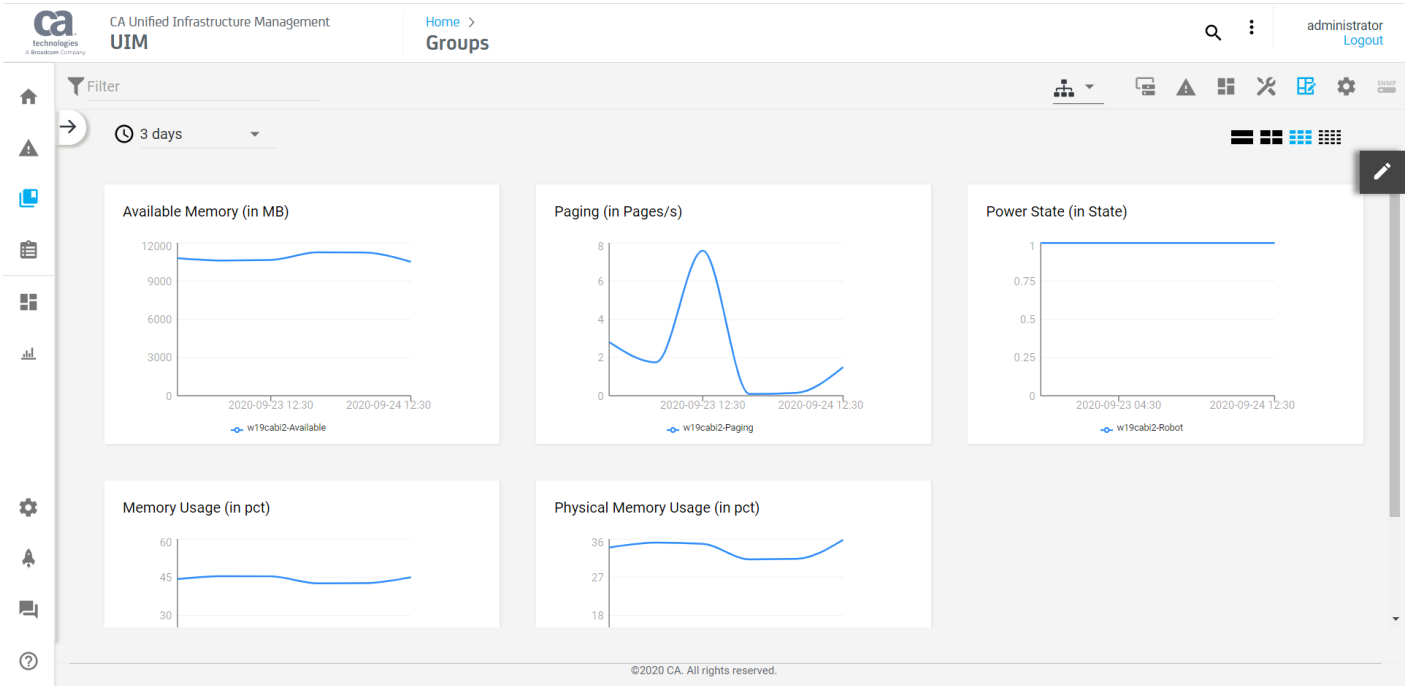
| <input type="checkbox"/> | | Name | Device Type | Operating sy... | Origin | IP address |
|--------------------------|--|--------------------------|-------------|-----------------|----------------|---------------|
| <input type="checkbox"/> | | systemrh1-node4 | NutanixVM | | W19SERVER2_hub | 10.17.169.101 |
| <input type="checkbox"/> | | systemrh1-node6 | NutanixVM | | W19SERVER2_hub | 10.17.167.189 |
| <input type="checkbox"/> | | syscapmdaopenjdk | NutanixVM | | W19SERVER2_hub | 10.17.164.140 |
| <input type="checkbox"/> | | sysnfsharvesteropenj... | NutanixVM | | W19SERVER2_hub | 10.17.165.101 |
| <input type="checkbox"/> | | systemspectrum | NutanixVM | | W19SERVER2_hub | 10.17.164.172 |
| <input type="checkbox"/> | | vm670517-SMTPserver | NutanixVM | | W19SERVER2_hub | |
| <input type="checkbox"/> | | sysadaconsoleopenjd... | NutanixVM | | W19SERVER2_hub | 10.17.165.168 |
| <input type="checkbox"/> | | sysadaconsoleopenjd... | NutanixVM | | W19SERVER2_hub | 10.17.164.99 |
| <input type="checkbox"/> | | doi-automation-spectr... | NutanixVM | | W19SERVER2_hub | 10.17.166.19 |
| <input type="checkbox"/> | | doi-automation-nfa1 | NutanixVM | | W19SERVER2_hub | 10.17.165.5 |
| <input type="checkbox"/> | | va654565-Spectrum4 | NutanixVM | | W19SERVER2_hub | 10.17.168.153 |

Inventory Tree

- Inventory (338)
 - W19SERVER2_domain/W19SERVER2 (0)
 - W19SERVER2_domain/vm668039vm1apm (0)
 - W19SERVER2_domain/w19robot22 (0)
 - W19SERVER2_domain/vm668039vm1uim1 (0)
 - W19SERVER2_domain/w19cabi2 (0)
 - W19SERVER2_domain/w19ump2 (0)
 - W19SERVER2_domain/w19robot21 (0)
 - W19SERVER2_domain/w19sechub2 (11)
 - Automatic (327)

©2020 CA. All rights reserved.

- View and compare performance metrics using the enhanced metric viewer.

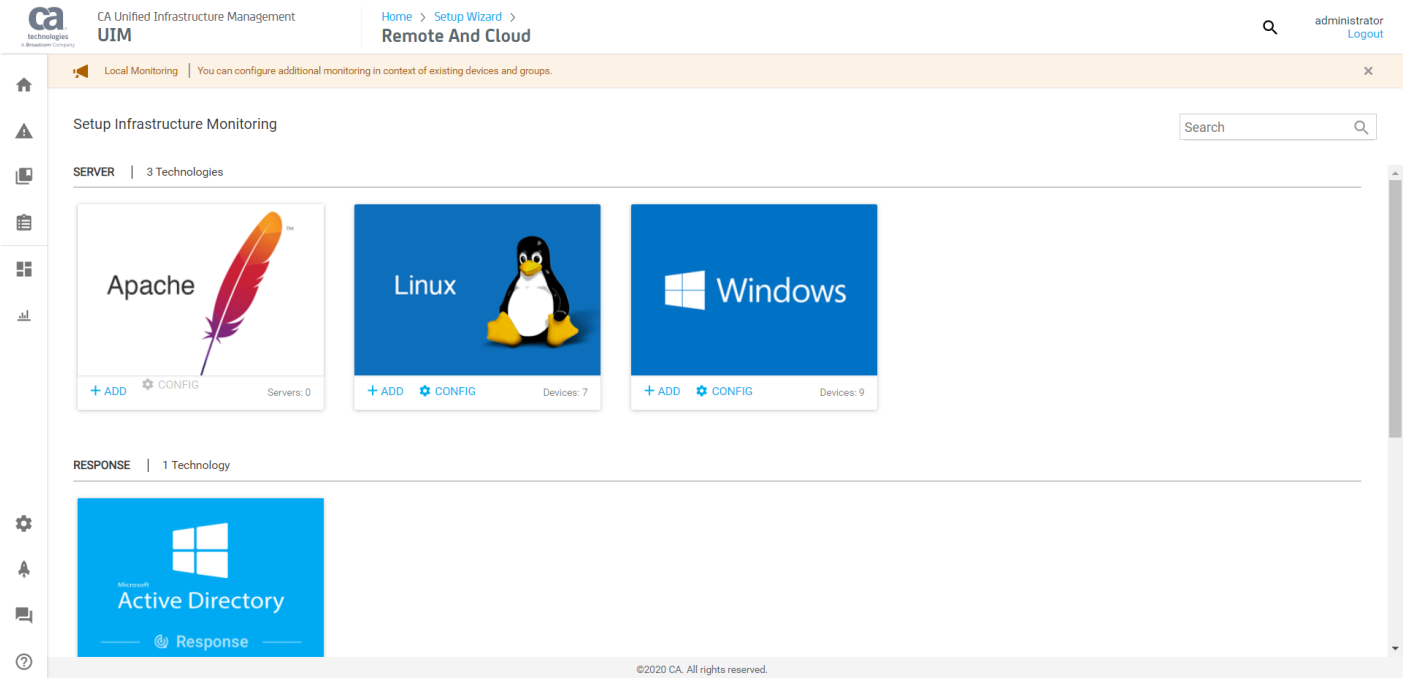


- Use the integrated discovery wizard for quick onboarding of computers and devices.

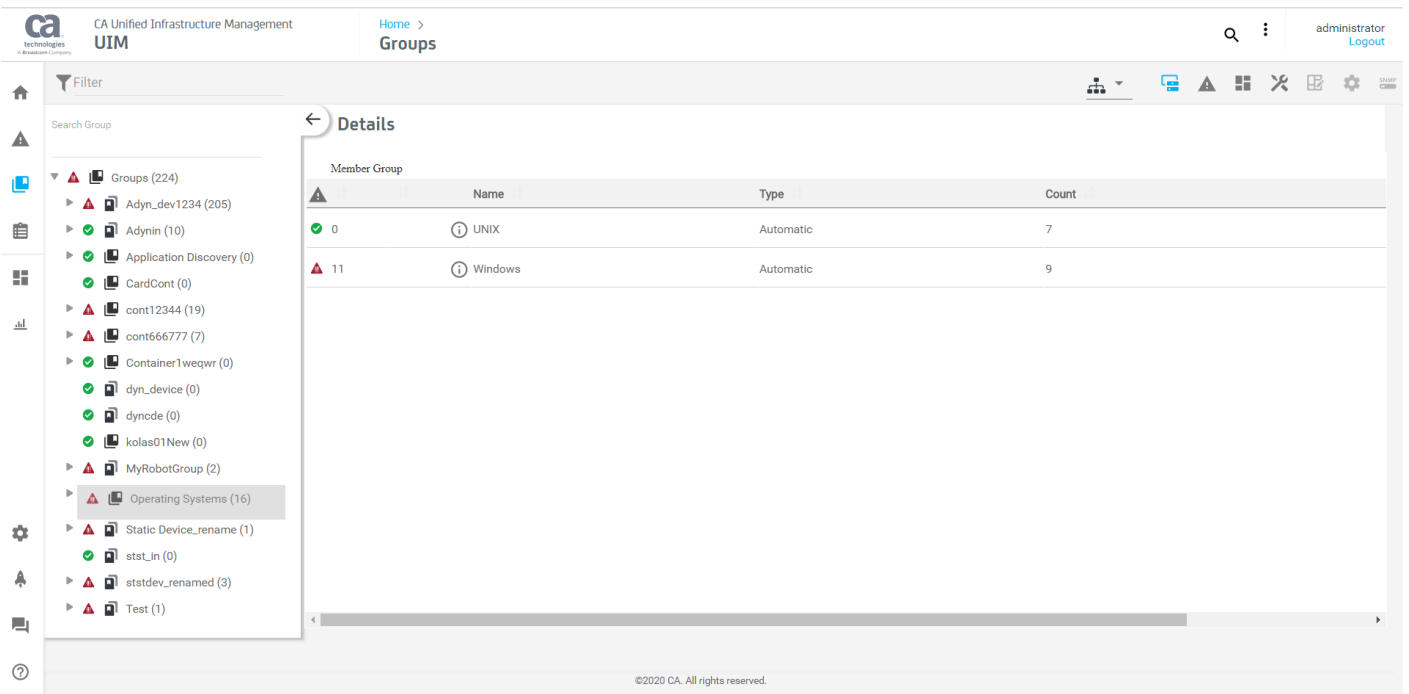
The screenshot shows the 'Discover Devices' step of the Setup Wizard in CA Unified Infrastructure Management (UIM). The breadcrumb trail is 'Home > Setup Wizard > Discover Devices'. The selected agent is 'W19SERVER2_hub/vm668039vm1apm'. The wizard includes tabs for 'Setup WMI Credentials', 'Setup Linux/Unix Credentials', 'Setup SNMP Credentials', 'Define Scopes', and 'Schedule Discovery'. The main content area features a search bar with a plus sign and the text: 'WMI (Windows Management Instrumentation) discovery scans servers running Windows to gather system information. Click + to add a WMI authentication profile, or click on an existing authentication profile to make changes.' Below this, it says 'No Items Available'. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

©2020 CA. All rights reserved.

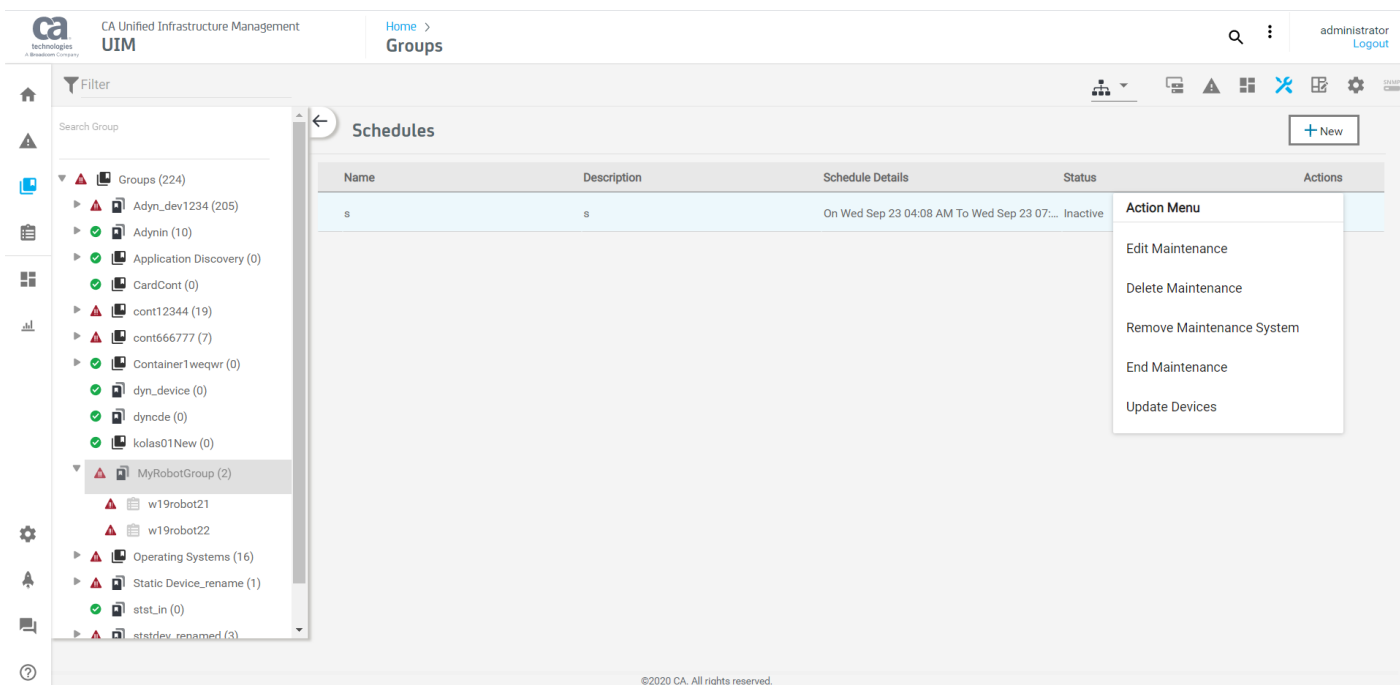
- Use the setup wizard for the agent monitoring configuration.



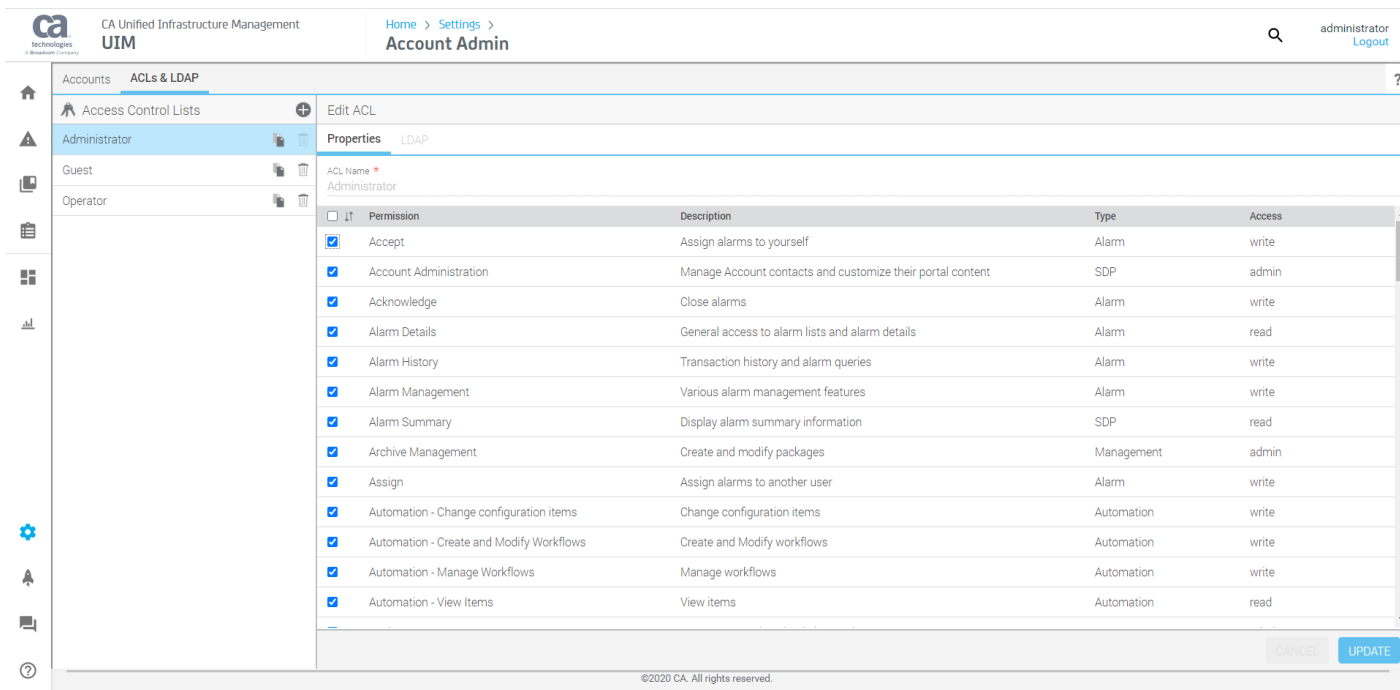
- Use the multiple viewing and contextual navigation options for groups and devices.



- Use the context-aware maintenance scheduling to temporarily suppress the alarms during the maintenance windows.



- Continue managing accounts, users, and access control lists (ACLs) for tenancy needs.

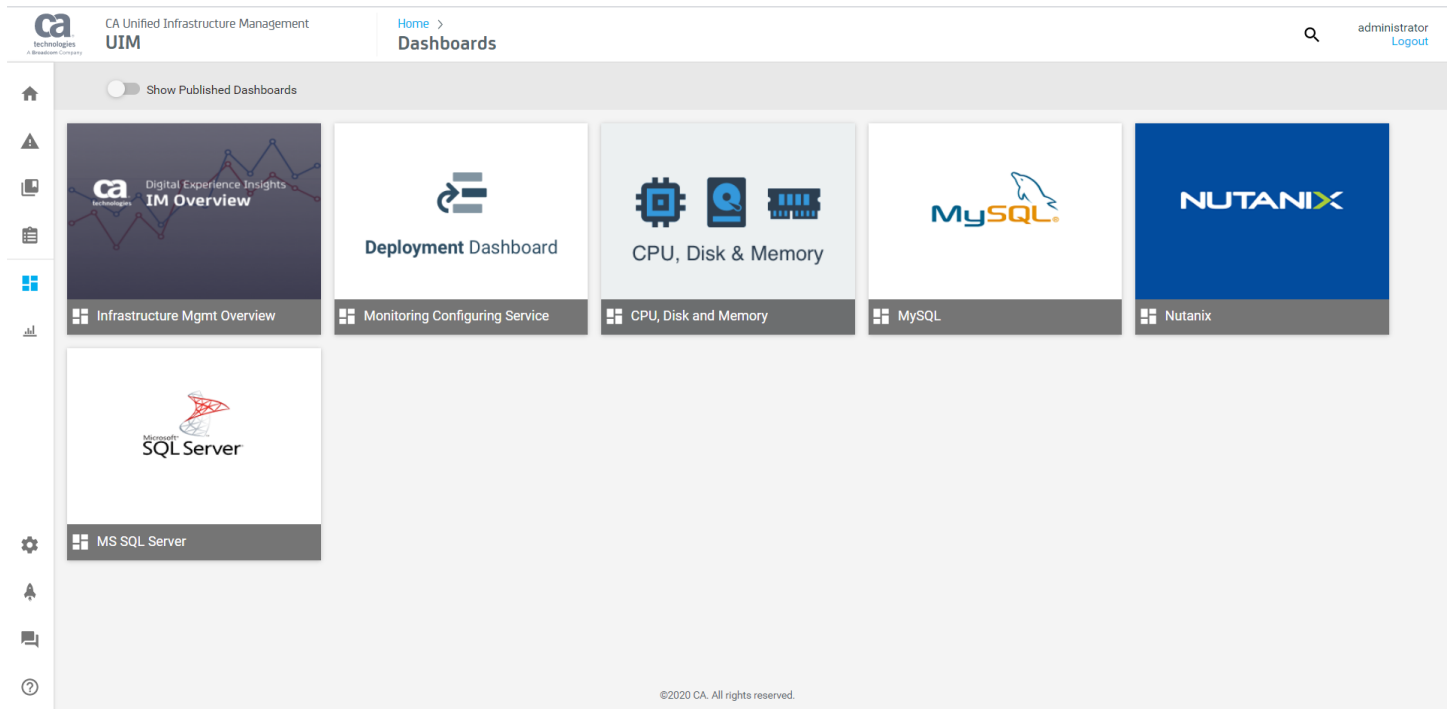


For more information, see [Operator Console](#).

CABI Integration in UIM 20.3.0

In UIM 20.3.0, bundled CABI supports the JasperSoft Server version 7.5, offering wider platform coverage and performance improvements. Bundled CABI supports fresh installation and upgrades. Upgrades are supported from the CABI version 3.4 (or later) based on the JasperSoft Server upgrade paths. JasperSoft Server 7.5 supports direct upgrades from JasperSoft Server 6.4.3 onwards.

cabi_external continues to support *Unified CABI with JasperSoft Server 7.1.1 integration*, which is the same as in UIM 20.1.0.



For more information, see [CA Business Intelligence JasperReports Server with CA UIM Release Notes](#).

For-Each Functionality

The For-Each functionality supports the bulk deployment of the profiles at a group level. Using the For-Each feature, you can now create profiles for all the devices at the group level.

For more information, see [For-Each](#).

Auditing in UIM Interfaces

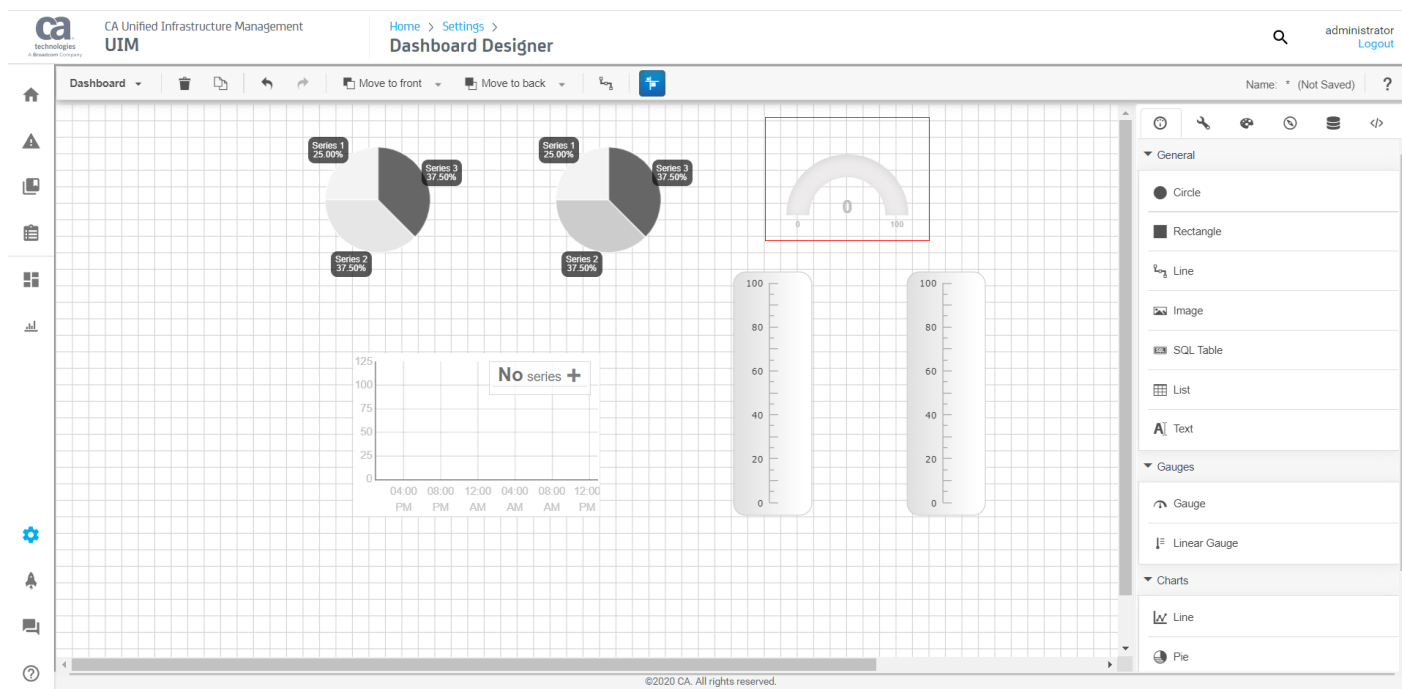
You can now monitor the administrative activities that are performed in UIM through the Operator Console or related APIs. These activities include creating, updating, or deleting device groups and policies. The information that is related to these activities (for example, actions performed, date, time, and change details) is captured for the auditing purposes.

For more information, see [Auditing in UIM Interfaces](#).

Custom Dashboard Enhancements

The dashboard designer includes the following enhancements:

- Allow users to select targets in the list views.
- View the dashboard entry.
- Use the **Edit Column** option to modify the record information.
- Export the table and list grids in the CSV format.



For more information, see [Add a Dashboard Widget](#).

- The following unused legacy ACL permissions are removed from the dashboard designer:
 - Dashboard Design
 - Dashboard Download
 - Dashboard Publish
 - Dashboard Upload

For more information, see [ACL Permissions List](#).

White Labeling in Operator Console

This release provides a new login screen in the Operator Console along with the white labeling functionality. This functionality lets you customize the Operator Console screens, including the login pages. UIM allows user-specific branding and logo on the Operator Console. The customization includes updating the product title, product logo, and footer text for all the UI screens of the Operator Console. You can also add organization-specific text and hyperlinks on the login screen.

For more information, see [White Labeling in Operator Console](#).

UIM API Enhancements

UIM 20.3.0 comes with an enriched UIM API catalog. The enhancements are included in the following APIs:

- Alarm policy APIs
- Import or export profile APIs
- Bulk profile import or export APIs
- Maintenance mode APIs

These APIs provide more capabilities to perform multiple operations; for example, alarm policy-related operations and import (or export) profiles. The information in the error messages is also updated to provide more comprehensive content. Additionally, the changes that are related to request, response, parameters, and content types are available in a user-friendly Swagger documentation.

For more information, see [UIM APIs](#) in the probes documentation.

Export and Import Alarm Policies

With UIM 20.3.0, you can export and import the alarm policies using the enhanced policy management API.

For more information, see [Export/Import Alarm Policies](#).

Bulk Profile Import

In this release, the bulk profile import supports import of one or more profiles from multiple groups to multiple groups.

For more information, see [Bulk Profile import functionality](#).

Alarm Policy Management in High Availability (HA) Mode

UIM 20.3.0 provides the alarm policy management in the High Availability (HA) mode. This functionality lets you configure the `policy_management_ws` probe to process the policies on only one node when the probe is deployed on multiple wasp nodes. If the policy-processing wasp node goes down, another node starts processing the policies automatically. This configuration can also be done manually.

For more information, see [Policy Management in High Availability Mode](#).

New APIs Added in Monitoring Configuration Service (MCS)

UIM 20.3.0 adds new REST APIs in Monitoring Configuration Service (MCS). These APIs provide more capabilities to the users for performing operations at the device and group levels.

For more information, see [Rest API](#) in the probes documentation.

Addressing the ACL Permission Vulnerability

This release of UIM addresses the ACL permission-related vulnerability for the UIM/robot installation path. In previous releases, the UIM/robot installation path was inheriting the ACLs from its parent folder. If the parent folder had weak ACLs, it was making the installation vulnerable to attacks. Now, with an enhanced security mechanism, this vulnerability is no longer applicable.

To resolve this issue, the `robot.cfg` file includes the following configuration parameters:

- `reset_folder_acls`: This parameter resets the folder ACLs. If the value is set to `yes`, the controller resets the ACLs of the Nimsoft installation folder (including its subfolders and files) during the startup. After the completion of this operation, the value of the parameter changes to `no`. The default value is `yes`. If you do not provide any value, the value is considered as `yes`.
- `copy_acls_from_programfiles`: This parameter lets you specify whether you want to copy the same ACLs that are applied to the system folder: Program Files (x86) or Program Files. If the value is set to `yes`, the controller takes the ACLs from the Program Files (x86) or Program Files folder. If the value is `no`, then a standard set of ACLs (with write access only to Administrators and SYSTEM) are applied, irrespective of whether it is a standard install path or a non-standard path. The Administrators and SYSTEM group will have full control. The Users group will have read and execute access. The default value is `yes`.

The standard path examples are Program Files (x86) and Program Files. The non-standard path examples are `C:\` and `C:\My Path`.

Addressing Admin Console and Operator Console Vulnerabilities

This release of UIM addresses vulnerabilities in Admin Console and Operator Console. Outdated UI libraries in Admin Console have been upgraded to fix the vulnerabilities. Many outdated third-party libraries have also been upgraded to fix the Operator Console vulnerabilities. This release also addresses the security vulnerabilities in the Operator Console. Some of the major vulnerabilities that are fixed in this release are as follows:

- 3.1.2 RED-14-007635-002: Information disclosure through detailed error messages
- 3.1.3 RED-14-007635-003: Insecure Content Security Policy configuration
- 3.1.4 RED-14-007635-004: Version information disclosure

Probes and Packages

To review the list of the probes and packages that are installed as part of the 20.3.0 deployment, see [Probes and Packages](#).

Resolved Issues

For a complete list of issues that have been resolved in this release, see [Resolved Issues](#).

Known Issues

To view the list of known issues that are applicable for this release, see [Known Issues](#).

Third-Party Software Agreements

To review the list of third-party software agreements (TPSRs) that are applicable for this release, see [Third-Party Software Agreements](#).

UIM 20.3.0 Installation Considerations

To help you quickly get started with UIM 20.3.0, review the following considerations. The UIM 20.3.0 release supports both fresh and upgrade installations.

- With fresh installation, it supports only non-secure installation.
- With upgrade installation, it supports both secure and non-secure installations.

The following are a few supported upgrade scenarios:

- For upgrade from UIM Server 20.1.0 to UIM Server 20.3.0
 - If 20.1.0 is a non-secure environment, you can upgrade to 20.3.0 secure or non-secure environment.
- For upgrade from UIM Server 9.2.0 to UIM Server 20.3.0
 - If 9.2.0 is a secure environment, you can upgrade only to 20.3 secure environment.
 - If 9.2.0 is a non-secure environment, you can upgrade to 20.3.0 secure or non-secure environment.

If you do not want to upgrade to the secure version of the packages currently, you can delete them from your archive. This deletion helps you avoid situations where you inadvertently use the secure version instead of the non-secure one. If you need the secure versions at a later stage, you can recover them from the uimserverpackages.zip file that is downloaded as part of the 20.3.0 package.

Release Comparison

This table compares the key features in various UIM releases:

| Key Features | UIM 20.3.3 | UIM 20.3.1 | UIM 20.3.0 | UIM 20.1.0 | CA UIM 9.2.0 | CA UIM 9.0.2 |
|--|------------|------------|------------|------------|--------------|--------------|
| Metrics Palette Enhancements | yes | no | no | no | no | no |
| Removing CABI Dependency (Native Operator Console) | yes | no | no | no | no | no |
| Availability of Report Scheduler | yes | no | no | no | no | no |

| | | | | | | |
|---|-----|-----|-----|-----|----|----|
| Packages Signed with GPG-Enabled Keys | yes | no | no | no | no | no |
| Secure Transmission of Certificates | yes | no | no | no | no | no |
| Ability to Change the Password | yes | no | no | no | no | no |
| Alarm Console Enhancements | yes | no | no | no | no | no |
| Creating New Custom Dashboards Views | yes | no | no | no | no | no |
| Group Management Enhancements | yes | no | no | no | no | no |
| Access Admin Console in OC | yes | yes | no | no | no | no |
| Service Level Management | yes | yes | no | no | no | no |
| Copy MCS Profiles | yes | yes | no | no | no | no |
| Delete a Device Using OC | yes | yes | no | no | no | no |
| Enable Read-Only Access for Profiles | yes | yes | no | no | no | no |
| Alarm Policy Enhancement | yes | yes | no | no | no | no |
| Enhanced Telemetry for the PLA Model | yes | yes | no | no | no | no |
| White Labeling in Operator Console | yes | yes | yes | no | no | no |
| Auditing in UIM Interfaces | yes | yes | yes | no | no | no |
| Policy Management in High Availability Mode | yes | yes | yes | no | no | no |
| Export/Import Alarm Policies | yes | yes | yes | no | no | no |
| Bulk Profile import functionality | yes | yes | yes | no | no | no |
| MCS Dashboards | yes | yes | yes | yes | no | no |
| Hub LDAP Client Authentication | yes | yes | yes | yes | no | no |

| | | | | | | |
|--|-----|-----|-----|-----|-----|-----|
| Secure Hub and Robot | yes | yes | yes | yes | yes | no |
| Telemetry Configuration for the PLA Model | yes | yes | yes | yes | yes | no |
| Enable Enhanced Multitenancy | yes | yes | yes | yes | yes | yes |
| RESTful API Monitoring | yes | yes | yes | yes | yes | yes |
| Webhook Integration Through messagegw Probe | yes | yes | yes | yes | yes | yes |
| Operator Console | yes | yes | yes | yes | yes | yes |
| IPv6 Support | yes | yes | yes | yes | yes | yes |
| TLS v1.2 Support (Oracle and Microsoft SQL Server) | yes | yes | yes | yes | yes | yes |
| Application Discovery | yes | yes | yes | yes | yes | yes |
| Inventory Device Deletion | yes | yes | yes | yes | yes | yes |
| Log Analytics | yes | yes | yes | yes | yes | yes |
| Telemetry | yes | yes | yes | yes | yes | yes |
| CA Business Intelligence Summary Dashboards | yes | yes | yes | yes | yes | yes |
| System Edge Integration | yes | yes | yes | yes | yes | yes |
| Improved Admin Console | yes | yes | yes | yes | yes | yes |
| CA Spectrum Bidirectional Integration | yes | yes | yes | yes | yes | yes |
| CA Business Intelligence in CA UIM | yes | yes | yes | yes | yes | yes |
| CA Application Delivery Analysis Integration | yes | yes | yes | yes | yes | yes |
| Monitoring Configuration Service | yes | yes | yes | yes | yes | yes |

Probes and Packages

This article provides information about how you can view the probes and packages that are installed as part of the 20.3.0 release.

Probes

You can locate the version number for individual probes in Admin Console. For documentation on the use of Admin Console, see [Using Admin Console](#). For documentation on probes, see the [Probes Documentation Space](#).

NOTE

The correct version number for the trellis probe is located on the **Installed Packages** tab. The version number for trellis that appears on the **Probes** tab displays the version number of the latest installed service.

| Component | Version Number |
|-----------------------------|----------------|
| ace | 20.30 |
| automated_deployment_engine | 20.30 |
| baseline_engine | 20.10 |
| cdm | 6.50 |
| cm_data_import | 20.30 |
| controller | 9.31 |
| data_engine | 20.30 |
| discovery_agent | 20.30 |
| discovery_server | 20.30 |
| distsrv | 9.31 |
| ems | 10.24 |
| hub | 9.31 |
| maintenance_mode | 20.30 |
| mon_config_service | 20.30 |
| mpse | 20.10 |
| nas | 9.31 |
| net_connect | 3.37 |
| nis_server | 20.30 |
| ppm | 20.10 |
| prediction_engine | 20.10 |
| qos_processor | 20.10 |
| rsp | 5.35 |
| sla_engine | 20.10 |
| spooler | 9.31 |
| telemetry | 1.24 |
| trellis | 20.30 |
| udm_manager | 20.30 |
| usage_metering | 9.27 |
| wasp | 20.30 |

| | |
|--------|------|
| webgtw | 8.44 |
|--------|------|

Packages

You can see your package versions in Admin Console. For documentation on the use of Admin Console, see [Using Admin Console](#).

| Component | Version Number |
|----------------------|----------------|
| adminconsoleapp | 20.30 |
| app_disco_apache | 7.95 |
| app_disco_iis_server | 7.95 |
| app_disco_mysql | 7.95 |
| app_disco_oracle | 7.95 |
| app_disco_sqlserver | 7.95 |
| attr_publisher | 9.31 |
| java_jre | 2.05 |
| mcsuiapp_portlet | 1.36 |
| mps | 20.10 |
| nisapi_wasp | 20.10 |
| policy_management_ws | 0.24 |
| pp_defaults | 2.12 |
| robot_aix | 9.31 |
| robot_deb | 9.31 |
| robot_exe | 9.31 |
| robot_hpux | 9.31 |
| robot_update | 9.31 |
| robot_rpm | 9.31 |
| robot_sol | 9.31 |
| robot_update | 9.31 |
| uimhome | 20.30 |
| uimapi | 20.30 |
| ump_accountadmin | 20.30 |
| ump_cabi | 4.21 |
| ump_dashboard | 20.30 |
| ump_operatorconsole | 20.30 |
| ump_selfcert | 20.30 |
| ump_slm | 20.30 |
| vs2017_vcrist_x64 | 1.01 |
| vs2017_vcrist_x86 | 1.01 |
| wasp_alarmviewer_api | 2.12 |
| wasp_service_wrapper | 20.30 |

The following MCS templates are deployed during CA UIM installation. For more information about MCS templates and supported probe version, see probe-specific Release Notes, and MCS Profile Type Configuration articles on the [Probes Documentation Space](#).

| Template Name | Version |
|--------------------------------|---------|
| ad_response_mcs_templates | 1.82 |
| apache_mcs_templates | 1.72 |
| attr_publisher_mcs_templates | 1.07 |
| cdm_mcs_templates | 6.50 |
| exchange_monitor_mcs_templates | 5.33 |
| iis_mcs_templates | 1.92 |
| mysql_mcs_templates | 1.53 |
| net_connect_mcs_templates | 3.42 |
| oracle_mcs_templates | 5.41 |
| rsp_mcs_templates | 5.35 |
| sharepoint_mcs_templates | 1.84 |
| sqlserver_mcs_templates | 5.43 |

Packages for Monitoring SystemEDGE-enabled Devices

cabi-sysedge-report Release Notes

The cabi-sysedge-report is a companion package that supports the SystemEDGE OnDemand Report that you can view in the Device Summary Dashboards, part of the CA Business Intelligence with CA UIM. The SystemEDGE OnDemand Report displays data for SystemEDGE-enabled devices that are monitored with the snmpcollector probe.

| Package Name | Description | State | Date |
|----------------------------|-----------------|-------|------------|
| cabi-sysedge-report | Initial Release | GA | March 2017 |

cabi-sysedge-report Installation Concerns

For more information about how to install the cabi-sysedge-report package, see [Monitor SystemEDGE-enabled Devices with the snmpcollector Probe](#) on the Probes Documentation Space.

cabi-sysedge-datasource Release Notes

The cabi-sysedge-datasource is a companion package that supports the bean data source that you create for use with the SystemEDGE OnDemand Report.

| Package Name | Description | State | Date |
|--------------------------------|-----------------|-------|------------|
| cabi-sysedge-datasource | Initial Release | GA | March 2017 |

cabi-sysedge-datasource Installation Concerns

For more information about to install the cabi-sysedge-datasource package, see [Monitor SystemEDGE-enabled Devices with the snmpcollector Probe](#).

Packages for CA Business Intelligence with CA UIM

The following optional probes are downloaded to the archive during CA UIM installation. For more information about CA Business Intelligence with CA UIM, refer to [CA Business Intelligence Server Release Notes](#).

| Component | Version Number |
|---------------------------------|----------------|
| cabi | 4.30 |
| cabi_external | 4.20 |
| ump_cabi | 4.21 |
| uim_core_dashboards_pack | 2.46 |
| uim_unified_reporter_pack | 1.04 |
| uim_cabi_health_report_pack | 1.31 |
| uim_aws_dashboards_pack | 2.40 |
| uim_azure_dashboards_pack | 2.40 |
| uim_sap_dashboards_pack | 1.00 |
| uim_citrix_dashboards_pack | 1.00 |
| uim_cabi_vmware_dashboards_pack | 1.11 |
| uim_cabi_mcs_dashboards_pack | 1.00 |

Resolved Issues

The following are the resolved issues in 20.3.0:

controller

- (9.20 HF12) Fixed an issue related to a problem closing e2e_appmon.rob on Windows 10 PCs. (Support Case: 20037327)
- (9.20 HF13) Fixed an issue related to frequent alarms "Unable to communicate with probe 'processes'. Restarting probe". (Support Case: 31784899)
- (9.20 HF13) Fixed an issue where [PDS] nimalarm do not work with option -c from UIM 9.2.0 on Linux anymore. (Support Case: 20093893)
- (9.20 HF14) Fixed an issue where primary hub is stopping and forcing all robots to switch to their secondary hub. (Support Cases: 20310110, 31888790)
- (9.20 HF14) Fixed an issue where robots without discovery_agent probe is being added into CM_DISCOVERY_AGENT. (Support Cases: 20122758, 20197812)
- (9.20 HF15) Fixed an issue where remote profiles were not getting deployed by MCS. (Support Case: 31819927)
- (9.20 HF17) Fixed an issue where robot does not execute all application discovery scripts. (Support Case: 32068693)
- (9.20 HF19) Fixed an issue where robot crashes and becomes unresponsive, and is required to manually restart. (Support Case: 32044603)
- (9.30 HF1) Fixed an issue while configuring passive robot on the NAT'ed network. (Support Case 20309641)

data_engine

- (20.10 HF1) Fixed an issue which displays useful message in logs when the error code is thrown. (Support Cases: 20320491)
- (20.10 HF1) Fixed an issue where after updating origin through qos_processor, and data_engine cannot store their metrics. (Support Case: 31722751)

hub

- (7.97 HF9) Fixed a tunnel problem with robot 7.97 HF8 (2). (Support Case: 20325857)
- (7.97 HF9) Fixed an issue where snmpgtw was interfering with hub. (Support Case: 20274225)
- (9.20 HF11) Fixed an issue with LDAP Authentication being failed due to password hardness (characters set). (Support Case: 20302003)
- (9.20 HF11) Fixed an issue with LDAP+SSL authentication while upgrading to UIM 20.1.0. (Support Case: 31829437)
- (9.20 HF16) Fixed an issue where renaming a robot causes hub to send "robot inactive" alarms. (Support Case: 31888942)

maintenance_mode

- (9.20 HF2T1) Fixed an issue where machines in maintenance mode still generate alerts. (Support Cases: 20280426, 31811590)

mon_config_service

- (9.20 HF5) Fixed an issue in which remote profiles are not getting deployed by MCS. (Support Case: 31819927)
- (9.20 HF5) Fixed an issue where the alarm policy entries in "error" status are with version=-1. (Support Case: 31927120)
- (9.20 HF5) Fixed an issue where alarm policies are not getting processed: excessive retry count. (Support Case: 31927103)

nas

- Fixed an issue related to no heartbeat alarms. (Support Case: 31888807)

Operator Console

- (2.0.2 HF3) Fixed an issue where Operator Console does not allow login after update to 9.20. (Support Cases: 31794960, 31882080)
- (2.0.2 HF4) Fixed an issue with the Operator Console groups tab issue. (Support Case: 31882603)
- (2.0.3 HF1) Fixed an issue where Operator Console CABI Summary Page does not Load Correctly: UI issues in groups and cabi dashboards. (Support Case: 31827021)

policy_management_api

- (0.2.2 HF6) Fixed an issue related to the alarm policy for aggregated CPU usage where it is alarming on idle values. (Support Case: 31897635)
- (0.2.2 HF6) Fixed an issue related to the priority change for alarm policies (earlier Regex). (Support Case: 31869330)

spooler

- (9.20 HF10) Fixed an issue where alarms from cdm probe are not being cleared - cdm MCS Enhanced Profile. (Support Case: 20141321)
- (9.20 HF10) Fixed an issue where alarm policies are not clearing alarms (Support Cases: 20104451, 20229009)
- (9.20 HF14) Fixed an issue where ToT alarms from MCS Enhanced profiles are randomly clearing and re-appearing. (Support Case: 20144688)
- (9.20 HF18) Fixed an issue where spooler is not honouring the policy precedence. (Support Case: 31905846)

Known Issues

The following known issues are applicable for UIM:

Application is Vulnerable to Insecure Communication Vulnerability

Symptom:

User-specific sensitive authentication data is transmitted in clear text, which can be sniffed by an attacker to compromise users identity and obtain unauthorized access to the application.

Solution:

Use SSL on any authenticated connection or whenever sensitive data is being transmitted. Use SSL for all connections that are authenticated or transmitting sensitive or value data, such as credentials, credit card details, health, and other private information. Ensure that communications between infrastructure elements, such as between web servers and database systems, are appropriately protected via the use of transport layer security or protocol level encryption for credential's and intrinsic data.

CABI Installation Fails When Using Special Characters in Operator Console (OC) and LDAP Account Names

When you use special characters (\, |, [,], ` , " , ' , ~ , ! , # , \$, % , ^ , & , [,] , * , + , = , ; , * : , ? , < , > , } , { ,) , (,) , [, / , @) in the Operator Console (OC) or LDAP account names, account synchronization with CABI fails which results in a failed installation.

Cannot Collect Non-Default QoS Metrics When Using Enhanced Templates

Symptom:

When using the enhanced templates, the probe configuration file is not updated with the QoS metric information.

Solution:

The QoS collection for default metrics works as expected for legacy templates. However, for enhanced templates, the probe configuration file is not updated as there is no mapping in the template for the non-default QoS collection.

CDM Probe Setting Might Impact the Performance of discovery_server When Monitored Devices Are Using a Shared File System

Symptom:

By default, the CDM Probe configuration has the Setup/allow_remote_disk_info set to Yes. This allows the CDM Probe to generate the Device ID for all shared drives on a monitored device using a shared file system. In this situation, cdm creates duplicate perspectives for the same shared file system. This can impact the performance of the discovery_server.

Solution:

To correct this issue, use Raw Configure to change the cdm Setup/allow_remote_disk_info set to No. Review the UIM database and remove duplicate perspectives. This should return the performance of the discovery_server to a normal operating level.

Deploying Probes on Dual Stack Mode (IPv4 and IPv6) Not Supported

Symptom:

When you run the Nimsoft Loader (nimldr) utility and configure the primary hub using IPv6 address and are running the dual stack mode, then one of the following occurs:

- When an IPv4 address is given for the Primary Hub, then the installation fails.
- When an IPv6 address is given for the Primary Hub, then the Robot is installed, however you cannot deploy or configure any probe on the Robot.

Solution:

Dual-stack mode does not work as the primary hub of the UIM environment is in the dual-stack IPv6 and the IP address that is used in the robot.cfg is dual-stack IPv4.

Dashboard Design Permission Requires Bus User Privileges

In the Account Admin, you can add the Dashboard Design permission to an ACL for an account contact user if the user wishes to create custom dashboards. However, the permission functions only for a bus user. Dashboard Design permission that is applied to an account contact user is ignored.

Exchange Monitor Setup Template Localization Issue

In CA UIM 9.0.2, the default profile name is not localized in the Exchange Monitor Setup MCS template.

Friendly Name with Special Characters Fails to Deploy the Schema

Symptom:

When you deploy a schema that has characters that are not valid in file names, the schema fails to deploy with the following error: Error occurred while creating/deploying schema probe package, Failed to deploy the probe package for the schema, <friendly_name> ScaleIO97db5264cdf49dbadf1de5928b0d9c98 :: <friendly_name>_schema.json."

Solution:

Define the friendly names with the characters that are valid in filenames.

Isilon Schema fails to Upload

Symptom:

Upload Isilon Schema fails with this error "There was a problem while importing. Please contact administrator." press OK to Continue

Solution:

This error typically occurs if the schema size is more than 1 MB. You can upload the Isilon schema with 1 MB as the maximum file size.

Interface Groups Not Supported with Mobile App

Currently, the application does not support interface groups with either Android or iOS devices.

Installation Fails on RHEL 7.4

Symptom:

UIM installation fails on RHEL 7.4 machines.

Solution:

If you are using RHEL 7.4, ensure that either the fonts local.conf file is configured or the dejavu-serif-fonts package is installed. For more information, see the [RHEL Documentation](#).

Option 1: The fonts local.conf file is configured. Create the /etc/fonts/local.conf file with the following contents:

```
<?xml version='1.0'?>
<!DOCTYPE fontconfig SYSTEM 'fonts.dtd'>
<fontconfig>
<alias>
<family>serif</family>
<prefer><family>Utopia</family></prefer>
</alias>

<alias>
<family>sans-serif</family>
<prefer><family>Utopia</family></prefer>
</alias>
```

```
<alias>
<family>monospace</family>
<prefer><family>Utopia</family></prefer>
</alias>
```

```
<alias>
<family>dialog</family>
<prefer><family>Utopia</family></prefer>
</alias>
```

```
<alias>
<family>dialoginput</family>
<prefer><family>Utopia</family></prefer>
</alias>
</fontconfig>
```

Option 2: Run the yum install command to install the dejavu-serif-fonts package.

```
yum install dejavu-serif-fonts
```

Java-Based Probes Might Not Start on Secondary Robot Deployment

CA Unified Infrastructure Manager v8.51 and later are installed with Java 8. When upgrading to CA UIM v8.51 or later, if Java-based probes that are previously deployed to a robot use an older version of Java (for instance, Java 7), the probes might not start. To resolve this, redeploy java_jre version 1.7 to the robot and then restart the robot.

Java SDK Environment Variable Requirement

If you use the Java SDK to send messages to UIM, set the following environment variable to designate the loopback IP address for contacting the local robot. For example:

```
NIM_ROBOT_IP=127.0.0.1
```

JSON Schema Validation Fails

Symptom:Subsystems

Upload a JSON schema and the validation fails resulting in the following error:

[<schema_name>.json] is/are missing UIM metric definitions syntax.

Solution:

This error typically occurs when the UIM **metrics** definition section is missing from the JSON file or contains incorrect values in the *operator* and *severity* attributes.

To resolve the error, edit the schema file, and perform either of the actions:

- In the **metrics** section of the schema, define only one value for the following attributes: *operator* and *severity*. These attributes do not support an array of values.
Or
- Remove the following attributes from the **metrics** section in the schema: *thresholdenabled*; *operator*; *severity*; *custom_message*; *custom_clear_message*

Manually Copy Security Certificates on the CABI External (Secondary Robot)

Before you deploy CABI External version and enable TLS v1.2 you need to manually copy the security certificates from the primary robot to the secondary robot.

When you are using Microsoft SQL Server as the database, you need to manually copy the trust store files (jks) from the primary robot to the secondary robot. The files are placed in the <Nimsoft>\security folder.

When you are using Oracle as the database, you need to manually copy the wallet files (SSO/PKCS12) from the primary robot to the secondary robot. The files are placed in the <Nimsoft>\security folder.

MCS Configuration Profiles Might Not Be Applied to All Members of Large Dynamic Groups

Dynamic groups are updated by default every 5 minutes. In large CA UIM environments, dynamic groups could have a thousand members or more. It is unlikely that Monitoring Configuration Service will be able to deploy or update configuration profiles to all members of a large dynamic group within the 5-minute interval. To resolve the issue, you can increase the configured interval. The interval is set with the `group_maintenance_interval` on `nis_server`. For details about modifying the `group_maintenance_interval` on `nis_server`, see the *Configure the Update Interval for Automatic Groups* section in the [Create and Manage Groups](#) article.

MCS MySQL, Oracle, or SQL Server Device-level Configuration Profile Overrides Might Not Be Marked with an Asterisk

Using Monitoring Configuration Service, you can create group-level MySQL, Oracle, or SQL Server configuration profiles. After MCS applies the group configuration profile to all members of a group, you can make device-level overrides. MCS marks each field with a device-level override on the device configuration profile with an asterisk. Under the following conditions, you might not see an asterisk on some of the device-level *alarm* fields that have overrides:

- The group-level profile for a checkpoint was set to publish *None* or *QoS*, and then
- The device-level override for the same checkpoint is set to *Alarm* or *QoS and Alarms*

mon_config_service Does Not Activate after Restart

Symptom:

When I restart the `mon_config_service` probe from Admin Console/ IM, the probe remains deactivated.

Solution:

If the `mon_config_service` probe remains deactivated after restarting, navigate to the Admin Console/ IM and select > Activate.

mon_config_service.log File Rotation Not Working Properly

Both `log4j` and `NimLog` are currently writing to the `mon_config_service.log` and this prevents the log file entries from rolling properly. To correct this issue, you need to modify the `log4j.properties` file and add an appropriate file size for the `mon_config_service.log` file. The workaround to correct this issue is:

1. In Remote Desktop, open the `log4j.properties` file that is at `<uim>\Nimsoft\probes\service\mon_config_service` in a text editor.
2. Remove `FILE` from the `'log4j.rootCategory=ERROR, FILE, CONSOLE'` statement on the first line of the file. The statement becomes `'log4j.rootCategory=ERROR, CONSOLE'`.
3. Save the file.
4. Specify an appropriate file size for the `mon_config_service.log` file. The default file size is 1024 KB.
 - a. Access Admin Console.
 - b. Select the hub on the **Robots** tab, and then select the **Probes** tab.
 - c. Select the inline menu button for the `mon_config_service.log` file, and select **Raw Configure**.

- d. Select the **Setup** section.
- e. Select '+' in the top right corner to create a key.
- f. Enter **logsize** in the Key field.
- g. In the Value field, enter an appropriate file size in kilobytes for the mon_config_service.log file.
- h. Select **Create** to add the log size key value.
- i. Select Update to save your changes.

Monitoring Configuration Service Profile Type Field Names

While MCS profile types and the associated probe configuration GUIs (either in Admin Console or Infrastructure Manager) for a particular probe will have the same configuration options, individual field names might not always match between them. For more information about the available fields for each probe GUI, see the documentation for each probe on the [Probes site](#).

Monitors Not Deleting Even After Removing the Last Child Template (Override) for a Device

Symptom:

Create a group and add a device to this group. Also, ensure that no other override template is defined for the device. Then, override a template in this group and verify that the override template applies (monitors are published). Now, delete the override template. Even after deleting the override template, monitors created from the template for the device do not delete.

Solution:

When all the child template profiles that are associated with a device are removed, the device entry is deleted from the probe configuration file. The probe processes for all the devices that are found in the configuration file. Therefore, any device that was found earlier and now not present in the file is not processed. That is, monitors created earlier are not dropped.

In the current implementation, no way is available to manage the devices that are removed from the configuration file. As a workaround, restart the probe whenever this scenario occurs.

Name Resolution Conflicts on Debian Systems with the automated_deployment_engine Probe

By default Debian v6 uses the address 127.0.1.1 as the name resolution address. When a robot is deployed to a Debian 7 or 8 system using automated_deployment_engine, after system restart, the robot attempts to bind to 127.0.1.1 as the available address. Use the following work-around to avoid contention for 127.0.1.1 on your Debian system:

- When installing the robot manually or with automated_deployment_engine, you must go to the target system after installation and must add the following line to the robot.cfg file:

```
robotip = ip_address
```

where **ip_address** is the desired IP address that the robot should bind to on the target system.

- When deploying to Debian 6.0.5 using XML, you must define the **<robotip>ip_address</robotip>** option, where **ip_address** is the IP address that the robot should bind to on the target system.

Oracle Instant Client 12.2 Not Working

Symptom:

CA UIM 9.0.2 does not work with Oracle Instant Client 12.2.

Solution:

As a workaround, use Oracle Instant Client 12.1.

Probe Administration Returns an Unknown Error in a Windows Cluster Environment

When you attempt to configure a probe, probe administration might return an *unknown error* message in a Windows Cluster environment. Specifically, this problem has occurred with the ems probe, but can happen with other probes. To work around the issue, follow these steps:

1. Log in to Infrastructure Manager as the administrator.
2. On the Security tab, select **Probe Administration**.
3. Select **New Probe** to add an entry for the ems probe.
 - a. Select ems in the **Probe** drop-down list.
 - b. Select Admin in the **Access** drop-down list.
 - c. Enter an asterisk (*) in the **IP Mask** field, and select **OK** to save your changes.

Profile Reconciliation Function Removed From Monitoring Configuration Service

The Reconciliation function was moved from the mon_config_service probe to a new MCS Utilities Tools. The MCS Utilities Tool provides more flexibility to schedule reconciliation, more in-depth reports of detected differences, and increases the performance of the mon_config_service probe. To fix differences in configuration profiles that are managed by Monitoring Configuration Service, use the [MCS Utilities Tool](#).

Probes Stop Working after Renaming the Robot Name and Restarting the Robot

Symptom:

The probes do not work after the robot name is changed and restarted.

Solution:

You must validate the probes after renaming the robot name. Validation can be done through the Infrastructure Manager interface.

Robot Installation Fails on UNIX

Symptom:

UNIX robot installation fails or the robot fails to start right after installation.

Solution:

Robot installations from Operator Console (OC) work as expected. However, this occurs with the silent installation using the Nimsoft Loader (nimldr) utility. If you see the following error message, then reattempt the installation a second time.

```
./niminit stop Failed to stop nimbus.service: Unit nimbus.service not loaded.  
./niminit start Failed to start nimbus.service: Unit nimbus.service failed to load: No  
such file or directory.
```

If a robot fails to start, then stop and restart the robot.

Sub-Tenancy is Not Supported by CABI Availability Reports

Symptom:

CABI availability reports currently do not support the sub-tenancy feature. The data of all origins would be visible to the user on the CABI availability reports.

Solution:

There is no workaround available for this issue.

The nas AO (Auto Operator) Command Action Does Not Execute When There Is A Space in the Path (Support Cases 246133, 315782)

A command action cannot be parsed when the path contains spaces. Do not use spaces in the AO command path.

Unable to Migrate Existing Profiles to Enhanced Profiles After Upgrading from UIM 8.5.1 to UIM 9.0.2

Symptom:

After upgrading to UIM 9.0.2 from UIM 8.5.1, I do not see the enhanced profiles on Operator Console (OC) for my existing profiles, even after deploying the MCS package for enhanced profiles.

Solution:

You need to upgrade to the latest (non-enhanced) MCS template package before attempting to migrate the existing profiles to enhanced profiles. For detailed instructions, see *Migrating and Converting Existing profiles* in the [Configuring Alarm Thresholds in MCS](#) page.

Unable to Change "Need Client Authentication" in the data_engine UI

Symptom:

This issue occurs when TLS v1.2 is enabled for Oracle (UIM database) and you try to change the **Need Client Authentication** option. In the data_engine IM interface, when you try to change the **Need Client Authentication** option, the appropriate value for this option is not set in the sqlnet.ora file. The sqlnet.ora file is available in the <Nimsoft>\security folder on the UIM Server computer.

Solution:

As a workaround, you must manually update the value of the SSL_CLIENT_AUTHENTICATION parameter. To do so, follow these steps:

1. On the UIM Server computer, navigate to the <Nimsoft>\security folder.
2. Locate and open the sqlnet.ora file.
3. Update the SSL_CLIENT_AUTHENTICATION parameter in the sqlnet.ora file based on whether the **Need Client Authentication** option is selected or not (in the data_engine IM interface).
For example, if the option is selected in the IM interface, the parameter must be set as follows:
SSL_CLIENT_AUTHENTICATION = TRUE
If the option is not selected, the parameter must be set as follows:
SSL_CLIENT_AUTHENTICATION = FALSE
4. Restart the data_engine probe.

Unable to Uninstall the Secondary Robot on an IPv6 Environment

Symptom:

On a pure IPv6 environment; if you try to remove the secondary robot from the hub, the **Ok** button is disabled after entering the IP address of the secondary robot.

Solution:

Detach the robot first from the hub and then uninstall it for successful removal of the secondary robot.

Unable to Create cdm Non-Enhanced Profile (Legacy)

Symptom:

When I try to create the cdm non-enhanced profile (legacy profile), I am unable to create it.

Solution:

The cdm non-enhanced (legacy) template requires cdm 6.30-MC to be present in the Local Archive. By default, cdm 6.30-MC is not present in the Local Archive. Therefore, if you want to create a cdm legacy template profile, ensure that cdm 6.30-MC is available in the Local Archive.

Unable to Open Probe Configuration Using Admin Console

Symptom:

The Configuration window does not open when you select the Configuration option for any probe in the Admin Console.

Solution:

This issue occurs when popups are blocked on your browser. Ensure that popup is not blocked for the Admin Console and select the Configuration option.

Upgrade Self-signed Certificates

The Java version was updated to Java 8. You must upgrade any self-signed certificates that are generated by CA UIM from previous CA UIM versions. If you do not upgrade the pre-existing certificates, HTTPS connections to CABI Server will not work due to the change in security encryption levels in Java 1.8. For more information, see [Configure HTTPS in Admin Console or Operator Console \(OC\)](#).

Using Variables for a Profile Name is Supported (Salesforce Case 418533)

The Monitoring Configuration Service now allows users to enter variable (for example, {device.ip} or {device.name}) for a Profile Name.

(For 9.0.2 or Later) Finding and Fixing Profile Differences using mon_config_service_cli

The following process to find and fix profile differences will not be applicable:

1. Issue the Find-Profile-Diffs command to find robots with configuration profile differences.
2. Issue the Fix-Profile-Diffs command to fix profile differences.
3. Re-issue the Find-Profile-Diffs command with a file that lists the robots that had profile differences to verify that profile differences no longer exist.

Wasp does not extract the webapps

Symptom:

wasp does not extract the webapps and the entries like below are found in the wasp.log:

```
Feb 24 17:18:41:028 INFO [Catalina-utility-1, org.apache.catalina.core.ContainerBase.[wasp-engine].
[localhost].[/]] No Spring WebApplicationInitializer types detected on classpath Feb 24 17:18:44:050
ERROR [Catalina-utility-1, org.apache.catalina.core.ContainerBase] startInternal() A child container failed
during start Feb 24 17:18:44:051 ERROR [Catalina-utility-1, org.apache.catalina.core.ContainerBase]
java.util.concurrent.ExecutionException: org.apache.catalina.LifecycleException: Failed
to start component [org.apache.catalina.webresources.StandardRoot@173e0d4f] at
java.util.concurrent.FutureTask.report(FutureTask.java:122) at java.util.concurrent.FutureTask.get(FutureTask.java:192)
at org.apache.catalina.core.ContainerBase.startInternal(ContainerBase.java:916)
at org.apache.catalina.core.StandardHost.startInternal(StandardHost.java:841) at
org.apache.catalina.util.LifecycleBase.start(LifecycleBase.java:183) at org.apache.catalina.core.ContainerBase
$StartChild.call(ContainerBase.java:1384) at org.apache.catalina.core.ContainerBase
$StartChild.call(ContainerBase.java:1374)
```

Solution:

1. Open registry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NimbusWatcherService` . In the key "ImagePath" change the value to path (same case) as it appears in Windows Explorer. (for.e.g. "C:\Program Files\Nimsoft\bin\nimbus.exe").
2. Restart the "Nimsoft Robot Watcher" service.

Origin update in hub probe and override origin set by the hub in controller probe functionality is not working properly

When the Origin is updated on the hub or the controller, Origin name is not updating on alarms until we clear the alarms manually or restarting robot manually.

In the NAS, key is created including origin, which is then compared with existing key to update the database on which new entry or required fields are updated. If origin is updated, then for every incoming suppressed alarm, to avoid the issues in the alarm clear, new entry is created.

Edit and Delete Options Not Working Properly in the Reports Schedule Menu

Symptom: When I try to schedule CABI reports in the OC UI, the Edit and Delete options are not working properly in the Schedule menu.

Solution: The workaround is to use Schedules within CABI with the "overrides_custom.css" file applied as described in the [KB Article](#).

[UIM 20.3.0] Device view columns are missing in Group and Inventory views of the Operator Console

In the new Operator Console, device view columns are missing at Group and Inventory views that are present in the UMP 20.1.

Group Device Columns: Alias, Caption, Description, OS Type, OS Version, OS Description, Origin, MAC Address, User Tag 1, User Tag 2, Removed, Bus Type.

Inventory Device Columns: Alias, Changed, Origin, Discovery Credentials.

[UIM 20.3.0] Interface group is not redirecting to device level in the Group view on the Operator Console

Interface group is not redirecting to device level at the Group view in the Operator Console. It is redirecting to group list view when clicking the interface group view.

[UIM 20.3.0] Select all checkbox in the Alarms table is not working properly

Symptom: Select all checkbox in the Alarms table is not working properly in the Operator Console. All the alarms are not getting cleared and only alarms that are visible in the page are cleared using the Select all option. Also when the alarms are cleared, if you select the existing alarms again and the select all checkbox is not selecting any alarms.

Solution: For the Select all feature to work properly, you must go to another page and come back to the alarm page.

[UIM 20.3.0] Generated PDFs for the Dashboards are not showing graphs for charts

In the Operator Console, generated PDFs for the dashboards are not showing graphs for charts. This issue happens for the existing dashboards.

[UIM 20.3.0] MCS Options: "Include Device Not in Group" and "Include Device Without Probe" are not working as expected

The "Include Device Not in Group" and "Include Device Without Probe" options are not returning all available devices with these conditions. In the Group profile settings of the MCS, when these settings are selected, the reference devices that are not in the group and the devices without the probes are not shown.

[UIM 20.3.0] Policy Id is displayed instead of Policy name in the Alarms view of the Operator Console

After creating an alarm policy in the Alarms view of the Operator Console, Policy Id is displayed instead of Policy name.

NOTE

This issue has been fixed as part of the [OC 20.3.2 patch](#) release.

[UIM 20.3.0] Maintenance schedule for Nth day of a month is not working when the user timezone or target schedule timezone and the server timezone are different

In UIM 20.3.0, the maintenance schedule for the Nth day of a month not working, the schedule does not start on the scheduled date and time and remains inactive. This happens when the user time zone or target schedule time zone and the server time zone are different. If the scheduled date and the server date are different due to the time zone difference the maintenance schedule does not start on the scheduled date and time.

NOTE

This issue has been fixed as part of the [UIM 20.3.3](#) release.

[UIM 20.3.0] Wasp is not coming to online state when we upgrade from ump which has Self-cert deployed

In UIM 20.3.0, while upgrading from UMP to OC, wasp does not come to online state if the existing UMP has Self-cert deployed.

NOTE

This issue is applicable only if you are upgrading from a version prior to UIM 20.3.0.

[UIM 20.3.0] In the alarms page, for the alarms that are created as a result of an alarm policy, the link to the policy is not enabled for newly created alarm policies

When the alarms are created as a result of an alarm policy in the alarms page of the Operator Console, the link to the alarm policy is not enabled for newly created alarm policies. After the restart of wasp, the policies are enabled with the links. New alarms that are created as a result of the new alarm policies after the restart will have the same issue.

NOTE

This issue has been fixed as part of the [OC 20.3.2 patch](#) release.

[UIM 20.3.0] No QOS metric for profile 'AD Server Services' in the Ad_server MCS template

In UIM 20.3.0, there is no QOS metric for profile 'AD Server Services' in the Ad_server MCS templates.

[UIM 20.3.0] Change Password for Account Users who are added manually in Account Admin is not available

In UIM 20.3.0, for any new users who are added manually in Account Admin, change password option is not available. Users cannot change the password using the Operator Console.

NOTE

This issue has been fixed in the [UIM 20.3.3](#) release.

[UIM 20.3.0] Alarm Policy search filters does not give accurate results

In UIM 20.3.0, the alarm policy search filters results give inaccurate results. The search results are shown for the partial search string when there are more than two letters in the search. The search results also take long to provide the alarm policies in the results.

[UIM 20.3.0] Operator Console does not timeout

In UIM 20.3.0, Operator Console does not timeout and the session remains active even after the session is idle for 72 hours.

NOTE

This issue has been fixed as part of the [OC 20.3.2 patch release](#).

Additional Known Issues**NOTE**

- For the new known issues in the UIM 20.3.1 release, see the Known Issues section in the [UIM 20.3.1](#) article.
- For the new known issues in the OC 20.3.2 release, see the Known Issues section in the [OC 20.3.2 Patch](#) article.
- For the new known issues in the UIM 20.3.3 release, see the Known Issues section in the [UIM 20.3.3](#) article.

International Support

The user interface is available in the following languages:

- Brazilian Portuguese
- Japanese
- Korean
- Simplified Chinese
- Spanish

The user documentation is available in the following languages:

- Brazilian Portuguese
- Japanese
- Spanish

NOTE

Multi-language support on a single CA UIM instance is currently not supported.

Third-Party Software Agreements

CA UIM 20.3.0 uses the following third-party software. To read the required license agreement, review the [zip file](#).

- accessors-smart 1.1
- activation 1.1.1
- adal4j 1.0.0
- adal4j 1.1.2
- Adopt OpenJDK 1.8u232 Hotspot
- AdoptOpenJDK 1.8.0_252 Hotspot
- AdoptOpenJDK 1.8.0_262 Hotspot
- animal-sniffer-annotations 1.14
- ant-contrib 1.0b3
- antlr3 3.5
- ant-nodeps 1.8.1
- aopalliance 1.0
- apache commons csv 1.1
- apache commons csv 1.4
- Apache Commons Daemon 1.0.15
- apache commons dbutils 1.2
- Apache Commons Lang 3.3.2
- Apache Commons Lang 3.5
- Apache JCS 1.3
- Apache Thrift 0.9.0
- Apache Tomcat 9.0.37
- apache tiles 2.1.4
- args4j 2.32
- ASM 1.5.3
- ASM 3.1
- ASM 4.1
- ASM 4.2
- ASM 5.0.3
- ASM 5.1
- aspectjrt 1.8.2
- aspectjrt 1.8.5
- aspectjweaver 1.8.5
- aspectjweaver 1.8.6
- aws cloudtrail processing library 1.1.0
- aws-java-sdk 1.10.50
- aws-java-sdk 1.11.18
- aws-java-sdk 1.11.77
- aws-java-sdk 1.9.39
- axios 0.15.3
- axios 0.19.2
- azure-core 0.9.3
- azure-keyvault 0.9.3
- azure-storage 4.0.0
- backbone.js 1.2.1
- backbone 1.4.0
- backport-util-concurrent 3.1
- batik-css 1.7
- bcprov 1.45
- bcprov 1.53
- BlazeDS 4.7.3
- Boilerpipe 1.1.0
- BoneCP 0.7.1
- BoneCP 0.8.0
- Bonney Castle 1.5.1

CA Business Intelligence JasperReports Server with CA UIM Release Notes

The CA Business Intelligence (CABI) Dashboards within CA UIM use CA Business Intelligence JasperReports Server (CABI Server). CABI Server provides rich reporting and integrates in-memory analysis capabilities. This article explains the new features in this release.

NOTE

- For a matrix of supported CABI package versions, see [CA Business Intelligence with CA UIM](#).
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

Contents

UIM Environment Requirements

The CA Business Intelligence dashboards require the following components

- UIM version 20.3.0. For more information, see the following articles:
 - [Release Notes](#)
 - [Install UIM Server](#)
 - [Install the Operator Console \(OC\)](#)

September 2020

New Features

This release includes the following updates:

In UIM 20.3.0, the bundled CABI provides **Jasper Server version 7.5**; whereas the `cabi_external` is the same as in UIM 20.1.0 (supports **Unified CABI 7.1.1 integration** only).

The versions that are provided with UIM 20.3 are:

1. Bundled CABI (probe name **cabi**)
 - a. **cabi probe** version is 4.30
 - b. Ensure that the following dependencies are deployed:
 - a. **uim_core_dashboards_pack** version 2.46
 - b. **uim_unified_reporter_pack** version 1.04
2. External CABI (probe name **cabi_external**)
 - a. **cabi_external** probe version is 4.20
 - b. Below dependencies need to be deployed:
 - a. **uim_core_dashboards_pack** version 2.45
 - b. **uim_unified_reporter_pack** version 1.03

NOTE

UIM 20.3.0 installer comes with **uim_core_dashboards_pack** version 2.46 and **uim_unified_reporter_pack** version 1.04 which are unsupported for the **cabi_external** probe version 4.20. Follow these steps for the **cabi_external** probe to work:

1. Remove **uim_core_dashboards_pack** version 2.46 and **uim_unified_reporter_pack** version 1.04.
2. Deploy **uim_core_dashboards_pack** version 2.45 and **uim_unified_reporter_pack** version 1.03 from the Archive.

The operating system (OS) and database compatibility where you can install CABI depends on the Jasper Server platform support matrix. Please refer the following for additional details on the Jasper Server platform support:

1. [Jasper Server 7.1.1](#)
2. [Jasper Server 7.5](#)

Bundled CABI supports fresh installation and upgrades. Upgrades are supported from CABI version 3.4 and above, based on the Jasper Server upgrade paths (Jasper Server 7.5 supports direct upgrades from Jasper Server 6.4.3 onwards).

Bundled CABI installation is supported on a different robot as well as on Operator Console system. You can install only one instance of CABI in a UIM domain.

High Availability (HA) of Jasper Server is not supported with the bundled CABI. HA-enabled Jasper Server instances can be pointed by using **cabi_external**.

April 2019

New Features The following updates are in the release:

- The **cabi** probe 4.1.0 is updated to deploy CABI Server version 7.1.1. The probe also supports Microsoft SQL Server 2016.
- Added the Availability Reports which enable you to view availability of devices and groups. For more information, see [Availability Reports](#) in Probes Documentation Space.

New Packages The following new packages are in the release:

- **uim_cabi_availability_report_pack** version 1.00 - Install this package to deploy the Availability reports.
- **cabi** probe package version 4.1.0 - Install this package to deploy an instance of CABI Server on a robot. This configuration simplifies the CABI Server installation process if you only need to use CABI Server with CA UIM. This version of the probe is required to support reports.
- **ump_cabi** portlet version 4.10 - Install this package to view CABI Dashboards in CA UIM 9.0.2.

NOTE

1. The **cabi** 4.10 probe supports TLS v1.2 when communicating with the UIM databases: Microsoft SQL Server - 2012, 2014, 2016 and Oracle - 11.2 and 12.1. Note that UIM 20.1 (and later) do not support Oracle 11.2.
2. The **cabi** 3.40 probe, available with UMP 9.0.2 HF2, supports TLS v1.2 when communicating with the UIM database: Microsoft SQL Server- 2012, 2014, and Oracle - 11.2 and 12.1. For more information about how to apply the UMP 9.0.2 HF2 for CABI TLS functionality, see [UMP 9.0.2 HF2](#). Note that UIM 20.1 (and later) do not support Oracle 11.2.
3. The **cabi** 3.32 probe does not support TLS v1.2 when communicating with the UIM database: Microsoft SQL Server or Oracle. As a result, you cannot view the Operator Console home page, OOTB CABI dashboards, and OOTB CABI reports.
4. TLS v1.2 support is not enabled by default when you install CA UIM 9.0.2.

February 2019

- The CABI TLS v1.2 feature is supported only for [UMP 902 HF2](#) for SQL Server and Oracle databases. The supported SQL Server versions are limited to 2012 and 2014 only.

December 2018

New Features

The following updates are in the release:

- The cabi probe is updated to deploy CABI Server version 6.4.3. The cabi probe now supports Transport Layer Security (TLS) v1.2 when communicating with the UIM database: Oracle or Microsoft SQL Server. This support enables the UIM Server to establish secure communication with the UIM database.
- The cabi_external probe is updated to deploy CABI Server version 6.4.3. The cabi external probe now supports Transport Layer Security (TLS) v1.2 when communicating with the UIM database: Oracle or Microsoft SQL Server. This support enables the UIM Server to establish secure communication with the UIM database.

WARNING

CABI is not supported for TLS v1.2 enabled UIM environments which have SQL Server 2016 and 2017 as the database. Currently, Jaspersoft does not provide support for TLS v1.2 on SQL Server 2016 and 2017. Therefore, if TLS v1.2 is enabled in your CA UIM environment, and your database is SQL Server 2016 or 2017, then CABI Dashboards will not be supported. As a result, you cannot view CABI reports in CA UIM.

New Packages

The following new packages are in the release:

- cabi probe package version 3.40 - Install this package to deploy an instance of CABI Server on a robot. This configuration simplifies the CABI Server installation process if you only need to use CABI Server with CA UIM. This version of the probe is required to support reports.
- cabi_external probe package version 3.40 - Install this package to deploy a probe that functions as a gateway for a separate CABI Server instance. This configuration allows you to share the CABI Server instance with CA UIM and multiple CA Agile Operations products. This version of the probe is required to support reports.
- ump_cabi portlet version 3.40 - Install this package to view CABI Dashboards in CA UIM 9.0.2.

October 2018

New Features

The following updates are in the release:

- When sub-tenancy is enabled for your UIM environment, user origin settings are applied and each sub-tenant has access to its reports (health reports and custom reports) and dashboards (core dashboards) data only. Currently, this sub-tenancy feature is not applicable for the CABI availability reports.

New Packages

The following new packages are in the release:

- cabi probe package version 3.32 - Install this package to deploy an instance of CABI Server on a robot. This configuration simplifies the CABI Server installation process if you only need to use CABI Server with CA UIM. This version of the probe is required to support reports.
- cabi_external probe package version 3.32 - Install this package to deploy a probe that functions as a gateway for a separate CABI Server instance. This configuration allows you to share the CABI Server instance with CA UIM and multiple CA Agile Operations products. This version of the probe is required to support reports.
- ump_cabi portlet version 3.32 - Install this package to view CABI Dashboards in CA UIM 9.0.2.
- uim_cabi_health_report_pack version 1.31 - Install this package to deploy the Health reports.

August 2018

New Packages

The following new packages are in the release:

- `cabi_external` probe package version 3.30 - Install this package to deploy a probe that functions as a gateway for a separate CABI Server instance. This configuration allows you to share the CABI Server instance with CA UIM and multiple CA Agile Operations products. This version of the probe is required to support reports.

April 2018

New Features

The following updates are in the release:

- The `cabi` probe is updated to support the latest wasp 9.0.1 release.
- The CA Business Intelligence Operator Console (OC) portlet is updated to support the version 3.30 release.
- Added new dashboards for monitoring VMware.
- Added new dashboards for monitoring MCS (Monitoring Configuration Service).

New Packages

The following new packages are in the release:

- `cabi` probe package version 3.30 - Install this package to deploy an instance of CABI Server on a robot. This configuration simplifies the CABI Server installation process if you only need to use CABI Server with CA UIM. This version of the probe is required to support reports.
- `ump_cabi` portlet version 3.30 - Install this package to view CABI Dashboards in CA UIM.
- `uim_vmware_dashboards_pack` version 1.00 - Install this package to deploy VMware dashboards. This package requires CA UIM, `uim_core_dashboards_pack.zip` version 2.40, and `vmware` probe version 6.87 or later.
- `uim_mcs_dashboards_pack` version 1.0.0 - Install this package to deploy MCS dashboards. This package requires CA UIM version, `uim_core_dashboards_pack.zip` version 2.40, and at least one MCS profile must exist.

November 2017

New Features

The following updates are in the release:

- ***Changed the deployment process for bundled CABI Server configuration and external CABI Server configuration.*** The significant changes are as follows:
 - There is now a specific probe to use for each configuration. Use the `cabi` probe for the bundled configuration and the `cabi_external` probe for the external configuration.
 - Removed the requirement for MCS.
- The `cabi` probe and `cabi_external` probe packages automatically deploy any package dependencies that exist in the archive. The dependencies include the `uim_core_dashboards_pack` and report packages.
- Added a [library of reports that you can access from dashboards](#).

NOTE

An additional requirement exists for the CA Business Intelligence (CABI) Unified Reporter (UR) reports that utilize data from the vmware probe. The vmware probe must be deployed and configured using MCS. For more information, see [vmware MCS Profile Type Configuration](#).

- Added the ability to view Unified Reporter reports in the CA Business Intelligence dashboards.
- Added legacy dashboard packages to the Archive.
- Added new dashboards for monitoring SAP.
- Added new dashboards for monitoring Citrix.
- Added the ability to migrate custom Unified Reporter reports to the CA Business Intelligence dashboards.
- Added UIM Metric Topic to expand reporting capabilities. The UIM Metric Topic allows you to create Ad Hoc views with data from multiple metrics and devices
- Added the ability to control the frequency of backups for probe and dashboard upgrades. The following keys were added to the cabi and cabi_external probes raw configuration: auto_backup_fequency_in_hours, auto_backup_on_import_enabled, auto_backup_on_import_max_time_in_sec. For more information, see the optional tasks in [Install or Upgrade for a Bundled CA Business Intelligence JasperReports Server](#) or [Install or Upgrade for an External CA Business Intelligence JasperReports Server](#).

New Packages

The following new packages are in the release:

- cabi probe package version 3.20 - Install this package to deploy an instance of CABI Server on a robot. This configuration simplifies the CABI Server installation process if you only need to use CABI Server with CA UIM. This version of the probe is required to support reports.
- cabi_external probe package version 3.20 - Install this package to deploy a probe that functions as a gateway for a separate CABI Server instance. This configuration allows you to share the CABI Server instance with CA UIM and multiple CA Agile Operations products. This version of the probe is required to support reports.
- ump_cabi portlet version 3.20 - Install this package to update the cabi portlet to support version 3.20 of the cabi probe.
- uim_core_dashboards_pack version 2.40 - Install this package to update your dashboards to support version 3.20 of the cabi probe.
- uim_aws_dashboards_pack.zip version 2.40 - Install this package to update the localization support for the AWS dashboards. This package requires uim_core_dashboards_pack.zip version 2.40 and aws probe version 5.25 or later.
- uim_azure_dashboards_pack.zip version 2.40 - Install this package to update the localization support for the Azure dashboards. This package requires uim_core_dashboards_pack.zip version 2.40 and azure probe version 3.02 or later.
- uim_sap_dashboards_pack version 1.00 - Install this package to deploy SAP dashboards. This package requires uim_core_dashboards_pack.zip version 2.40 and sap_basis probe version 2.01 or later.
- uim_citrix_dashboards_pack version 1.00 - Install this package to deploy Citrix dashboards. This package requires uim_core_dashboards_pack.zip version 2.40 and xendesktop probe version 4.20 or later.
- uim_unified_reporter_pack version 1.02 - Install this package to deploy the CABI for CA UIM library reports for applications, DBs (database), networks, and servers.

NOTE

An additional requirement exists for the CA Business Intelligence (CABI) Unified Reporter (UR) reports that utilize data from the vmware probe. The vmware probe must be deployed and configured using MCS. For more information, see [vmware MCS Profile Type Configuration](#).

- uim_cabi_health_report_pack version 1.20 - Install this package to deploy the Health reports.

Fixed Defects

The following known issues have been resolved:

- Version 3.0 dashboards not displaying metric detail data - The metrics details reports now display metric data. (Case 008382, 00847337)

July 2017

New Features

The following updates are in the release:

- The cabi probe was updated to support deployment in either a Bundled mode or an External mode.
 - **Bundled mode**
Bundled mode installs and configures an instance of CA Business Intelligence JasperReports Server (CABI Server) on a robot. This mode simplifies the CABI Server installation process if you only need to use a JasperReports Server (CABI Server) instance with CA UIM.
 - **External mode**
External mode allows a pre-existing CA Business Intelligence JasperReports Server (CABI Server) instance to communicate with CA UIM. This is a CABI Server instance that is not deployed through the cabi probe. This mode reduces the number of CABI Server instances that you must deploy and maintain. You can share a single CA Business Intelligence (CABI) server instance with multiple CA Agile Operations products. For more information, see [Unified Dashboards and Reporting for Infrastructure Management](#).
- The CA Business Intelligence core dashboards were updated to support the version 3.00 release.

New Packages

The following packages were added to the release:

- cabi-mcs-template version 3.00 - Install this package to configure version 3.00 of the cabi probe.
- cabi probe package version 3.00 - Install this package to upgrade to the latest cabi probe version. This version of the probe deploys CABI Server version 6.3 when configured in bundled mode.
- ump_cabi version 3.00 - Install this package to update the cabi portlet to support version 3.00 of the cabi probe.
- uim_core_dashboards_pack.zip version 2.20 - Install this package to update your dashboards to support version 3.00 of the cabi probe.

Known Issues

The following known issues exist:

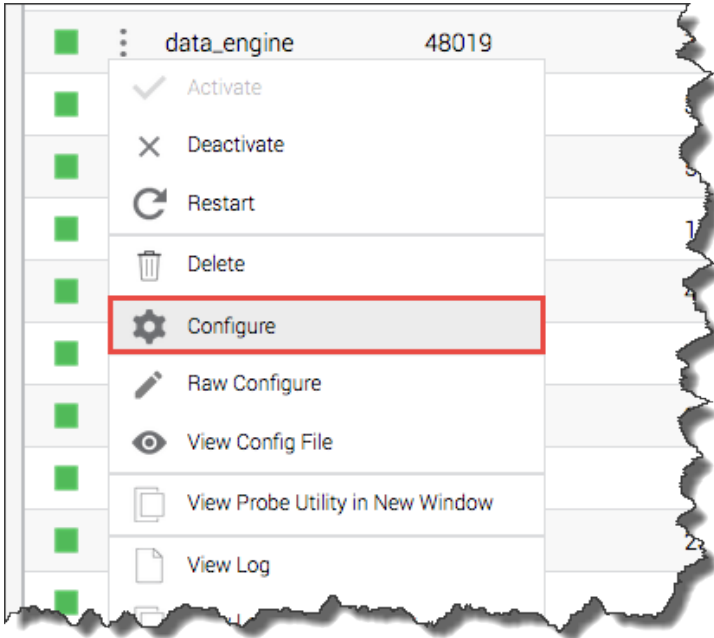
Error 403 (Forbidden) message for CABI dashboards

(Reported version 3.00) To resolve this issue check your cabi probe and ump_cabi package versions. This error occurs when incompatible package versions are installed. For example, your cabi probe is version 3.0 and your ump_cabi version is 2.0. For more information about versions, see [CA Business Intelligence with CA UIM](#). Download and deploy the ump_cabi portlet package to the Operator Console (OC) server and restart wasp on the Operator Console (OC) server.

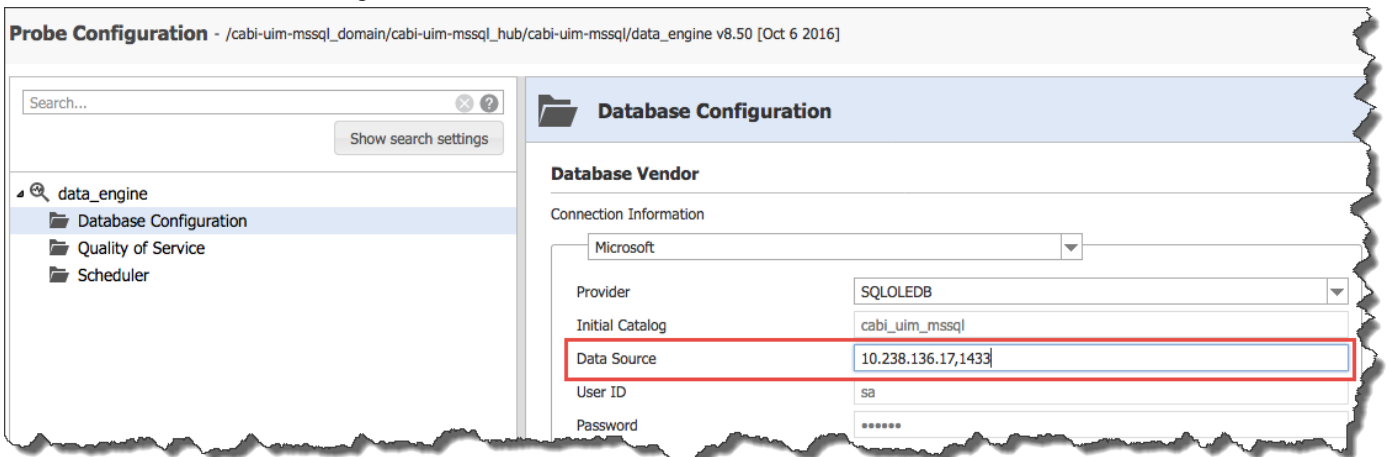
CABI Server installation fails when CA UIM is upgraded from version 8.31 to version 8.5.1, and the CA UIM database is MSSQL.

(Reported version 2.00) To resolve this issue you must restart data_engine.

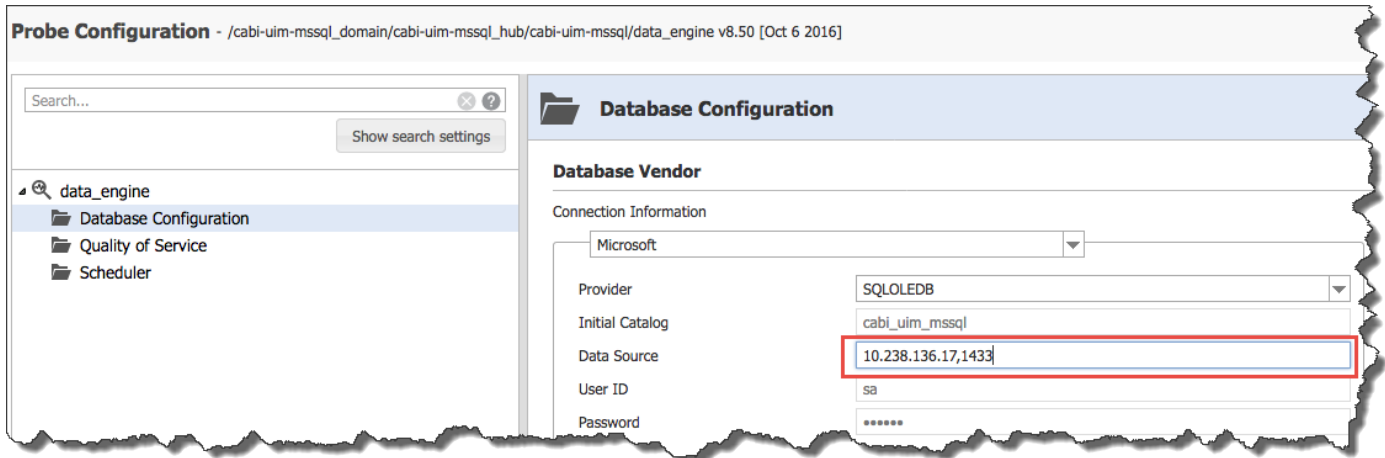
1. Go to the data_engine configuration GUI.



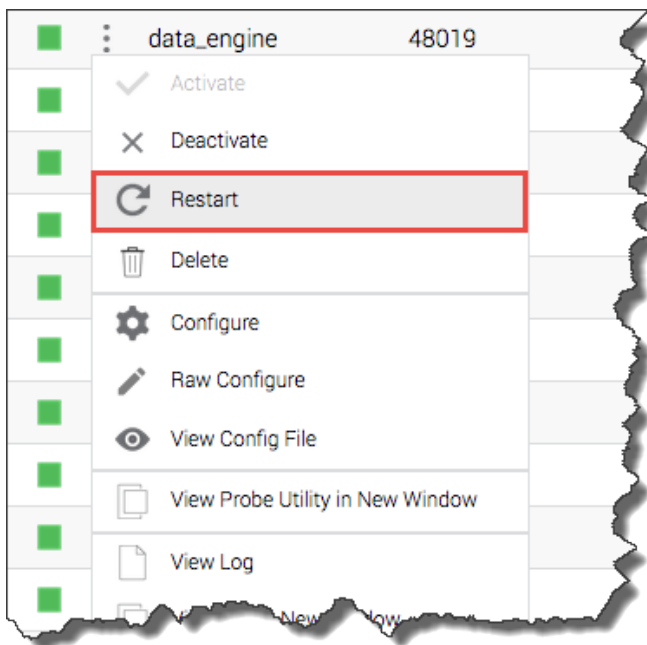
2. Locate the Data Source setting.



3. Reapply the configuration. To activate the Apply button, make a minor change and then revert to the original setting.



4. Restart data_engine.



5. Reinstall CABI Server.

The Java version was updated to Java 1.8 starting with CA UIM 8.5.1.

(Reported version 2.00) You must upgrade any self-signed certificates that are generated by CA UIM from previous CA UIM versions. If you do not upgrade the pre-existing certificates, HTTPS connections to CABI Server will not work due to the change in security encryption levels in Java 1.8.

The AM, PM, and Interval labels do not appear when you export the Open Alarms Details report in a non-English language.

(Reported version 2.00) No work-around exists at this time.

The CABI portlet icons fail to load on an intermittent basis.

(Reported version 1.10) Refresh the page to resolve this issue.

The rendering of some dashboards might be slow in large-scale environments collecting a large amount of QoS data.

(Reported version 1.10) No work-around exists at this time.

CA UIM bus user accounts with special characters (#?~ \$ % ^ & *, (- + ? [{ " | \ / ? < >) are not automatically added to CABI.

(Reported version 1.00) No work-around exists at this time.

CABI Installation Fails When Using Special Characters in Operator Console (OC) and LDAP Account Names

(Reported version 1.00) When you use special characters (\, |, [,], ` , " , ' , ~ , ! , # , \$, % , ^ , & , [,] , * , + , = , ; , : , ? , < , > , } , { ,) , (,) , [, / , @) in the Operator Console (OC) or LDAP account names, account synchronization with CABI fails which results in a failed installation.

Bus users should not share an ACL with LDAP users, or bus users inherit LDAP accounts.

(Reported version 1.00) To avoid this issue, create an ACL to configure for use with LDAP and leave the default ACLs in place. This ACL allows the CA UIM administrator to create Bus users without association to any LDAP account link. For more information, see the Connecting Access Control Lists to LDAP Users section in [Enable Login with LDAP](#).

Data points are offset when you hover over a dashlet in a maximized view.

(Reported version 1.00) This issue is a known Jaspersoft issue.

NOTE**More information:**

- [UIM Release Notes](#)
- [CA Business Intelligence with CA UIM](#)

Product Accessibility Features

CA Technologies is committed to ensuring that all customers, regardless of ability, can successfully use its products and supporting documentation to accomplish vital business tasks.

Getting Started

This section includes information about CA UIM concepts, architecture, components, roles, and other resources. The goal of this section is to help you quickly get started with CA UIM. Review the information in this section before you start with the product. Additionally, the articles in this section help users become familiar with CA UIM processes and tools. After you go through this section, you can then review the more comprehensive content that is available further down in other sections.

For example, if you want to know the steps that can help you get started with CA UIM, follow the instructions in the [New User](#) section. Or, if you want to quickly understand the CA UIM architecture or interfaces, see [CA UIM Architecture Overview](#) or [CA UIM Interfaces](#), as appropriate.

Role-based Documentation

Some of the content in the CA UIM documentation is of interest to a wide range of software development and IT professionals. This section provides you with links to topics that are organized by professional role and common task scenarios. Because the roles in your organization might be different from what is presented here, consider this information as a recommendation to the location of the content that you need.

Evaluator

As an evaluator, you have many options when selecting a network monitoring solution for your organization. CA UIM provides a single, unified platform that allows you to monitor your entire IT environment, both inside and outside the data center. The solution offers the ease-of-use and simplicity that is associated with point IT monitoring tools, featuring a unique powerful architecture with a lightweight footprint. The solution delivers enterprise scalability and multi-tenancy that power some of the most complex infrastructures.

More information:

- [Evaluator](#)

New User

As a new user of CA UIM, we want you to get the most out of your [CA Technologies](#) experience and your investment with us. We are committed to your success. When you adopt a solution from CA Technologies, you gain access to an award-winning team of professionals with the mission to ensure that you see the outcomes and business value that you expected.

Follow the steps in the [New User Quick Start](#), and you will be up and running quickly.

More information:

- [New User](#)

Product Administrator

As a Product Administrator, you have a deep technical knowledge of CA UIM. You are responsible for setting up and managing the product's infrastructure and other software products that your organization uses.

The following table includes your tasks, goals, and challenges.

| Task | Goal | Challenge |
|---|---|--|
| <ul style="list-style-type: none"> • Install and upgrade CA UIM. • Set up and manage robots, hubs, and tunnels infrastructure. • Troubleshoot CA UIM when it does not work as expected. • Stay up to date on new product features. • Create custom probes for Monitoring Administrators. | <ul style="list-style-type: none"> • CA UIM should always be available for monitoring users. • Reduce the time that it takes to install and upgrade CA UIM. • Reduce the time that it takes to resolve product issues. • Reduce the frequency in which product issues occur. • Stay up to date on new product features and training. | <ul style="list-style-type: none"> • Monitoring users can corrupt the product infrastructure configuration. • Troubleshooting tools might not work when the product fails. • Failover might not be supported. • Increasing product complexity. • More bugs mean more issues to fix. |

More information:

- [Product Administrator](#)

Monitoring Administrator

As a Monitoring Administrator, you are responsible for monitoring systems, networks, and applications in your organization. You set monitoring policies on groups of devices and can determine if others can override the policies. You work with the Product Administrator when issues happen.

The following table includes your tasks, goals, and challenges.

| Task | Goal | Challenge |
|---|--|---|
| <ul style="list-style-type: none"> • Oversee the creation of monitoring policies. • Configure data collection and alarm thresholds. • Create reports. • Manage different monitoring configurations for Managed Service Providers (MSPs). • Develop and automate processes to maintain and monitor services. • Assist with the setup and maintenance of the physical infrastructure. • Work with the Product Administrator to identify infrastructure requirements. | <ul style="list-style-type: none"> • Ensure the accurate monitoring of your organizations infrastructure resources. • Reduce the amount of time and resources that it takes to configure monitoring. • Reduce the amount of time when issues are found. • Reduce the frequency in which issues occur using predictive analytics. • Reduce the amount of irrelevant or redundant alarms (event storm). | <ul style="list-style-type: none"> • Increased complexity of the product configuration. • Managing different monitoring needs and permissions for various end users. • Creating effective monitoring policies for large, dynamic environments. • Difficult to distinguish between important alarms and noise. |

More information:

- [Monitoring Administrator](#)

Operations Manager

As an Operations Manager, you view metric data and alarms in dashboards and reports and resolve issues that are identified by monitoring alarms. You ensure that the system is never down.

The following table includes your tasks, goals, and challenges.

| Task | Goal | Challenge |
|--|---|---|
| <ul style="list-style-type: none"> Accept and resolve issues that are identified by monitoring alarms. Accept, respond to, and resolve issue tickets that are submitted by customers. Accept, respond to, and resolve issues that are identified by supervisors. Including high-level technicians, IT Operation Managers, and Network and System Administrators. Escalate issues that cannot be resolved. Maintain the network. | <ul style="list-style-type: none"> The system is never down. Collaborate with customers. Take their feedback and use it to improve the system. Know as much as possible about networks and network monitoring. | <ul style="list-style-type: none"> I cannot see the data that helps me prevent issues. I can only see the data that shows that an issue has occurred. I frequently need a better understanding of the tools than my manager knows. My manager typically cannot help me do my job. |

More information:

- [Operations Manager](#)

IT Administrator

As an IT Administrator, you integrate CA UIM with other CA Technologies products and create customized monitoring solutions.

The following table includes your tasks, goals, and challenges.

| Task | Goal | Challenge |
|--|--|---|
| <ul style="list-style-type: none"> Configure monitoring and be alerted of issues that affect business applications. Work with other departments and application teams to ensure that issues are resolved. Take proactive measures to avoid IT issues. Develop and automate processes to maintain and monitor services. Manage the implementation of configuration, change, backup, and recovery policies. | <ul style="list-style-type: none"> Ensure constant availability of infrastructure components that the organization's applications are running through. Be warned of issues that may affect application performance. Know quickly of application performance issues. Find the root cause of issues that affect application performance. | <ul style="list-style-type: none"> Difficult to keep track of which infrastructure components an application uses. Identifying the root cause of application issues. Involves constant communication between teams, which can take a long time. No visibility into application key performance indicators which can be used to predict issues. Difficult to determine which alerts and relevant to application performance. |

More information:

- [IT Administrator](#)

Developer

As a Developer, you develop software applications that run in hybrid, public, and private cloud environments.

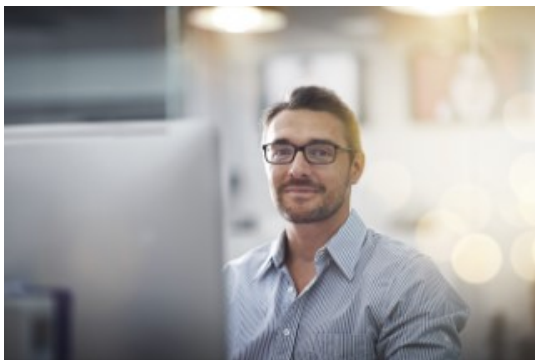
The following table includes your tasks, goals, and challenges.

| Task | Goal | Challenge |
|---|--|--|
| <ul style="list-style-type: none"> • Develop software applications. • Work with CloudOps to allocate the appropriate resources for applications. • Identify and fix bugs in applications that are related to the cloud. • Help troubleshoot issues with the cloud environment that affect an application. | <ul style="list-style-type: none"> • Automate cloud deployment and management. • Better visibility in CloudOps to application resource needs. The visibility can help minimize troubleshooting time. • Cloud management integration with the same SDKs and tools that are used to write code. | <ul style="list-style-type: none"> • Set up cloud environments with little knowledge about how they work. • Management portals for cloud resources are different based on the vendor. It is difficult to learn how to deploy and manage multiple services. • Code development gets blocked when there are unresolved issues with cloud resources. • Requirements change from service owners. As a result, it is challenging to predict cloud resource needs. |

More information:

- [Developer](#)

Evaluator



Discover a wealth of information to help you during your investigation, evaluation, and purchasing decision. See why businesses are choosing our unified management solution over the competition.

Up Your App Game with CA UIM

See why businesses are choosing our unified infrastructure management solution over the competition. Consider five factors when selecting an infrastructure management vendor:

1. Ease of management
2. Unified platform
3. Analytics and reporting
4. Depth of infrastructure management
5. Enables monitoring as a service.

[View the Apprize 360 Intelligence Report](#)

How CA UIM Stacks Up Against the Competition

Market research firm Apprize360 rates CA UIM the highest against HP, SolarWinds, and Microsoft. CA UIM wins again among open source IT infrastructure monitoring and management solutions, including Nagios, Zabbix, and Icinga,

| Apprize360 Intelligence | CA Unified Infrastructure Management | HP Operations Manager | SolarWinds Server & Application Manager | Microsoft System Center (formerly SCOM) |
|---|--------------------------------------|-----------------------|---|---|
| Ease of Deployment | | | | |
| Ease of Management | | | | |
| Breadth of IT Monitoring | | | | |
| Interactive Reports with Self-Service Analytics | | | | |

Customer Reviews

CA UIM is recognized by users at [IT Central Station](#) as the number one system monitoring solution, the number one cloud monitoring solution, and the number one event monitoring solution.



Video: CA UIM Review

Watch the following video and learn why Craig Darnell, manager of an end-to-end monitoring team, selected CA UIM to consolidate many disparate systems into a single solution. CA UIM provided Dave's team with the flexibility to gain more insights into the end-user experience.

TIP

To play this video in full screen, click the YouTube logo to the right of Settings at the bottom of the video.



[Read all customer reviews](#)

Forrester Study

CA Technologies commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study to examine the potential return on investment (ROI) that enterprises may realize by deploying CA Unified Infrastructure Management (CA UIM). The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of CA UIM on their organization.

[Read the Forrester Study](#)

Customer Success

TriZetto, a Cognizant company and business unit within Cognizant's healthcare practice, provides world-class information technologies to make better healthcare happen. TriZetto reduces resolution times by seventy-six percent and prevents eighteen outages with CA Technologies and the CA UIM solution.

eBook

The CA Unified Infrastructure Management: Most comprehensive hybrid cloud and IT monitoring eBook is available.

[View the eBook](#)

Product Documentation

Read our product documentation and quickly understand the business value that CA UIM provides, the architecture, components, and how scalable the solution is. In addition, get up to speed on what's new in the current release.

- [Business Value: UIM](#)
- [UIM Architecture](#)
- [UIM Interfaces](#)
- [Release Comparison](#)
- [What's New](#)
- [Release Notes](#)

Get Answers Before Purchasing

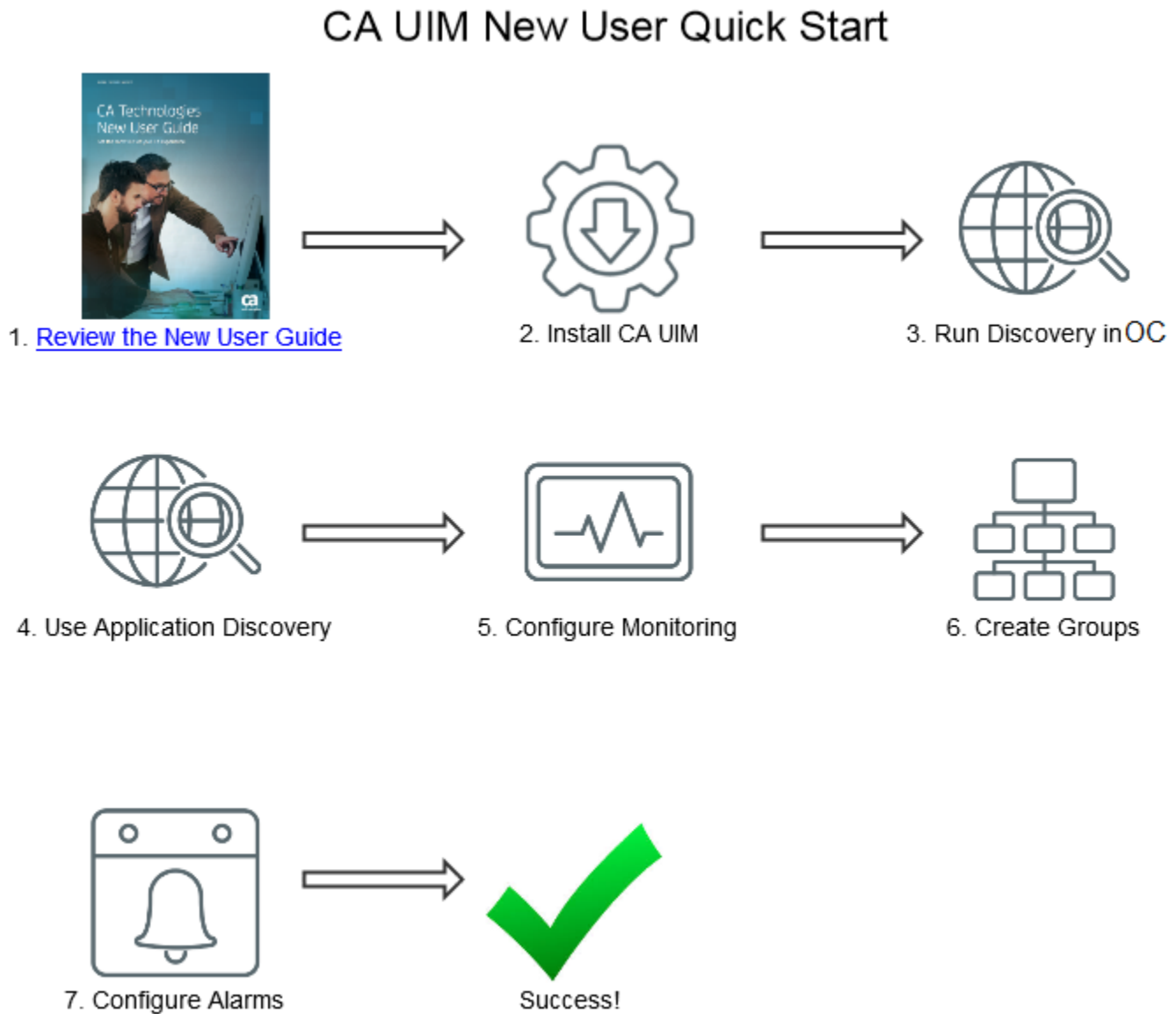
Our product experts are available to help you find the right solution to meet your specific needs.

New User



New to CA UIM and not sure where to begin? Don't worry, we have you covered. Follow these steps, and you will be up and running quickly.

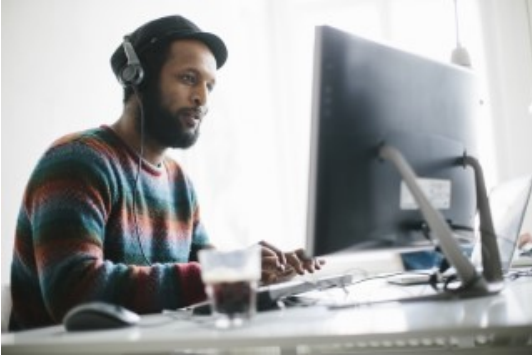
Figure 1: New User Quick Start



Follow these sections for more information:

1. [Review UIM Concepts](#)
2. [Install UIM](#)
3. [Run Discovery in OC](#)
4. [Use Application Discovery](#)
5. [Configure Monitoring](#)
6. [Create Groups](#)
7. [Configure Alarms](#)

Product Administrator



Learn how to optimize the CA UIM features and monitor your devices and infrastructure.

- [Research](#)
 - Stay up to date on the new product features.
- [Install](#)
 - Install the product.
- [Administer](#)
 - Set up and manage robots, hubs, and tunnels.
- [Probes](#)
 - Deploy probes for monitoring administrators.
- [Upgrade](#)
 - Upgrade the product to the current release.
- [Troubleshoot](#)
 - Troubleshoot when the product does not work as expected.
- [Videos](#)
 - Watch videos to help you become more productive.

Monitoring Administrator



Learn how to use the probes to configure data collection and alarm thresholds and ensure accurate monitoring of infrastructure resources.

- Probe Deployment ([Automatic](#) | [Manual](#) | [Bulk](#))
 - Automatically deploy and configure monitoring probes with the MCS, manually with Admin Console, or by bulk.
- [Application Discovery](#)

- Automatically discover, group, and monitor devices in your environment.
- [Alphabetic List of Probes](#)
 - Learn about the available probes.
- [CA Business Intelligence Dashboards](#)
 - Use these dashboards to monitor the state of your environment.
- [Monitoring Configuration Service](#)
 - Deploy probes, deploy configuration profiles, apply configuration changes, and manage deployed configuration profiles.
- [Videos](#)
 - Watch videos to help you become more productive.

Operations Manager



Learn how to view metric data and alarms in dashboards and reports and resolve issues identified by monitoring alarms. You help ensure the system is never down.

- [Alarm Management](#)
 - View alarms in OC, clear alarms, assign alarms to others, edit existing alarms, and more.
- [CA Business Intelligence Dashboards](#)
 - Use these dashboards to monitor the state of your environment.
- [Troubleshoot Alarms](#)
 - Use Log Analytics to troubleshoot raised alarms.
- [Videos](#)
 - Watch videos to help you become more productive.

IT Administrator



Learn how to integrate CA UIM with other CA Technologies products and create customized monitoring solutions.

- [Log Analytics](#)
 - Integrate CA UIM with Log Analytics and CA App Experience Analytics.
- [Integrate CA Application Delivery Analysis](#)
 - Integrate CA UIM with CA Application Delivery Analysis.
- [Integrate CA Network Flow Analysis](#)
 - Integrate CA UIM with CA Network Flow Analysis.
- [Integrate CA SiteMinder](#)
 - Integrate CA UIM with CA SiteMinder.
- [Integrate CA Spectrum](#)
 - Integrate CA UIM with CA Spectrum.
- [Videos](#)
 - Watch videos to help you become more productive.

Developer



Learn how to use the development tools that CA UIM provides to create and manage CA UIM components such as Operator Console (OC) portlets and probes. Software Development Kits (SDKs) and Application Programming Interfaces (APIs) are available for several different programming languages.

- [Working with Development Tools](#)

- Learn what development tools are available for .NET API, C SDK, Java SDK, nas script editor, Perl SDK, and RESTful web services.
- [Probe Developer](#)
 - I'm a probe developer who creates monitoring probes that are configurable using the Admin Console. I need more information about the Probe Software Developer Kit.
- [NimAlarm Utility](#)
 - I use the NimAlarm Utility to send alarm messages across the UIM Message Bus using the operating system command line.
- [Videos](#)
 - Watch videos to help you become more productive.

CA UIM Overview

In today's economy, the applications that deliver a differentiated and superior experience provide a distinct competitive advantage. The underlying infrastructure that powers an application can make or break the user's experience. Proactively managing the experience that infrastructures deliver is a necessity, but can be challenging as infrastructures continue to become more dynamic and hybrid in nature. Many enterprise IT and service provider organizations are battling against the inefficient tools they have implemented. Adoption of such tools poses challenges; such as, underutilized resources, lack of agility, and poor user experience.

CA UIM provides a single, analytics-driven solution for proactively and efficiently managing modern, cloud and hybrid IT infrastructures. CA UIM is the only solution that provides intelligent analytics, comprehensive coverage and an open, extensible architecture. By leveraging the solution, you can speed mean time to repair, reduce monitoring efforts, accelerate new deployments and improve the end-user experience. The solution also provides unified, automated monitoring configuration and deployment, making it optimally suited to today's DevOps and high-scale environments.

By leveraging a single, unified solution that offers a comprehensive infrastructure coverage, you can stop having to rely on dozens of disjointed point tools. Consequently, you can streamline administration and more quickly support the delivery of new services, applications, and technologies.

View this short video for a summary of how CA UIM delivers a single view and unified analytics across all elements of your IT infrastructure. The video shows all the elements of your IT network in a single view, helping you streamline your infrastructure management:

CA UIM Architecture

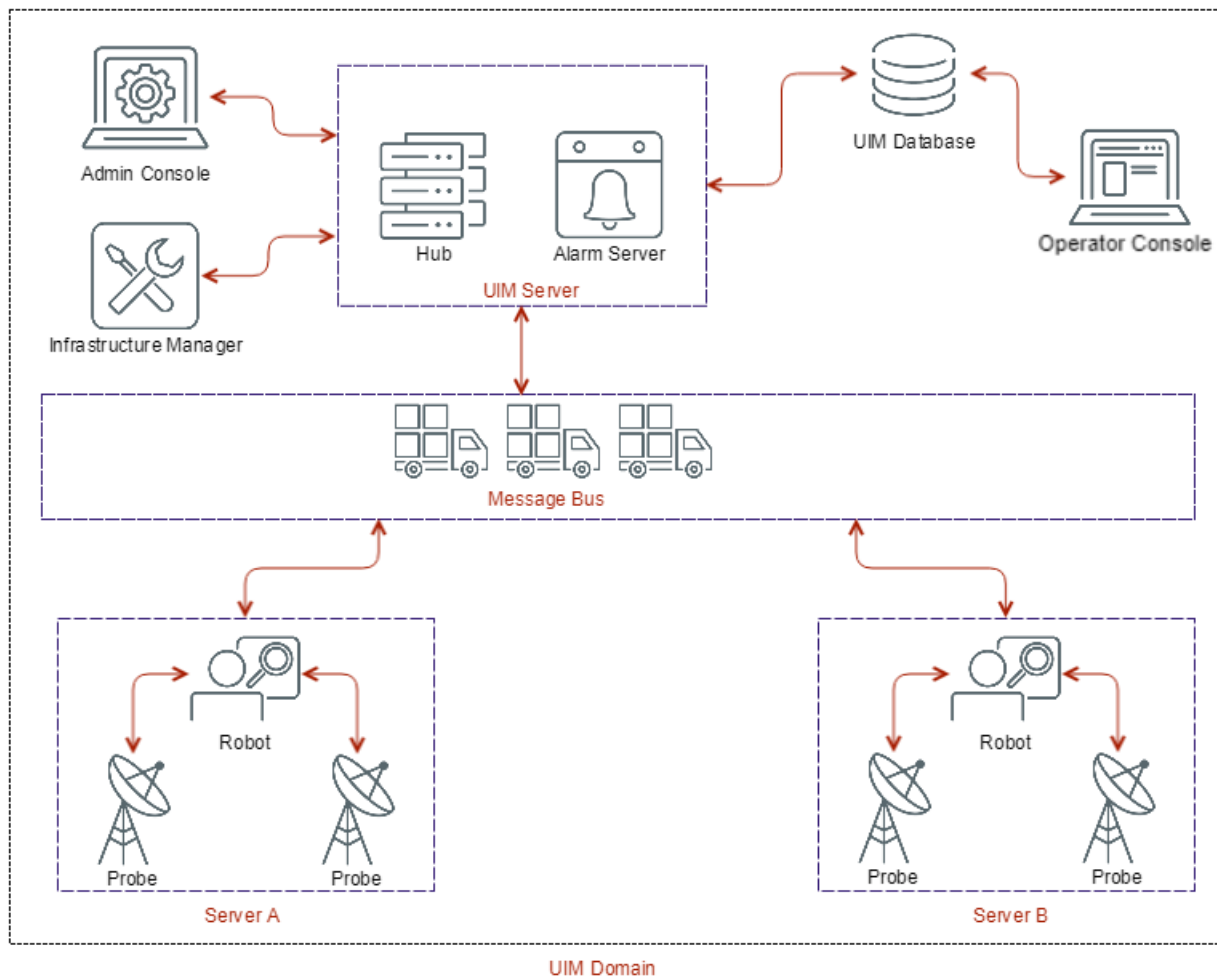
This article provides an architectural overview of the CA UIM monitoring solution. The following topics cover the complete information:

Architecture Diagram

All infrastructure components are organized in a hierarchy. From bottom to top, the components are:

- Probes
- Robots
- Hub
- Domain

The following illustration shows a CA UIM domain, encompassing the server, database, infrastructure (hub, robots, probes), and user interfaces:

Figure 2: Architecture

Monitoring Configuration Capabilities

CA UIM is built on a unified architecture that enables organizations to monitor:

- Servers
- Applications
- Databases
- Networking services
- Network devices
- Private and public clouds

CA UIM offers the following monitoring configuration capabilities:

- **Local monitoring** - CA UIM provides local monitoring, which allows a managed device to be monitored even when the device becomes temporarily disconnected from the rest of the management system.
- **Remote monitoring** - CA UIM can also remotely monitor devices and applications. For example, CA UIM can act as a remote client in client-server environments.

- **SNMP monitoring** - CA UIM can communicate with network devices using SNMP. In addition, CA UIM can receive and process SNMP traps.

CA UIM Components

This article includes information about the following CA UIM components:

Message Bus

Applications within the CA UIM domain communicate by exchanging messages. The CA UIM message bus provides the capabilities that are required to communicate across an entire enterprise infrastructure. Data flow in the message bus is based on request/response and publish/subscribe models:

- **Request/response** is the standard way of communicating over the network. A client issues a request to a server and the server responds to the request.
- **Publish/subscribe** allows clients to send data such as alerts, performance data, or messages targeted for gateway servers without a designated receiver. This method also allows clients to select messages based on subject.

When a system within a CA UIM domain has new data, it automatically publishes it to the message bus. All applications that subscribe to updates for that system automatically receive that update. Together with the associated application APIs, the message bus enables all monitoring components to communicate with each other, without direct program-to-program connections.

The following video highlights the message bus architecture of CA UIM and the value it brings to the customer:

The Subscribe Mechanism

The subscribe mechanism enables probes and robots to select messages based on the message subject. A client that is configured to receive CA UIM messages sends a subscribe request to the hub. The client then receives messages matching the subscribed subjects from the hub. A client can use the following methods when subscribing:

- **Subscribe** - The client connects to the hub and gets messages as long as the client is running.
- **Attach** - The hub configures a message queue to hold the messages if the client is not running. When the client comes back up, all messages are passed on. This includes messages that were received when the client was inactive.

Types of Messages

The two main types of messages that are sent across the message bus are:

- **Quality of Service (QoS) messages** - The metrics that probes collect are sent to the CA UIM database in the form of QoS messages.
- **Alarm messages** - Alarm messages are sent from probes and the baseline_engine. These alarm messages are processed by a CA UIM alarm server (nas or ems).

Probes

CA UIM probes provide the intelligence to manage specific components on a managed device. For example, one common probe, the CDM probe, is responsible for monitoring CPU, disk, and memory utilization on target hosts. More than 140 probes are available, allowing users to manage the entire IT infrastructure, including servers, network devices, applications, and databases as well as usage metering and data center power consumption. Probes can be easily deployed across an entire network either using a simple drag-and-drop interface or programmatically. You can also write custom probes with CA UIM SDKs.

Robots

Robots manage the CA UIM probes. A robot starts and stops its probes at the required times, and collects, queues, and forwards the monitoring data. Robots can be deployed to support either local (agent-based) or remote (agent-less) monitoring,

Each robot has three dedicated tasks:

- **Control the probes** attached to the robot, which includes starting and stopping them at the required times (accomplished with the robot controller probe).
- **Collect, queue and forward** the probe messages (accomplished with the *spooler* probe).
- **Provide a simple database service** for its probes. This action allows the robot to store data for threshold monitoring and data trending, and ensures that collected data survives power outages (accomplished with the *hdb* probe).

The three probes that are mentioned here are service probes that are present on every robot.

All robots are identical; it is the collections of probes they manage that distinguish them. Probes can be grouped together into packages so that you can appropriately deploy them to various types of servers.

If a robot contains a hub probe, it is promoted to the next level in the domain hierarchy: the hub.

Hub

A hub is a vital component within a CA UIM deployment. A hub is a software component within a CA UIM domain that enables components to connect to the message bus. A hub receives all messages posted by any client and distributes these messages to a set of subscribers of the publishing subject. A hub also keeps track of the addresses in the hub's domain, and information about each of the systems being monitored by robots. A CA UIM domain can have multiple hubs, which enable failover in the case of a communication disruption. Multiple hubs are also used to connect managed networks together across the Internet using SSL tunnels between the hubs.

Hubs have the following designations depending on their purpose:

- The **primary hub** communicates with the database. Every deployment has one, and only one, primary hub. This hub is created when you install the CA UIM Server software.
- **Secondary hubs** can be used to scan the network (device discovery), perform baseline calculations on QoS metrics, or group robots according to function, geographical location, departmental code, or other criteria. Although secondary hubs are optional, almost all deployments have them. Secondary hubs are created after CA UIM Server is installed. They can be created or removed as needed to meet the needs of your IT environment.
- A **failover hub** is a secondary hub that performs primary hub actions when the primary hub becomes unavailable.
- **Tunnel hubs** use VPN-like connections to communicate through firewalls.

Alarm Server

CA UIM features an alarm server (nas or ems) that is responsible for receiving and managing incoming alarm messages. The alarm server also supports message suppression and provides clients with such services as event updates, message filtering, automated actions, and mirroring capabilities. The alarm server also allows customers to enable advanced event correlation capabilities.

User Interfaces

There are several different user interfaces that you can use to manage each part of CA UIM:

- [Admin Console](#)
- [Operator Console](#)
- [Infrastructure Manager](#)

CA UIM Key Features

CA UIM provides the following key features:

- **Most comprehensive coverage:** CA UIM provides the most comprehensive coverage of modern cloud-based infrastructures and traditional IT resources. As a result, the solution reduces complexity, speeds mean time to resolution and streamlines cloud adoption.
- **Complete visibility of infrastructure stacks:** No matter what your application or infrastructure stack is built on, CA UIM provides the monitoring capabilities to manage its performance. The solution provides support for monitoring physical and virtual servers, public or private cloud environments, storage platforms, databases, hyper-converged infrastructures, packaged applications, mainframes and big data technologies.
- **Intelligent analytics:** CA UIM offers intelligent, intuitive insights through these key analytics:
 - **Unified application-centric analytics:** CA UIM analytics offer complete coverage of complex, hybrid infrastructures and provide end-to-end visibility from an application perspective.
 - **Contextual log analytics:** The solution automatically correlates structured infrastructure performance data with unstructured event logs to facilitate rapid issue identification.
 - **Predictive analytics:** CA UIM helps you proactively identify issues before the user experience suffers.
- **Open, multi-tenant, extensible architecture:** CA UIM delivers the flexibility you need to extend coverage to support new technologies or to expand coverage to support more devices, services, users or tenants. The solution is also easy to integrate with other IT operations tools.
- **Rapid, automated deployment and configuration:** CA UIM provides an automated, template-based approach to monitor your entire infrastructure, enabling you to meet the needs of highly dynamic environments.

Additionally, by adopting CA UIM, you can also achieve the following:

- **Optimize the user experience:** Use a single, analytics-driven solution to speed mean time to repair and enhance the user experience.
- **Reduce complexity and boost productivity:** Eliminate the effort associated with using and managing multiple monitoring tools.
- **Improve resource utilization:** Gain intelligent and holistic insights to optimize utilization across hybrid infrastructures.
- **Future proof your business:** Leverage comprehensive coverage and an open, scalable architecture that can address your needs of today and adapt to quickly to emerging requirements.

Service and System Monitoring

CA UIM allows you to monitor and manage the following systems and services:

- Servers such as Windows, Linux, UNIX, Cisco UCS, Novell Open Enterprise Server, and IBM Power Systems
- Storage, including EMC, Hitachi, IBM System Storage, and NetApp
- Networks, including routers, switches, and firewalls
- Virtualization platforms, such as VMware and vCloud Monitor, Microsoft Hyper-V, Solaris Zones, IBM PowerVM, Citrix XenServer, and XenDesktop and Red Hat Enterprise Virtualization.
- Databases, such as Oracle, Sybase, Microsoft SQL Server, IBM Informix, and IBM DB2
- Applications like Microsoft Exchange, Microsoft IIS, Active Directory, Citrix, WebSphere, JBoss, home-grown applications and much more
- Cloud environments, such as Amazon Web Services, Rackspace, Google Apps, Salesforce.com, Vblock, and FlexPod.
- VoIP environments from Cisco
- Virtual desktop infrastructures, including Citrix XenDesktop and XenApp
- Data center power, cooling, and energy

CA UIM Reference Architecture

Reference Architecture provides information about the baseline functional feature and technical architecture that are required to deliver the CA UIM solution. View and download the [CA UIM Reference Architecture](#) document.

CA UIM Interfaces

You can access information in CA UIM through the following interfaces:

- [Admin Console](#)
- [Operator Console](#)
- [Infrastructure Manager](#)
- [RESTful Web Services](#)

You can use these interfaces based on your requirements.

Admin Console

A web-based management console that allows you to manage your CA UIM infrastructure on virtually any desktop or server operating system. An alternative to Infrastructure Manager, Admin Console provides a growing number of equivalent management capabilities.

Users with administrator or superuser permissions can access the Admin Console.

Admin Console (accessible in a web browser, or "stand-alone" mode) is installed and available on the primary hub after CA UIM Server installation is complete. To access it, go to the CA UIM web page (http://<servername_or_IP_address>:<service_host_port>), then click **Admin Console** in the **CA UIM Server Administration** section. The Admin Console view is installed during Operator Console (OC) installation.

Admin Console Interface

Admin Console has the following elements.

- The **Main window** provides a view of your infrastructure:
 - The left navigation pane displays the hubs.
 - The right pane displays either robot or probe information based on your selection in the navigation pane.
 - At the top of each section is a filter you can use to customize your view of the interface.
- The **Infrastructure** button in the upper left of the main window displays your infrastructure components in the right pane. If you:
 - Select a hub in the navigation pane, the right side of the screen displays the robot information and properties for that hub.
 - Select a robot in the navigation pane, the right pane provides four options for accessing information about your robot: **Robot Properties**, **Probes**, **Packages Installed**, and **Environment variables**.
- The **Archive** button in the upper left of the main window displays the probe package archive in the right pane:
 - You can deploy, import, and delete probe packages in this view.
 - The *local packages* screen displays the probes that reside in the archive on the hub. The local archive contains all probes that were installed during CA UIM installation, and those that have been downloaded subsequently.
 - The *web packages* screen displays the list of probe packages on the CA UIM support archive.
 - The *distribution activity* screen displays a log of probe package distributions, along with the status of each distribution.

For more information about Admin Console, see [Using Admin Console](#).

Operator Console

The Operator Console(OC) is a web-based interface that allows you to:

- discover and monitor systems
- graph QoS data
- view and manage alarms
- create SLAs and view SLA performance reports
- create, view, and schedule reports
- create and view dashboards
- manage users

The Operator Console webapps-based interface design allows you to configure and view monitoring applications in ways that suit your particular needs. Each component contains a set of graphical user interface controls, which you can use to manage how the applications display their data and results. Some components require an additional purchase. For more information about OC, see the OC topics in [Configure and View Monitoring Data](#).

The Operator Console provides views to help you monitor your infrastructure technology stack that is spread across hybrid cloud, physical and virtual servers, storage, database, and network resources.

- **Home View** - provides a quick at-a glance view of the state of your deployment in terms of what is being monitored. You can view the alarm charts, alarm summary, monitored technologies that are sorted by alarm severity and count, devices discovered and actively monitored, role spread of monitored devices, top devices sorted by alarms, and top groups sorted by alarms.
- **Alarms View** - displays all the alarms that are generated in your environment.
- **Groups View** - displays cards, tree view, and list view for each group.
- **Inventory View** - provides an easy way to view the devices in UIM inventory that is generated for environments you are monitoring. You can also view information around them like alarms and see which devices have robots that are deployed.
- **Dashboards View** - lets you access the dashboards.
- **Reports View** - displays all the reports that are created in your environment.

NOTE

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

Prerequisite

- To view the data in Operator Console, ensure that you have the Operator Console Basic permission. When upgrading to UIM 20.3.0, users will not have access to the Operator Console. You must add the *Operator Console Basic* ACL permission in the Account Admin view. By default, this permission is only available to Administrators and Superusers.
- The Operator Console is supported only on Edge, Chrome and Firefox browsers. For more information, see [Compatibility Matrix](#).

After you log in to the Operator Console, you can perform related actions based on your access permissions.

NOTE

For more information about how to use Operator Console, see [Operator Console Functions](#).

Infrastructure Manager

Infrastructure Manager is a Windows application that lets you configure and manage your CA UIM deployment. It provides:

- A hierarchical view of systems being monitored
- An alarm window to view all alarms and messages
- Interfaces that allow you to configure your hubs, robots, and probes

Infrastructure Manager connects to an active hub and allows you to control, configure, and manage the robots and probes in your deployment.

The Infrastructure Manager Interface

The Infrastructure Manager window has the following elements:

- **Main menu** and **toolbar** provide pull-down menus and quick access buttons that let you customize your view of the interface, locate infrastructure elements, and manage user accounts.
- **Console pane** (left) provides a hierarchical view of your infrastructure and uses color-coded icons to indicate element status. This pane contains the following nodes:
 - **Domains** shows your hub-robot-probe structure
 - **Dynamic Views** groups robots by operating system
 - **Groups** displays user-created groups of hubs, robots or probes
 - **Archive** lets you access probe packages and licenses stored in the current hub's archive

NOTE

The above-mentioned licensing functionality is no longer applicable for CA UIM 9.2.0. From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).

- **URLs** and **Applications** let you launch web pages or other applications
- **Main window pane** (upper right) displays details about the element selected in the console pane. For example, if you click a hub in the console pane, all of the hub's robots are displayed in the main window pane. This pane also has its own dynamic toolbar, which provides quick access to functions related to the displayed elements.
- **Doc Pane** (lower right) appears if the **View > Dock Pane** menu option is checked. It can display:
 - Alarms
 - System messages
 - Contents of the main window pane
 - Previously docked windows

For more information about Infrastructure Manager, see [Using Infrastructure Manager](#).

RESTful Web Services

A Representational State Transfer (RESTful) web service interface for CA UIM. This interface offers customers the functionality to access their CA UIM installation using REST-based web service calls.

For more information, see the Probe Development Tools section of the [Probes Documentation Space](#).

Videos

This article includes videos that provide extra information, context, and examples that augment the product documentation.

UIM 20.3: New Capabilities

This video demonstrates the following new capabilities in UIM 20.3:

- Setup wizard for probe configuration.
- Inventory tree
- Enhanced alarm console

UIM 20.3: Inventory View in OC

This video demonstrates the functionalities that the inventory view provides in the Operator Console (OC).

UIM 20.3: How to Manage Alarms in OC

This video demonstrates how to manage alarms in the Operator Console (OC).

UIM 20.3: Maintenance in OC

This video demonstrates how the maintenance functionality works in the Operator Console (OC).

UIM 20.3: Administrative Auditing

This video demonstrates how to audit administrative operations in UIM.

UIM 20.3: UIMAPI and MCS CLI Enhancements

The following videos demonstrate the UIMAPI and MCS CLI enhancements in UIM 20.3:

CA UIM Security

This document provides a summary of the security information in the existing CA UIM documentation. This information is provided as a reference and is not intended to override your own internal policies and security best practices.

Review the following topics:

- [Account Management](#)
 - [Types of Users](#)
 - [Password Policies](#)
 - [ACL Permissions List](#)
 - [Permissions Reference for Operator Console \(OC\) Views](#)
- [Systems Access](#)

- [CA UIM Interface](#)
- [Port Requirements](#)
- [HTTPS Configuration](#)
- [CA UIM Installer Creates the Database Schema and User](#)
- Software Installation and Upgrades
 - [Installation Parameters](#)
 - [Optional Post-Installation Tasks](#)

Additional points for some of the topics are as follows:

- For **Account Management**, the Account Admin view allows bus users to manage account contact users and access control lists (ACLs) for user groups. You must have appropriate ACL permissions to view and make changes within the Account Admin view.
- For **HTTPS Configuration**, during the initial installation of UIM Server, HTTP access to the UIM Server webpage and Admin Console is configured on port 8080. The default port for HTTPS configuration in Admin Console is 8443. After you configure HTTPS in Admin Console, port 8080 is not required.
- For **Software Installation and Upgrades**, download CA UIM software from support.broadcom.com, [Download Management](#) section. You must have Administrator permissions on a system to install CA UIM and OC.

Additional Resources

This section provides resources to assist you in maximizing your product experience.

CA UIM Education and Training

Just one hour of training saves five hours of lost productivity. Trained users make 35% fewer support calls. A well-trained team also delivers more value from their technology investments.

Ensure that your team can fully leverage your CA UIM investment to meet your business needs today and into the future through training courses and CA Learning Subscriptions.

CA Learning Subscription

[CA Learning Subscriptions](#) provide access to an extensive library of videos, e-learning courses, dynamic labs and more so you can learn what you need to know, when and where you need it. Content is added and updated regularly so you always have access to the latest courses and training materials.

Free Training

Learn about free training, as well as how to personalize your learning experience. See [CA Education and Training](#).

CA UIM User Community

The CA UIM [Community](#) is the place to share ideas, tips, information, insights, and more with your business peers and Broadcom experts. The community provides a unique opportunity to network and help you maximize your software investment by tapping into a community of expertise, open 24/7.

CA UIM Knowledge Base (KB) Articles

CA UIM has a vast [Knowledge Base](#) to help you identify workarounds for known issues or resolve popular issues with your implementation.

CA UIM Videos

Watch the CA UIM [videos](#) available on YouTube from CA Technologies to increase your product knowledge.

Getting Started with Broadcom

Review the [CA Technologies New User Guide](#) to get the most out of your CA experience. This guide provides information about how a new user can get started with Broadcom; for example, register with CA, partner with CA Services, access helpful online resources.

Contact CA and Support

For information about CA products and solutions, go to support.broadcom.com - to access the CA Support website

Accessing support.nimsoft.com

All support.nimsoft.com accounts have been migrated to use Broadcom authentication; however, passwords have not been migrated to maintain security. Perform this mandatory step to continue accessing support.nimsoft.com. Once you perform this step, you need to use the same credentials to access the archive through the Admin Console (AC) or the Infrastructure Manager (IM).

Follow these steps:

1. Log in to support.broadcom.com with your existing user name. You are prompted to reset your password. An email with a link to reset the password is sent to you.
2. After resetting your password in support.broadcom.com, navigate to support.nimsoft.com, and verify that you can log in to the portal.

NOTE

Use the same name that you used to access support.broadcom.com.

3. After you have verified, you can now reset your credentials in the AC and the IM.

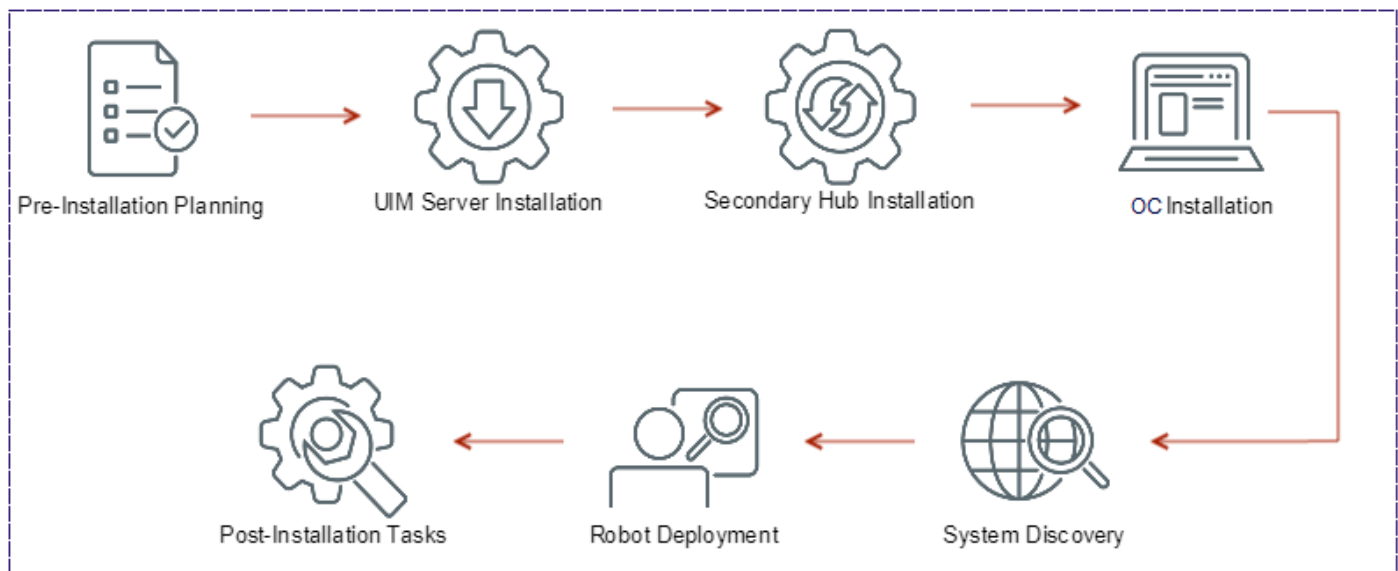
Installing

CA UIM consists of several distributed software components. The process for installing each of these components can be divided into different steps.

Installation Process Diagram

The following diagram shows the high-level process:

Figure 3: Installing Various Components



Installation Process Steps

The high-level process is divided into the following steps:

1. [Plan Pre-Installation](#)
2. [Install UIM Server](#)
3. [Install Secondary Hubs](#)
4. [Install Operator Console](#)
5. [Discover Systems to Monitor](#)
6. [Deploy Robot](#)
7. [Perform Post-Installation Tasks](#)

Pre-Installation Planning

Before you attempt to install CA UIM components, complete all documented pre-installation tasks. These tasks include the following:

1. [Preparing your server hardware for each UIM component.](#)
2. [Configuring the operating systems for each piece of server hardware in the CA UIM environment.](#)
3. [Installing and configuring the third-party database software that hosts the UIM database.](#)

After you complete all the pre-installation planning tasks, you can proceed to the article [Install UIM Server](#).

Once installed, the CA UIM environment contains several components:

- **The Database Server:** The Database Server is the location of the UIM database. QoS data and other required system information is written to the Database Server.
- **The Primary Hub Server:** The Primary Hub Server is the location of the robot that controls the UIM Primary Hub. The Primary Hub Server is also known as the UIM Server.
- **The OC Server (Optional):** The OC Server contains all the components that are required to run the Operator Console (OC). It is recommended that you install the OC Server on a separate computer. However, in small deployments that you want to use for Proof of Concepts (PoCs) or for product demonstrations, you can install OC on the Primary Hub Server.
- **Secondary Hub Servers (Optional):** You can deploy Secondary Hub Servers in your environment for load-balancing and failover capability.

NOTE

More information:

- [Prepare Your Server Hardware](#)
- [Configure Your Operating Systems](#)
- [Install and Configure Your Database Software](#)
- [Configure IPv6 Support](#)
- [Password Policies](#)
- [Firewall Port Reference](#)
- [CA UIM Sizing Recommendations](#)
- [Product Compatibility](#)

Prepare Your Server Hardware

This article details the deployment guidelines and hardware requirements for each component in your UIM environment. The following topics cover the complete information:

Hardware Overview

For the best CA UIM performance, the physical or virtual servers that host your primary components must have:

- Processing power and memory that are sufficient for the size of your deployment
- Supported software that is installed and configured

Assessing the hardware requirements for any large and complex software system is a challenge. Over-sizing seems wasteful, but underestimating can create performance problems. Because each environment is unique, no fixed rules or formulas can ensure a minimum optimal configuration. Consider the following items:

- Keep in mind that a hardware configuration that works today can require growth in the future. Take forecast growth into consideration when planning your hardware requirements.
- Use the information in this article to begin planning your deployment. However, your situation can impose greater or lesser demands on the system.
- If possible, obtain hardware of the most current generation to anticipate the longest useful life.
- Consult your presales consultant if you have any doubts or concerns about your hardware needs.
- For evaluations, you can install the database, UIM Server, and OC on a single system. For production environments, distribute them across multiple virtual or physical servers. A distributed deployment gives each component sufficient computing power and memory to perform optimally.

While every situation is unique, the following deployment size categories can give you a starting point for assessing your hardware requirements:

| Example Use Case | Deployment Size | Recommended Number of Hubs | Recommended Number of Robots |
|------------------------------------|-----------------|----------------------------|------------------------------|
| A small company or individual team | Small | <5 | <200 |
| A medium-sized company | Medium | 5-20 | 200-1000 |
| A large company | Large | 20+ | >1000 |

WARNING

If you require a deployment with over 50 hubs and 1000 robots, it is recommended that you consult CA professional services or a CA UIM certified partner.

Database Server Requirements

Minimum processor: 64-bit XEON-class.

| Deployment size | Processor | Memory | Disk Size |
|-----------------|--------------------|--------|-----------|
| Small | 8 cores x 2.8 Ghz | 12 GB | 100 GB |
| Medium | 16 cores x 2.8 Ghz | 16 GB | 500 GB |
| Large | 16 cores x 2.7 Ghz | 32 GB | 2-3 TB |

Additional storage recommendations:

- Use RAID 10 (for speed and reliability).
- Spread database files across multiple disks to improve I/O.
- Choose drive subsystems with low latency/seek times, high spindle speeds, high interconnect bandwidth.
- Consider using SSD drives if you have significant reporting needs.
- Consider data redundancy, synchronization, and database growth.

NOTE

Disk I/O performance and server bus bandwidth impact relational database server performance. Crowded VM hosts, clusters, or heavily shared storage in VM environments are not recommended for hosting the database. Selecting the right database storage solution is beyond the scope of this article. Consult your storage vendor if you need further assistance.

Primary Hub Server Requirements

Minimum processor: 64-bit XEON-class

| Deployment size | Processor | Memory | Disk Size |
|-----------------|-------------------|--------|---|
| Small | 8 cores x 2.8 Ghz | 12 GB | 100 GB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows) |

| | | | |
|--------|--------------------|-------|---|
| Medium | 16 cores x 2.8 Ghz | 16 GB | 100 GB for main drive and 100-300 GB for hub queues (as desired to enable queues to fill up on disk in the case of extended outages or maintenance windows) |
| Large | 16 cores x 2.5 Ghz | 32 GB | 200 GB for main drive and 200-500 GB for hub queues (as desired to enable queues to fill up on disk in the case of extended outages or maintenance windows) |

Secondary Hub Server Requirements

The requirements for a secondary hub vary, depending on the load the hub carries. Consider the following items:

- A secondary hub requires hardware equal to that of your primary hub if:
 - The hub manages a large number of robots.
 - The hub is configured for high availability and must take over the role of the primary hub.
- If the secondary hub manages a small number of robots (for example, for a remote subnet with limited components to monitor), less powerful hardware can be used.

OC Server Requirements

Minimum processor: 64-bit XEON-class

| Deployment | Processor | Memory | Disk Size |
|------------|--------------------|--------|-----------|
| Small | 8 cores x 2.8 Ghz | 12 GB | 50 GB |
| Medium | 16 cores x 2.8 Ghz | 16 GB | 50 GB |
| Large | 16 cores x 2.5 Ghz | 24 GB | 100 GB |

NOTE

OC performance can be affected by the number of concurrent users accessing a single OC instance. We recommend installing additional OC servers to accommodate a large number of concurrent users on the network. The following are general guidelines for the number of concurrent users suitable for a single OC instance on each size of deployment:

- Small: 5 concurrent users
- Medium: 10 concurrent users
- Large: 20 concurrent users

For information on adding OC servers to a network, see the topic [Configure Multiple Operator Console \(OC\) Servers](#).

Distributed Discovery Server Requirements

The Discovery Agent (discovery_agent) is released as a part of the core Unified Infrastructure Management Server release. For optimal discovery in larger environments, more than one discovery agent can be deployed. Some users, particularly service providers and those with very large networks, find it useful to deploy multiple discovery agents in various locations. Discovery of a large network can be divided across administrative boundaries with no direct connectivity to devices at a remote site because of firewall constraints or network-address translation (NAT). For efficient discovery, deploy discovery agents such that each one discovers an exclusive part of the network.

Recommended minimum hardware requirements for deploying Discovery Agent on a server are:

Memory:

- 4 GB minimum RAM for up to 16K IP addresses
- 2GB additional RAM per additional 8K addresses

64-bit CPU:

- 2 minimum core processor for up to 16K IP addresses.
- 1 additional core processor per additional 8K addresses

Port Requirements

For more information about port requirements, see the article [Firewall Port Reference](#).

Virtual Machine Installation Requirements

You can install CA UIM components on a virtual machine. The requirements for virtual machine installation are as follows:

- The guest OS on the virtual machine must run a CA UIM-supported operating system. For more information about supported operating systems, refer to the [Compatibility Support Matrix](#).
- The virtual machine must meet the hardware requirements that are described in this article.

VMware Virtual Machine Installation Requirements

TIP

Review the [Enterprise Java Applications on VMware -- Best Practices Guide](#) for general guidelines regarding installation on VMware virtual machines. Refer the [CA Support Statement for VMWare](#) also for additional information.

To install CA UIM on a VMware virtual machine, VMware ESXi 5.5 or later is required.

Configure Your Operating Systems

Before you run the CA UIM installer, configure the operating systems for the servers that will host the CA UIM environment.

The following topics cover the complete information:

TIP

If you have questions regarding which operating systems are supported with CA UIM, refer to the [Compatibility Support Matrix](#).

General Operating System Prerequisites

The systems you are installing CA UIM on **require** x64 (64-bit) architecture.

NOTE

All your servers do not require the same operating system.

This section includes the following information:

- Java on VMware Virtual Machines
- Java Runtime Environment (JRE) Requirements
- Firewalls and Virus Scanners
- Localization Requirements
- Swap Space Requirements
- Timezone Requirements

Java on VMware Virtual Machines

Review the VMware *Enterprise Java Applications on VMware - Best Practices Guide* available at <http://www.vmware.com/resources/techresources/1087> (not affiliated with CA Technologies).

Java Runtime Environment (JRE) Requirements

The UIM Server installer contains the proper JRE version for CA UIM. If you are installing UIM Server on a system where another JRE is already installed, we recommend removing the existing JRE. Running multiple JRE versions on the same system can cause issues in your CA UIM environment.

Firewalls and Virus Scanners

Before you install CA UIM:

1. Shut down any antivirus software.
2. **(Optional)** Shut down your firewall. While not always necessary, this action maximizes your chance of a successful installation. If you keep your firewall running:
 - Ensure the port between the CA UIM system and the database system is open.
 - Specify a starting port during CA UIM installation (the recommended default is port 48000).
 - Ensure that an adequate range of ports are open (for example, ports 48000 through 48020). At a minimum, the first three ports assigned (controller, spooler, and hub) must be open. The port that is used for the distsrv probe communication is dynamically assigned.

NOTE

Restart the firewall and anti-virus software when installation is complete.

Localization Requirements

If the system is set to a language that is not English, the following error message appears during installation:

```
The database does not exist or could not be created.
```

To prevent this error, execute:

```
export LC_ALL=locale
```

Locale is the appropriate locale string (for example, *Norwegian*) for your language.

Swap Space Requirements

The system must be configured with either:

- 4 GB of swap space (minimum)
- 6 GB or more of swap space (recommended for optimal performance and reliability)

This requirement applies to both the CA UIM system and the Operator Console (OC) system.

Timezone Requirements

For data time-stamping to work correctly across a distributed UIM deployment, the UIM Server, the OC server, and the UIM database server must all be set to the same time zone, regardless of the geographic locations of the servers.

POSIX-Oriented Operating System Prerequisites

The `/etc/hosts` file on your system must map:

- 127.0.0.1 to localhost
- The system IP address to its hostname

Linux-Specific Prerequisites

The standard C++ Library must be present.

NOTE

The installer verifies that the minimum version requirement is met.

For some probes, the **compat-libstd** library is also required.

Security-Enhanced Linux

Security-Enhanced Linux (SELinux) is a Linux feature that supports access control security policies. While shutting down SELinux before installing UIM Server is not always necessary, doing so maximizes your chance for a successful installation.

If SELinux status is enabled, a **Current mode** of **permissive** is acceptable. Disabling SELinux entirely is an even safer approach.

If you must run UIM Server in SELinux **Enforcing** mode, add the CA UIM shared libraries to a safe list. After you install CA UIM, execute:

```
chcon -f -t textrel_shlib_t /<UIM_install>/hub/libldapssl.so.0
chcon -f -t textrel_shlib_t /<UIM_install>/hub/libldapsdk.so.0
chcon -f -t textrel_shlib_t /<UIM_install>/hub/libldapx.so.0
```

UIM_install is the directory where CA UIM is installed.

NOTE

After installation, CA UIM cannot function correctly in SELinux **Enforcing** mode until you add the CA UIM shared libraries to the safe list.

RHEL 7.4

If you are using RHEL 7.4, ensure that either the `fonts.local.conf` file is configured or the `dejavu-serif-fonts` package is installed. For more information, see the [RHEL Documentation](#).

Option 1: The `fonts.local.conf` file is configured. Create the `/etc/fonts/local.conf` file with the following contents:

```
<?xml version='1.0'?>
<!DOCTYPE fontconfig SYSTEM 'fonts.dtd'>
<fontconfig>
  <alias>
    <family>serif</family>
    <prefer><family>Utopia</family></prefer>
  </alias>
</fontconfig>
```

```

    <family>sans-serif</family>
    <prefer><family>Utopia</family></prefer>
</alias>
<alias>
    <family>monospace</family>
    <prefer><family>Utopia</family></prefer>
</alias>
<alias>
    <family>dialog</family>
    <prefer><family>Utopia</family></prefer>
</alias>
<alias>
    <family>dialoginput</family>
    <prefer><family>Utopia</family></prefer>
</alias>
</fontconfig>

```

Option 2: Run the yum install command to install the dejavu-serif-fonts package.

```
yum install dejavu-serif-fonts
```

Windows-Specific Prerequisites

The hub message queue is stored on disk and is constantly undergoing read and write activity. Because disk compression reduces I/O performance, CA UIM does not support compression on Windows.

This section includes the following information:

- Administrator Privileges
- Microsoft Windows User Account Control
- Write Privileges on Windows Server 2008

Administrator Privileges

UIM can only be installed by a user with administrator privileges.

Follow these steps:

1. In Windows, open **Administrative Tools > Services**
2. Right click on the Nimsoft Robot Watcher and select **Properties**.
3. Select the **Log On** tab.
4. Select the **This account** radio button.
5. Enter the account and password for an administrator.

Microsoft Windows User Account Control

Windows platforms newer than Windows XP and Windows 2003 use User Account Control (UAC). UAC prevents unauthorized modifications to your computer system.

If UAC is turned on, administrative privileges are required for CA UIM installation.

NOTE

Although we do not recommend it, you can turn off UAC. See your Windows documentation for details.

Write Privileges on Windows Server 2008

Write privileges are required for writing to the UIM program folder (default is C:\Program Files (x86)\Nimsoft) after installation. If you log in as a user without administrator privileges after installation, you must manually set these write privileges.

Install and Configure Your Database Software

This article describes the steps that are required to configure the CA UIM database before CA UIM installation. The following topics cover the information:

TIP

If you have questions regarding which database vendor software is supported with CA UIM, refer to the [Compatibility Support Matrix](#). For general database installation procedures, refer to the product documentation provided by your database vendor

Determine Your Database Creation Method

Determine the method that is used to create the UIM database before you run the UIM Server installer. Once you have chosen a creation method, follow the instructions for your database software.

Review the following information in this section:

- UIM Server Installer Creates the Database Schema
- Manual Creation of the Database Schema and User

UIM Server Installer Creates the Database Schema

The UIM Server installer can create the UIM database as part of the installation process. If you use this method, the UIM installer requires access to a database account with administrator privileges. Examples include:

- root in MySQL
- sa in Microsoft SQL Server
- SYS in Oracle

When you run the installer, enter the credentials for designated account.

If you use this installation method, skip the **Manual Creation of the Database Schema (or Tablespace) and User** section for your database software.

Manual Creation of the Database Schema and User

If you do not want to give the UIM Server installer access to an administrator account, you can create the UIM database and associated user manually. We recommend manual database creation in environments that have a dedicated Database Administrator. Before you install UIM Server, verify that the created user is the schema owner in Oracle or MySQL instances, or the Database Owner (DBO) in Microsoft SQL Server instances. Also, verify that the user is granted all permissions for the schema. If you create the database and user in advance, click **Use existing database** when prompted by the CA UIM installer.

WARNING

We recommend that you begin with a fresh database installation on a clean system. Using a pre-existing database can cause subtle configuration conflicts that are hard to diagnose.

Access Database-Specific Information

Access the appropriate section depending on your database:

- [Microsoft SQL Server](#)
- [MySQL Server](#)
- [Oracle](#)

Microsoft SQL Server

CA UIM supports only the full licensed product version with database authentication or Windows authentication for production environments. To obtain a copy of Microsoft SQL Server, go to www.microsoft.com/sqlserver and follow the installation instructions available with the download.

NOTE

Microsoft SQL Server is only supported for Windows UIM server installations.

NOTE

Both the Enterprise and Standard Editions of Microsoft SQL Server are supported with CA UIM. However, we generally recommend that you use the Enterprise Edition. CA UIM supports Always On availability groups for SQL Server high availability and disaster recovery.

Review the following information in this section:

Considerations

When installing Microsoft SQL Server, the simplest solution is to:

- Accept the default instance name when you install Microsoft SQL Server
- Use the default port (1433) when you install CA UIM
- Run the installer as the domain logon user to be associated with the UIM Server installation.

NOTE

Collations in Microsoft SQL Server provide sorting rules, case, and accent sensitivity properties for your data. Ensure that the collate option for the case is set to CI (Case Insensitive) for the UIM application.

Other solutions have different requirements. If you:

- **Use a non-default instance name for the Microsoft SQL Server:** Use the default port (1433) when installing CA UIM.
- **Use a port other than 1433 for CA UIM:** Use the default Microsoft SQL Server instance name.

During UIM server installation, you can select one of the following authentication options:

- **SQL Server with SQL Server login:** Provide the SQL Server user name and password during installation. No modifications are needed.
- **SQL Server with Windows authentication:** You might need to make database modifications in advance, as described in the next section.

The following limitations are applicable for the Standard Edition of Microsoft SQL Server:

- Table partitioning is not supported in the Standard Edition of Microsoft SQL Server. Therefore, the data maintenance jobs and the index maintenance jobs, which are scheduled from the data_engine probe UI, will not be effective because of the unsupported version.
- During the scheduled data maintenance job, the data is deleted in batches based on the values set in the data_engine configuration file. Ensure that enough space is available on the drive where the transaction log file is located to avoid space issues.
- During the table maintenance and the index maintenance, you must use the offline option in the data_engine UI before scheduling the index maintenance. The online index maintenance is not supported in the Standard Edition of Microsoft SQL Server.

Requirements for Windows Authentication

If you are also using Windows Authentication, review the following points:

- The database access account must be a domain account.
- The database access account must be in the Windows local administrators group on the UIM, OC, and CABI servers.
- The database access account must have sysadmin SQL permission on the MS SQL server during the installation (for database creation). Then, it can fall back to dbo to the CA_UIM database.
 - To enable the SA account and set the password, see <https://msdn.microsoft.com/en-us/library/ms188670.aspx>.
- Add the **Log on as a Service** permission on both the CA UIM system (UIM/OC/CABI servers) and the database system. For instructions, go to <http://technet.microsoft.com/en-us/library/dd277404.aspx>.
- Run the “Nimsoft Robot Watcher” service with the database access account.
- To configure SQL Server to use Windows authentication, see <http://msdn.microsoft.com/en-us/library/aa337562.aspx>.

NOTE

The user installing CA UIM must have the same administrative rights that were used to install the SQL Server. Specifically, the data_engine probe must have identical administrative rights on both the CA UIM system and the database system. These credentials are supplied during installation.

Manual Creation of the Database Schema and User

Manually create the Microsoft SQL Server database schema and user.

Follow these steps:

1. Log in to SQL Server Management Studio as the system administrator (sa).
2. Execute the following commands individually:

```
CREATE DATABASE <UIM_db_name>;
USE <UIM_db_name>;
CREATE LOGIN <UIM_db_user> with PASSWORD = '<UIM_db_password>', DEFAULT_DATABASE = <UIM_db_name>;
CREATE USER <UIM_db_user> FOR LOGIN <UIM_db_user>;
EXEC sp_addrolemember 'db_owner', <UIM_db_user>;
EXEC sp_addmessage @msgnum = 55000, @severity = 16, @msgtext = N'%', @replace = 'replace', @lang =
'us_english';
```

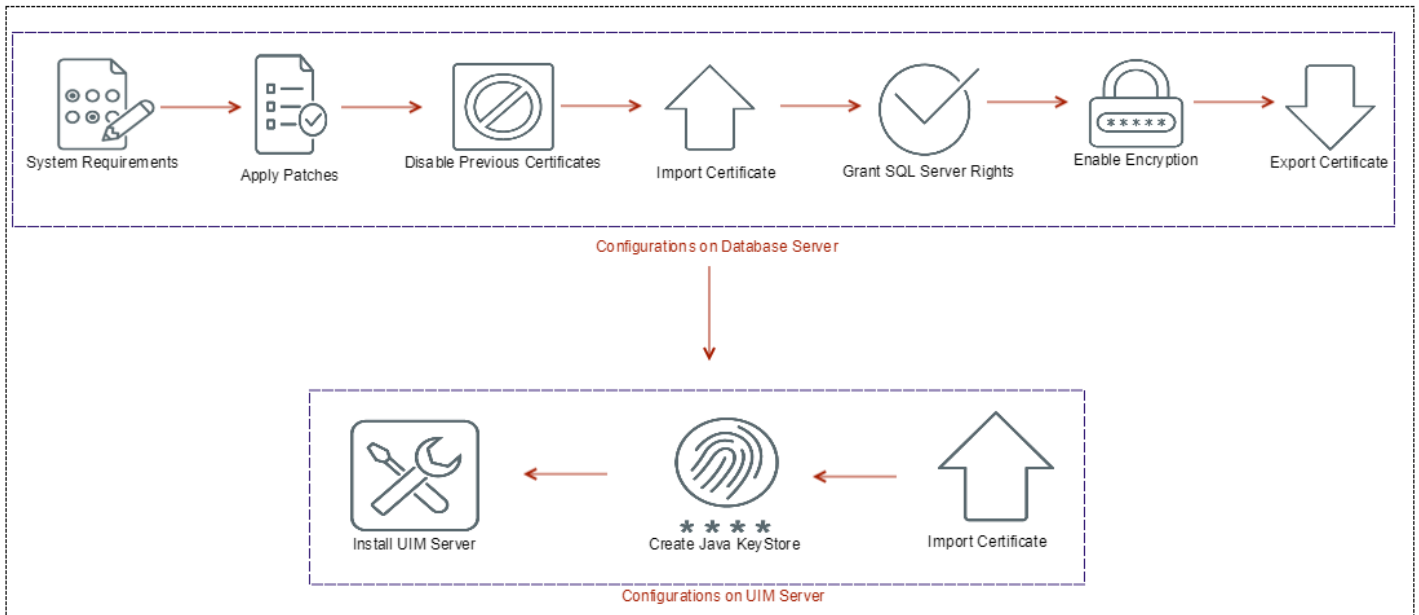
Support for TLS v1.2 (Microsoft SQL Server)

CA UIM supports Transport Layer Security (TLS) v1.2 when communicating with the UIM database: Microsoft SQL Server. This support enables the UIM Server to establish secure communication with the UIM database. To enable TLS v1.2 support for Microsoft SQL Server, ensure that you perform the required configurations on the Microsoft SQL Server computer (database server) and UIM Server (client computer).

The following Microsoft SQL Server versions are supported:

- 2012
- 2014
- 2016
- 2017
- 2019

The following diagram shows the high-level process:

Figure 4: Microsoft SQL Server TLS 1.2 Support**NOTE**

- CABI is not supported for Microsoft SQL Server 2017.
- The cabi 4.30 probe supports TLS v1.2 except if Microsoft SQL Server 2012, 2014, or 2016 is installed on Windows Server 2016.
- The cabi 4.10 probe supports TLS v1.2 when communicating with the UIM database: Microsoft SQL Server 2012, 2014, and 2016. However, CABI is not supported if Microsoft SQL Server 2012, 2014, or 2016 is installed on Windows Server 2016 and TLS v1.2 is enabled.
- The cabi 3.40 probe, available with UMP 9.0.2 HF2, supports TLS v1.2 when communicating with the UIM database: Microsoft SQL Server 2012 and 2014. However, CABI is not supported if Microsoft SQL Server 2012 or 2014 is installed on Windows Server 2016 and TLS v1.2 is enabled. For more information about how to apply the UMP 9.0.2 HF2 for CABI TLS functionality, see [UMP 9.0.2 HF2](#).
- The cabi 3.32 probe does not support TLS v1.2 when communicating with the UIM database: Microsoft SQL Server 2012, 2014, 2016, and 2017. As a result, you cannot view the Operator Console home page, OOTB CABI dashboards, and OOTB CABI reports.
- TLS v1.2 support is not enabled by default when you install CA UIM 9.0.2.

Configurations on Database Server

Perform the following tasks on the database server.

1. Verify FQDN Requirement
2. Verify and Apply Patches for Microsoft SQL Server
3. Disable Previous Versions of Certificates
4. Import the Certificate to Database Server
5. Grant SQL Server Rights to Use the Certificate
6. Enable Encryption on Database Server
7. Export the Certificate on Database Server

Verify FQDN Requirement

Verify that your full computer name is FQDN (for example, VI02-E74.ca.com). If not, add the domain name (for example, ca.com) to the computer name.

Follow these steps:

1. Access the properties panel of your computer (for example, right-click the Computer icon on your desktop and select **Properties**).
2. Click **Advanced system settings** in the left pane.
3. Click the **Computer Name** tab.
4. Click **Change**.
5. Click **More**.
6. Enter your domain name in the **Primary DNS suffix of this computer** field.
7. Click **OK** and restart the computer.
8. Verify that your full computer name is now FQDN.

The following example screenshot shows that the full computer name is FQDN:



Verify and Apply Patches for Microsoft SQL Server

For Microsoft SQL Server versions that do not provide support for TLS v1.2 by default, follow the information in the article [TLS 1.2 support for Microsoft SQL Server](#). By following the instructions in this article, you can download and apply the required packages depending on your Microsoft SQL Server version. For Microsoft SQL Server versions (for example, 2016) that support TLS v1.2 by default, you do not need to perform this manual process.

Disable Previous Versions of Certificates

Change the registry keys to disable all the previous versions of certificates on the database server. Verify the following registry keys on the database server:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server

For the Client and Server entries, enter the following DWord and Value entries:

- DisabledByDefault=00000000
- Enabled=00000001

For more information, see the TLS 1.2 section on [TLS/SSL Settings](#).

Import the Certificate to Database Server

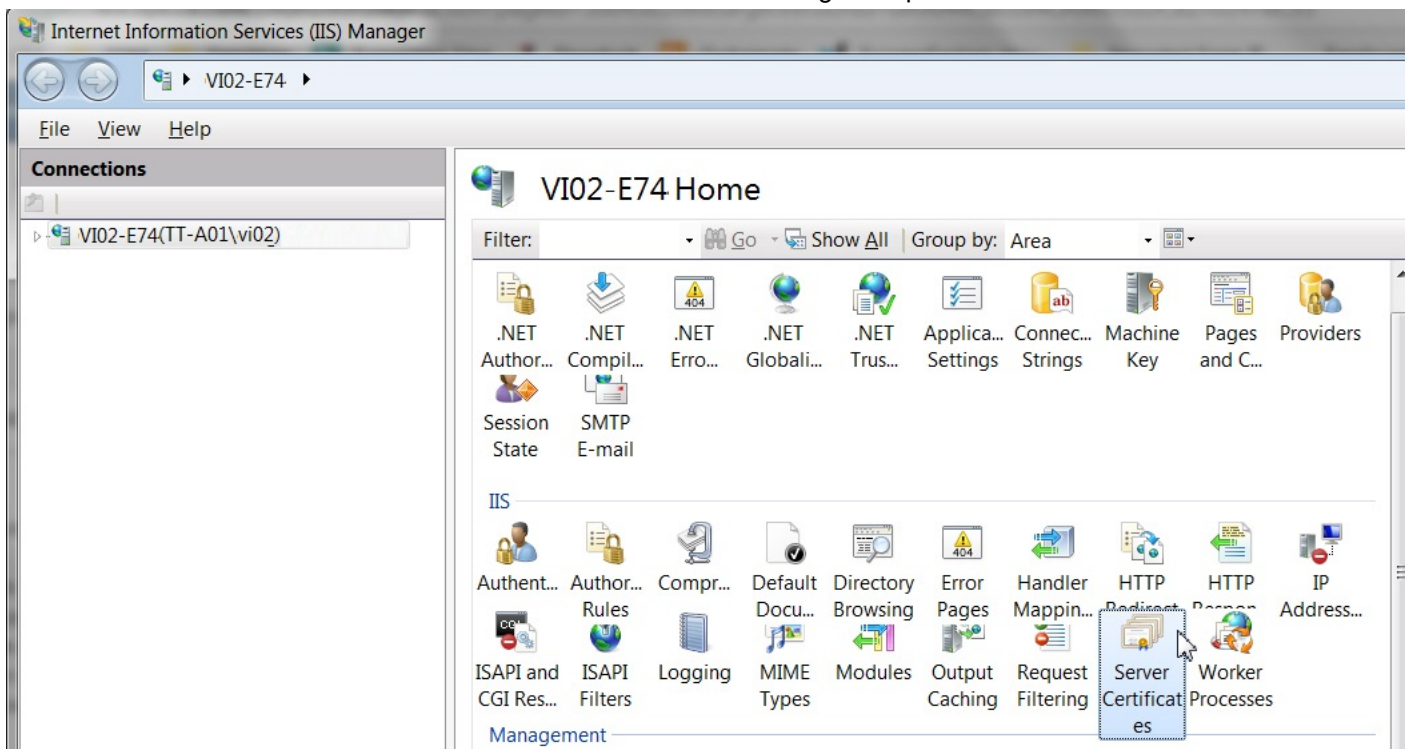
(For certification authority-approved certificates) Use Internet Information Services (IIS) to import the CA-approved certificate to the database server. Ensure that you have the required certificate available with you.

NOTE

Install IIS on the database server if it is not already installed.

Follow these steps:

1. Click Start, Run, and enter inetmgr to open IIS.
2. Click **<server_name>**.
3. Locate and double-click **Server Certificates** as shown in the following example screenshot:



4. Right-click in the right pane and select **Import** from the context menu. The **Import Certificate** dialog opens.
5. Navigate to the location where your certificate file is available.
6. Enter the required password.
7. Click **OK**.

The certificate is imported to the database server. The following example screenshot shows an imported certificate:



Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

| Name | Issued To | Issued By | Expiration Date |
|---------|-----------------|-----------------|---------------------|
| Testing | VI02-E74.ca.com | VI02-E74.ca.com | 2/7/2019 5:30:00 AM |

NOTE

When using certificates, the certificate must be issued to FQDN (Fully Qualified Domain Name) of the computer, not the host name. Also, ensure that the database server name must also be FQDN. If both the certificate and the server name are not FQDN, you will encounter connection issues.

The import procedure explained above is not required for self-signed certificates. When you create self-signed certificates using IIS, they become available in IIS. Therefore, you do not need to perform this import process.

Create Self-Signed Certificates Using IIS

Review the following steps if you want to create a self-signed certificate using IIS:

1. Verify that your full computer name is FQDN (for example, sa-01.ca.com). If not, follow the steps that are mentioned in the System Requirements section.
2. Click Start, Run, and enter inetmgr to open IIS.
3. Click **<server_name>**.
4. Locate and double-click **Server Certificates**.
5. Right-click in the right pane and select Create Self-Signed Certificate from the context menu.
6. Enter the FQDN name (for example, <computer_name>.ca.com) for the certificate.
7. Click **OK**.

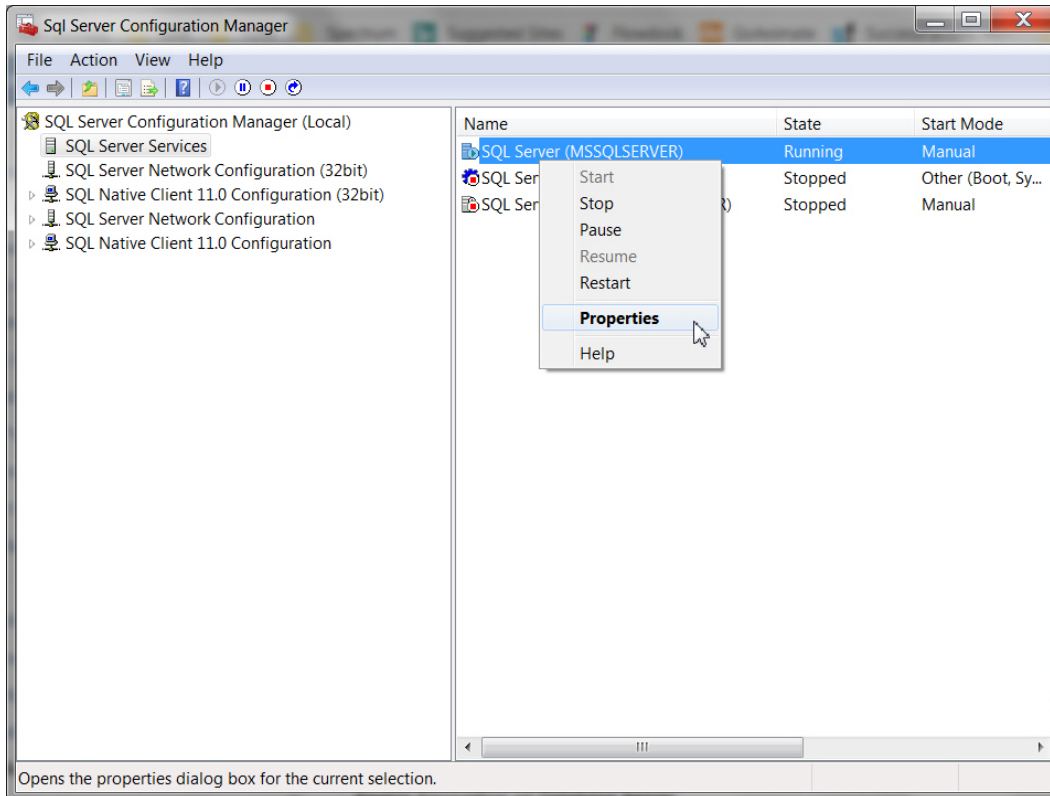
The self-signed certificate is created and is listed in the **Server Certificates** pane.

Grant SQL Server Rights to Use the Certificate

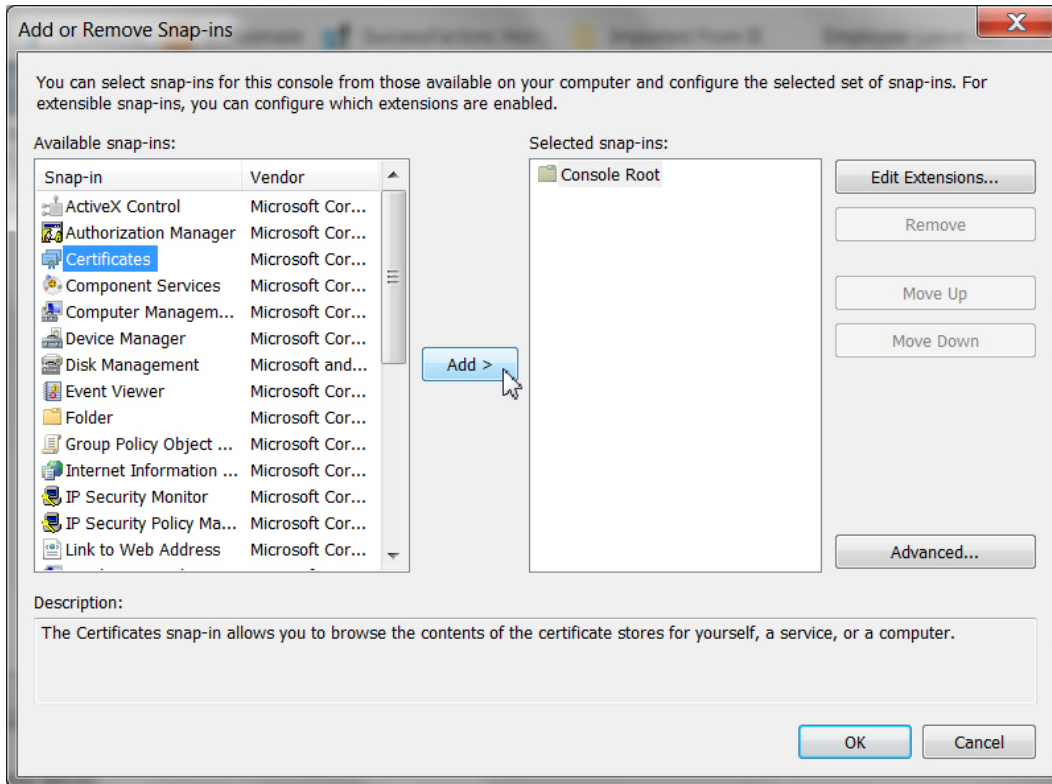
You must provide the SQL Server rights to use the certificate. You use SQL Server Configuration Manager and Microsoft Management Console to perform this task.

Follow these steps:

1. Open SQL Server Configuration Manager.
2. Locate and select **SQL Server Services** in the left pane.
3. Select your SQL Server instance in the right pane.
4. Right-click SQL Server instance and select **Properties** from the context menu as shown in the following screenshot:



5. Copy the account name entry present in the **Account Name** field.
6. Open the Microsoft Management Console (MMC).
7. Click **File, Add/Remove Snap-in**.
8. Click **Certificates**.
9. Click **Add** as shown in the following example screenshot:



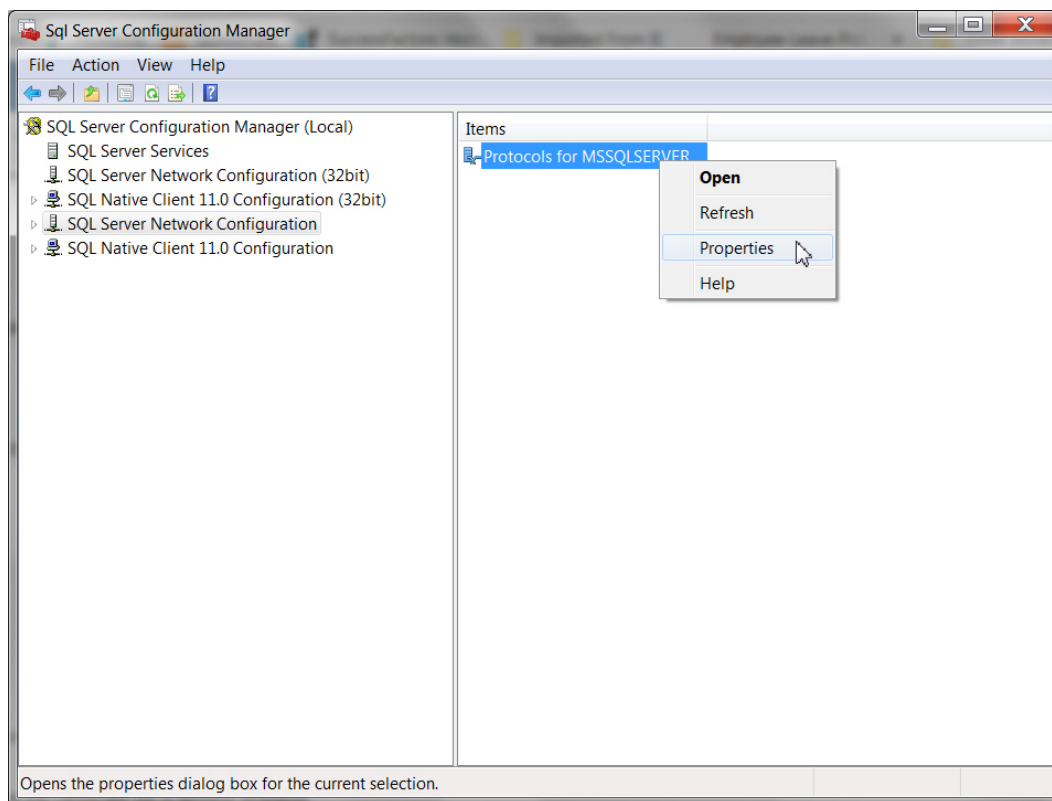
10. Select **Computer account**.
11. Click **Next**.
12. Select the local computer option.
13. Click **Finish**.
14. Click **OK**.
15. Locate and select the certificate.
16. Right-click the certificate, select **All Tasks, Manage Private Keys** from the context menu.
17. Add the copied account name.
18. Grant the Read access to the account name.

Enable Encryption on Database Server

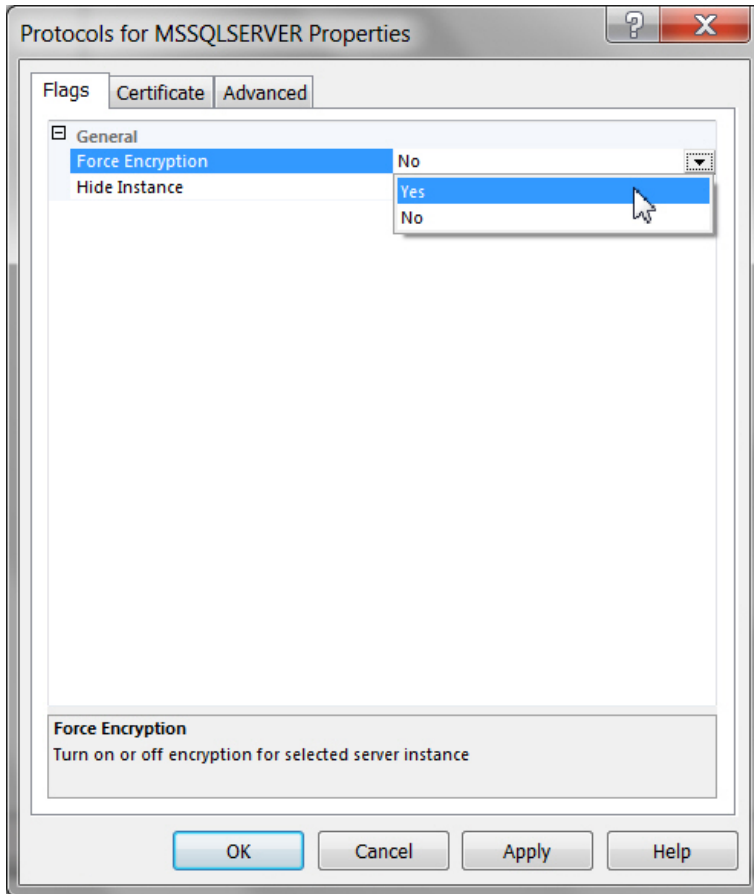
Use the SQL Server Configuration Manager to enable the encryption on the database server.

Follow these steps:

1. Open SQL Server Configuration Manager.
2. Locate and expand **SQL Server Network Configuration**.
3. Right-click on **Protocols for <SQL_Server>** and select **Properties** from the context menu as shown in the following example screenshot:



4. Click the **Certificate** tab.
5. Select the required certificate from the **Certificate** drop-down list.
6. Click the **Flags** tab.
7. Select **Yes** for the **Forced Encryption** option as shown in the following example screenshot:



8. Click **OK**.
 9. Restart the SQL Server service.
- The encryption is enabled on the database server for the certificate.

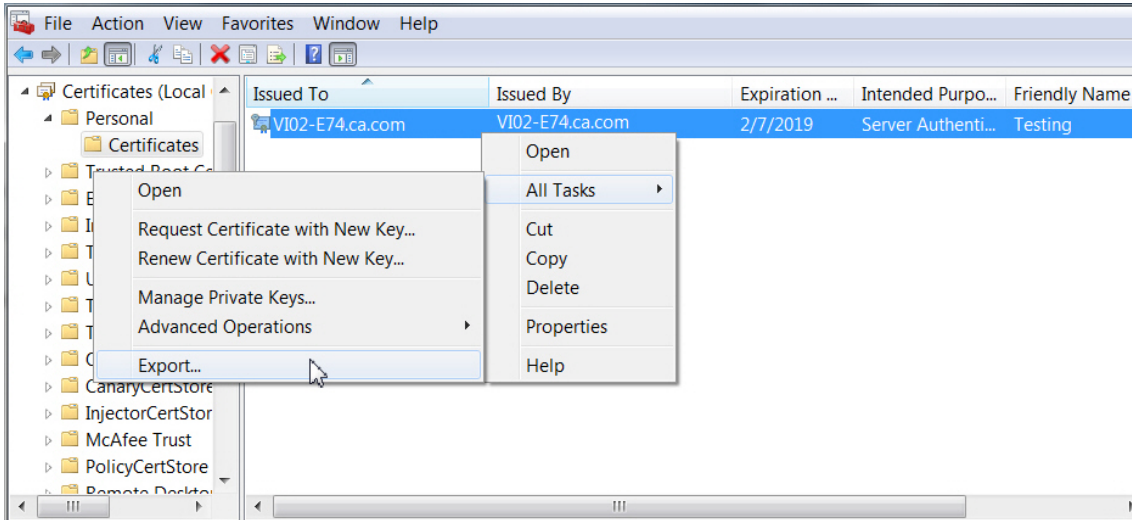
Export the Certificate from Database Server

(For self-signed certificates) Export the self-signed certificate to the database server so that the UIM Server (client in this case) can use it. The UIM Server (client) must trust the certificate that is available on the database server.

You do not need to perform this task in case of CA-approved certificates because the certificate file is already available.

Follow these steps:

1. Open the Microsoft Management Console (MMC).
2. Click **File, Add/Remove Snap-in**.
3. Click **Certificates**.
4. Click **Add**.
5. Select **Computer account**.
6. Click **Next**.
7. Select the local computer option.
8. Click **Finish**.
9. Click **OK**.
10. Locate the certificate.
11. Right-click the certificate and select **All Tasks, Export** from the context menu as shown in the following screenshot:



12. Click **Next** on the Certificate Export Wizard.

13. Follow the required selections for **Base-64 encoded X.509 (.CER)** and specify the location where you want to save the exported file. The location must be accessible to the UIM Server (client computer).

The self-signed certificate is successfully exported to a location on the database server that is accessible to the UIM Server.

You have successfully configured your UIM database server for the TLS v1.2 support.

Configurations on UIM Server

Perform the following tasks on the client (UIM Server).

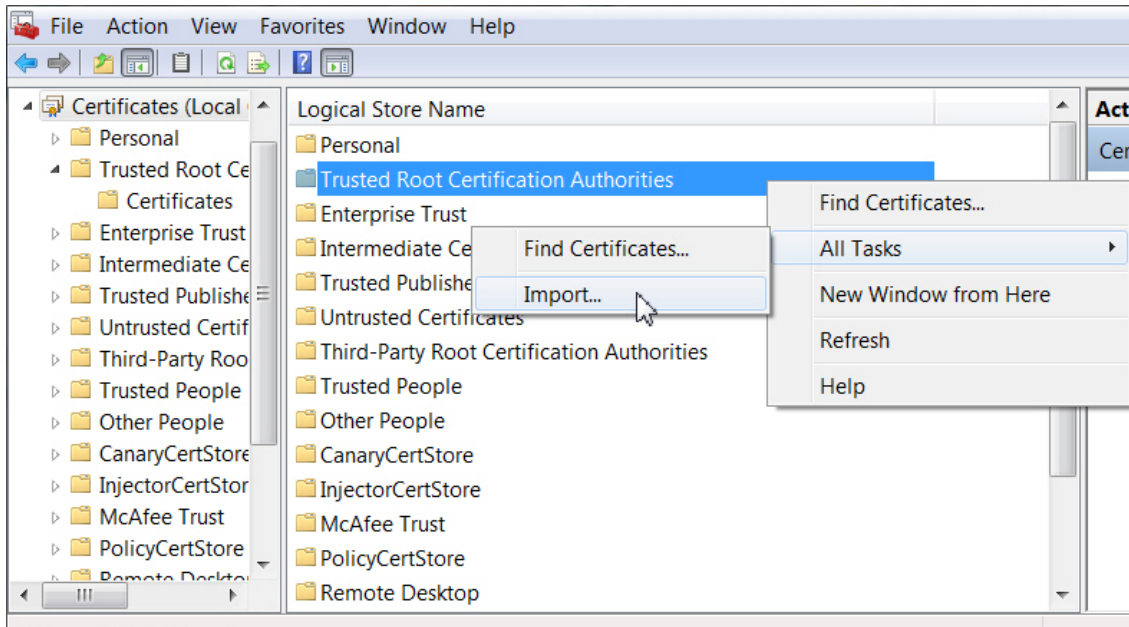
1. Import the Certificate on UIM Server
2. Create Java KeyStore for Server Certificate
3. Install UIM Server

Import the Certificate on UIM Server

Import the certificate on the UIM Server (client computer). This step is required to ensure that the UIM Server can trust the certificate that is available on the database server. You must import the certificate into the Trusted Root Certification Authorities certificate store on the UIM Server.

Follow these steps:

1. Open the Microsoft Management Console (MMC).
2. Click **File, Add/Remove Snap-in**.
3. Select **Certificates** and click **Add**.
4. Select **Computer account**.
5. Select the local computer option.
6. Click **Finish**.
7. Click **OK**.
8. Click **Certificates (Local Computer)**.
9. Navigate to the **Trusted Root Certification Authorities** folder.
10. Right-click the **Trusted Root Certification Authorities** folder and select **All Tasks, Import** from the context menu as shown in the following screenshot:



11. Click **Next** on the Certificate Import Wizard.
12. Click **Browse** and navigate to the location where you saved the certificate file.
13. Click **Next**.
14. Verify that **Trusted Root Certification Authorities** is selected as the place to store all certificates.
15. Click **Finish**.
16. Click **OK**.

The certificate is imported on the UIM Server (client computer) as a trusted certificate.

NOTE

You must also import the certificate onto the robot where CABI is available. After the import, deactivate and activate CABI.

Create a .jks File for Server Certificate

You also need to create a .jks file (Java keystore file) on the UIM Server to store the server certificate. The .jks file, when created, includes your database server certificate. You can use Java keytool, which is a key and certificate management tool, to generate your .jks file. The tool stores the keys and certificates in a store called keystore.

NOTE

You specify the location of the generated .jks file during the UIM Server installation. The UIM Server installer copies the .jks file from the specified location and places it in the <Nimsoft>\security folder during the installation. The installer then renames the copied file to truststore.jks.

Follow these steps:

1. Ensure that JRE (jre1.8.0) is installed on the computer.
2. Specify the JRE location in the `PATH` environment variable; for example, `C:\Program Files\Java\jre1.8.0_131\bin;`
3. Run the following command using the .cer certificate to generate the .jks file:
Syntax: `keytool -import -alias <alias_name> -file <certificate_file> -keystore <jks_filename> -storepass <password>`
Example: `C:\keytool -import -alias sa-01.ca.com -file sa-01.ca.com.cer -keystore sa-01.ca.com.jks -storepass Abc@123`

4. Enter *yes* when prompted whether you want to trust the certificate.
The .jks file is created.

This command uses the following options:

- `-file`
Specifies the location where the source certificate file is available.
- `-keystore`
Specifies the location where you want to save the .jks file that gets created when the command is executed successfully.
- `-storepass`
Specifies the password for the .jks file.
- `-alias`
Specifies the alias name, which is the database server name (FQDN) in this case.

If your certification authority (CA) provides you a .p12 file, you can use the following command to import it into the .jks file:

Syntax: `keytool -importkeystore -srckeystore <certificate_filename> -srcstoretype <type> -srcstorepass <password> -destkeystore <jks_filename> -deststorepass <password> -alias <alias_name>`

Example: `C:\keytool -importkeystore -srckeystore sa01-i185.ca.com.p12 -srcstoretype PKCS12 -srcstorepass Abc@123 -destkeystore sa01-i185.ca.com.jks -deststorepass Abc@123 -alias sa01-i185.ca.com`

The command uses the following options:

- `-srckeystore`
Specifies the location where the self-signed or CA-approved certificate file is available.
- `-srcstoretype`
Specifies the source type.
- `-srcstorepass`
Specifies the password that is associated with the source certificate file.
- `-destkeystore`
Specifies the location where you want to save the .jks file that gets created when the command is executed successfully.
- `-deststorepass`
Specifies the password for the .jks file.
- `-alias`
Specifies the alias name, which is the database server name (FQDN) in this case.

NOTE

- Certificate name and database server name must be FQDN.
- Before you deploy CABI External version 3.4 on a secondary robot, copy the Java keystore file (truststore.jks) file from the UIM Server (<Nimsoft>\security) to the CABI External secondary robot (<Nimsoft>\security).

Install UIM Server

After you perform all the tasks that are listed in this section, review the other pre-installation planning tasks. You can then start the UIM Server installation. During the installation, ensure that you enable the TLS v1.2 option and provide the required information. The UIM Server installer automatically installs the required driver (SQLNCLI11) on the computer during the installation. Also, for the .jks file, browse to the location where you have created the .jks file. The installer copies that file to the <Nimsoft>\security folder as truststore.jks.

For more information about the UIM Server installation, see [Install UIM Server](#) and [Installation Parameters](#). The following screenshot shows the TLS v1.2 options (**Enable TLS**, **Trust Store Path**, and **TrustStore Password**) during the UIM Server installation:

CA UIM Server 9.0.2

Database Configuration

Select your database provider, enter the field data, and click Test. Any modifications require the test to be performed again.

Microsoft SQL Server

Database Creation Mode: Create New Database ?

Database Server Hostname or IP: e7440 ?

Database Server Port: 1433 ?

Database Name: CA_UIM ?

Database Authentication Mode: SQL Server Authentication ?

Database Username: sa ?

Database Password: ●●●●●●●● ?

Enable TLS: ?

Trust Store Path: C:\certificate\certificates.jks ?

TrustStore Password: ●●●●●● ?

The TLS v1.2-related options are as follows:

- **Enable TLS:** Select the option to enable TLS v1.2 in CA UIM, which lets the UIM Server establish a secure communication with the UIM database (Microsoft SQL Server in this case).
- **Trust Store Path:** Specify the location of the generated .jks file. The UIM Server installer copies the .jks file from the specified location and places it in the <Nimsoft>\security folder during the installation. The installer then renames the copied file to truststore.jks. This file includes your database server certificate.
- **TrustStore Password:** Specify the password to access the source .jks file.

You have successfully enabled the TLS v1.2 support, which allows secure communication with the UIM database (Microsoft SQL Server).

Additional Information

Review the following additional information:

- In upgrade scenarios and in situations where you want to enable TLS v1.2 support after the UIM Server installation, perform the following tasks on the UIM Server:
 - a. Verify and install the required driver (SQLNCLI11), if necessary.
For more information, follow the information in the "Client component downloads" section in the article [TLS 1.2 support for Microsoft SQL Server](#).
 - b. Import the server certificate as a trusted certificate.
 - c. Create the Java KeyStore.
 - d. Use the data_engine [Admin Console](#) or [Infrastructure Manager](#) to configure the TLS v1.2-related parameters. When specifying the .jks file location, browse to the location where you have created the .jks file. When you click **Apply** or **OK**, the .jks file is copied to the <Nimsoft>\security folder as truststore.jks. This location is then

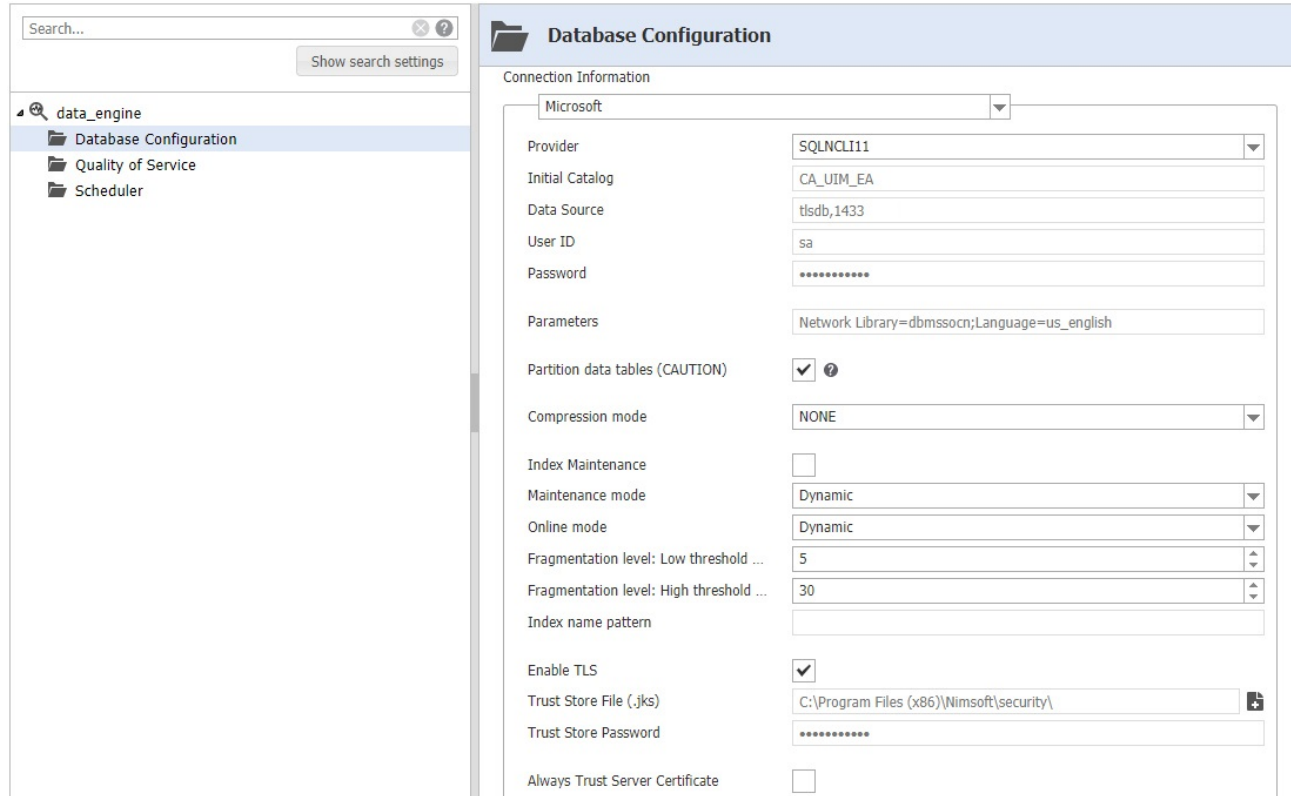
displayed in the **Trust Store File (.jks)** field. When you click the **Test Connection** option, CA UIM does not verify the validity of the specified .jks file. Instead, it verifies the validity of the certificate that you have imported into the Microsoft Management Console (MMC) on the UIM Server.

After specifying the options, restart the data_engine probe. The data_engine probe is successfully configured to support TLS v1.2. You can now deploy other probes and use the secure communication when interacting with the UIM database (Microsoft SQL Server). Also, review the impacted probes and packages list. These items have been updated to support TLS v1.2. Ensure that you use the latest version of these items if you want them to work in the TLS v1.2 environment.

NOTE

Ensure that the ppm probe version is 3.48 or later and robot version is 7.96 or later to display TLS v1.2 configuration options in Admin Console. Otherwise, TLS v1.2 options are not displayed in Admin Console.

The following screenshot shows the TLS v1.2 configuration options (**Enable TLS, Trust Store File (.jks), Trust Store Password, Always Trust Server Certificate**) in Admin Console:



- For upgrade scenarios, the CA UIM system can be either TLS v1.2 enabled or disabled for all components; it cannot be a partial TLS v1.2-enabled system. That is, all the infrastructure components across layers (for example, primary hub, secondary hub, probes) should be upgraded to TLS v1.2-supported version.
- You can enable or disable the TLS v1.2 mode by configuring the data_engine UI. Also, restart of data_engine is needed whenever TLS v1.2 mode is changed.
- If you upgrade from a previous version of CA UIM to this version, the state of the system remains in non-TLS v1.2 mode. To enable TLS v1.2 mode, perform all the required manual steps that are mentioned above and use the data_engine UI to enable TLS v1.2.
- When you want to update a certificate (for example, older certificate has expired), create a new .jks file and specify the location of the .jks file and its password in the data_engine UI. The data_engine probe uses that information to create the truststore.jks file in the same <Nimsoft>\security folder.
- To run probes that can work on remote computers (other than the primary hub) in TLS v1.2 environment, install the required driver (SQLNCLI11) on the remote computers. For more information, follow the information in the "Client component downloads" section in the article [TLS 1.2 support for Microsoft SQL Server](#).
- If you encounter any database-connectivity issue in a TLS v1.2-enabled environment, the most probable reason for this issue might be that your certificate is not using FQDN.

Probes and Packages Updated for TLS v1.2

TLS v1.2 related updates have been made to the following items so that they can work in a TLS v1.2 environment. These are the minimum versions with the TLS v1.2 related updates.

- ace 9.03
- alarm_routing_service 10.20
- apmgwtw 3.20
- audit 9.03
- axagateway 1.32
- cisco_ucm 2.00
- cm_data_import 9.02
- data_engine 9.02
- discovery_agent 9.02
- discovery_server 9.02
- ems 10.20
- hub 7.96
- maintenance_mode 9.02
- mon_config_service 9.02
- mpse 9.03
- nas 9.03
- nis_server 9.03
- qos_processor 9.02
- robot 7.96
- sla_engine 9.02
- telemetry 1.20
- trellis 9.02
- udm_manager 9.02
- usage_metering 9.11
- wasp 9.02
- webservices_rest 9.02

Troubleshooting

The following topics help you troubleshoot a few TLS v1.2-related issues:

data_engine Fails to Start When TLS v1.2 is Enabled

Symptom: When I try to start data_engine after enabling the TLS v1.2 mode, I get the following connection error:

```
May 1 10:10:21:897 [4068] 0 de: [main] Open - 3 errors
May 1 10:10:21:897 [4068] 0 de: (1) Open [Microsoft SQL Server Native Client 11.0]
  Invalid connection string attribute
May 1 10:10:21:897 [4068] 0 de: (2) Open [Microsoft SQL Server Native Client 11.0] SSL
  Provider: The target principal name is incorrect.

May 1 10:10:21:897 [4068] 0 de: (3) Open [Microsoft SQL Server Native Client 11.0]
  Client unable to establish connection
May 1 10:10:21:897 [4068] 0 de: COM Error [0x80004005] Unspecified error - [Microsoft
  SQL Server Native Client 11.0] Invalid connection string attribute
May 1 10:10:21:897 [4068] 1 de: Database script - processing 3 database scripts
```

How can I address this issue?

Solution: Your data source uses FQDN for connecting to the database server in the data_engine configuration, but your certificate is not created with FQDN. In such scenarios, the certificate validation fails. Ensure that both the database server name and the certificate use FQDN.

Self-Signed SSL Certificate for Microsoft SQL Server Fails to Validate

Symptom: I used self-signed certificate the local KeyStore, but I received the following error:

```
2018-04-30 15:12:15,379 ERROR
dbconfig.UIMServerDatabaseConfigBaseParamsPanel:processTestDBAccess:152 [AWT-
EventQueue-0] -
Failed to connect to database server with provided field values. Recheck fields for
accuracy.
The driver could not establish a secure connection to SQL Server by using Secure Sockets
Layer
(SSL) encryption. Error: "java.security.cert.CertificateException: Failed to validate
the server
name in a certificate during Secure Sockets Layer (SSL) initialization.".
ClientConnectionId:89ef826a-2460-4faa-ala8-d8aba2fc28f2 (501) , Failed to connect to
database
server with provided field values. Recheck fields for accuracy.
```

How can I resolve this issue?

Solution: This issue is the same as described in the first troubleshooting topic "data_engine Fails to Start When TLS v1.2 is Enabled". Therefore, follow the same solution of ensuring that the database server name and the certificate use FQDN.

MySQL Server

CA UIM 9.0.2 and above supports only a commercial version of the MySQL database software. Obtain a copy of the commercial version from the [MySQL](#) website.

Review the following information in this section:

- [MySQL Server Variables](#)
- [View the Variable Setting](#)
- [MySQL in Large Environments](#)
- [Manual Creation of the Database Schema and User](#)

MySQL Server Variables

MySQL variables must be set as follows:

- **lower_case_table_names=1**
- **local_infile=ON**
- **table_definition_cache=2000**
- **innodb_file_per_table=0**
- **max_connections = 1000**
- **location** = default location of my.cnf or my.ini configuration
 - In Linux, default location of my.cnf file is /etc/my.cnf
 - In Windows, to get the location of my.ini
 - go to->Services.msc->mysqld service->properties->default-fil
- **session** = the session in which these variables need to be set are under mysqld process : [mysqld]

NOTE

If you have a replication server configuration, the variable "gtid-mode" should be set to "OFF" and the variable "enforce-gtid-consistency" should be set to "0" in my.cnf or my.ini configuration as below:

```
gtid-mode=off
enforce-gtid-consistency=0
```

Enable the binary logs only if you use a backup or replication service, which requires the binary log files. To do so, set the following variables:

- **log_bin**

WARNING

The status of the system variable `log_bin` specifies whether the binary log is enabled. The `--log-bin [=base_name]` command-line option enables the binary logging. When you set the `--log-bin` option, the `log_bin` system variable is set to **ON**, not to the base name. The binary log file name is present in the `log_bin_basename` variable. For more information, see your MySQL documentation.

- **log_bin_trust_function_creators=ON** (if `log_bin` is enabled)
- **binlog_format=mixed** (if `log_bin` is enabled)
- **expire_logs_days=<number of days after which to remove binary log files>** (if `log_bin` is enabled)

View the Variable Setting

Use the following procedure to view the setting for each variable.

Follow these steps:

1. Log in to the MySQL server as the administrator.
2. For each variable, execute:


```
show variables like 'variable_name';
```
3. If a variable is incorrect or missing, edit the MySQL server configuration file as instructed in your MySQL documentation.
4. Restart the database if you made any changes,

MySQL in Large Environments

If you are preparing for a large-scale or major deployment, you can change more database parameters to allow for greater demands of such an environment. We recommend that you begin with the values shown in the following example, and then fine-tune settings depending on your circumstances.

As the MySQL administrator, add these lines to the MySQL server configuration file:

```
[mysqld]
max_heap_table_size=134217728
query_cache_limit=4194304
query_cache_size=268435456
sort_buffer_size=25165824
join_buffer_size=67108864
max_tmp_tables=64
```

Manual Creation of the Database Schema and User

Manually create the MySQL database schema and user.

Follow these steps:

1. Log in as the MySQL administrator.

2. Create the database. Execute:

```
CREATE DATABASE IF NOT EXISTS <uim_db_name> DEFAULT CHARACTER SET = utf8 DEFAULT COLLATE =
utf8_unicode_ci;
```

Where *<uim_db_name>* is the desired database name

3. Create the user and assign required privileges. Execute:

```
CREATE USER '<uim_db_owner>'@'%' IDENTIFIED BY '<uim_db_owner_password>';
GRANT ALL PRIVILEGES ON <uim_db_name>.* TO 'uim_db_owner'@'%';
FLUSH PRIVILEGES;
```

Where *uim_db_owner* is the desired user name for the owner, *uim_db_owner_password* is the desired password, and *uim_db_name* is the name of the database you created.

NOTE

The single-quotation marks (') are required.

Oracle

This section includes information about how to perform appropriate settings for the Oracle database.

Review the following information in this section:

NOTE

CA UIM requires a back-end database to store performance data and events. When CA UIM performance data is stored in an Oracle database, it executes PL/SQL blocks; for example, stored procedures, functions, and triggers. The execution requires DBA privilege be given/granted explicitly to the CA_UIM user. Granting the privilege through a *role* will NOT work because of an Oracle database limitation. For more information about this Oracle database limitation, see [How Roles Work in PL/SQL Blocks](#).

Install Oracle Instant Client

The Oracle Instant Client must be installed on the CA UIM system so it can access the Oracle database.

Follow these steps:

1. Go to www.oracle.com and download the zip file for the **Instant Client Package - Basic SQL *Plus Package** (use version 12.x.x.x or 19.x.x.x.x).
2. Install the Instant Client according to the instructions in the [Installation guide](#) on the Oracle web site. The UIM installer asks for the location of the Instant Client.
3. Please make sure that you have downloaded SQL *Plus package and verify if you are able to connect with net service name to Oracle Server to avoid any errors during UIM installation.
4. Restart the system.

Set the Configuration Parameters

The Oracle administrator must also set the following required configuration parameters before installing CA UIM.

Follow these steps:

1. As the Oracle database administrator, execute:


```
ALTER SYSTEM SET PROCESSES = 300 SCOPE=SPFILE;
ALTER SYSTEM SET SESSIONS = 335 SCOPE=SPFILE; -- 1.1 * PROCESSES +5
ALTER SYSTEM SET OPEN_CURSORS = 500 SCOPE=BOTH;
```
2. Restart the database.

Grant Permission

As the Oracle database administrator, execute the following command to grant permission to the CA UIM user:

```
Grant execute on DBMS_CRYPTO TO <UIM_USER>;
```

Configure Settings for Oracle Shared Server

If your Oracle database is configured for shared server use, you can increase the total number of allowed shared server sessions using the **SHARED_SERVER_SESSIONS** parameter. Generally, we recommend increasing the **SHARED_SERVER_SESSIONS** to 300 as a starting point.

WARNING

The error message **ORA-00018: maximum number of sessions exceeded** during UIM installation indicates that the number of allowed shared server sessions should be increased.

(OC Only) Turn off the Oracle Recycle Bin

If you will install the Operator Console (OC), then the recycle bin must be turned off before you install UIM Server.

Follow these steps:

1. Use a tool such as SQL Developer to connect to the Oracle database.

2. Enter the following commands:

```
ALTER SYSTEM SET recyclebin = OFF DEFERRED;
ALTER SESSION SET recyclebin = off;
```

3. Verify that the recycle bin is off using the following command:

```
show parameter recyclebin;
```

NOTE

We do not recommend turning the Oracle Recycle Bin back on after installing OC.

Verify Linking for Shared Oracle Libraries on Unix Systems

Shared Oracle libraries on Unix-based systems must be linked.

Follow these steps:

1. Go to the Instant Client.

2. Execute:

```
ldd libociei.so
```

3. Verify that there are links for all the libraries and that there are no **not found** messages. The output should look similar to the following:

```
linux-vdso.so.1 +> (0x00007fff5b0e2000)
libclntsh.so.11.1 => /root/instantclient_11_1/libclntsh.so.11.1 (0x00007f36030b3000)
libdl.so.2 => /lib64/libdl.so.2 (0x00007f3602eae000)
libm.so.6 => /lib64/libm.so.6 (0x00007f3602c57000)
libpthread.so.0 +> /lib64/libpthread.so.0 (0x00007f3602a3a000)
libnsl.so.1 => /lib64/libnsl.so.1 (0x00007f3602821000)
libc.so.6 => /lib64/libc.so.6 (0x00007f36024c1000)
libnnz11.so => /root/instantclient_11_1/libnnz11.so (0x00007f3602064000)
libaio.so.1 => /lib64/libaio.so.1 (0x00007f3601e61000)
/lib64/ld-linux-x36-64.so.2 (0x00007f360a0a0000)
```

Manual Creation of the Tablespace and User

The procedure for creating a tablespace manually depends on the version of Oracle that you are using.

Oracle 12c or higher

Create a pluggable database using the files of a seed database. See the [Oracle documentation](#) for details about the options available when you create a database from a seed.

Follow these steps:

1. Log in to the Oracle database as the administrator (sys as sysdba).
2. Connect to the pluggable database using

```
sys as sysdba
```

The service name for the connection is the pluggable database name where you would like to create your user and tablespace.

3. Create the tablespace. Execute the following statement, where *ts_name* is a tablespace name of your choice (typically, *CA_UIM*):

```
create tablespace ts_name datafile 'ts_name.dbf' size 1000m autoextend on maxsize
unlimited;
```

4. Create the owner and assign the required privileges. Execute the following statement, where *db_owner* is the name of the user to create, and *ts_name* is the tablespace:

```
create user db_owner IDENTIFIED BY owner_password DEFAULT TABLESPACE ts_name;
grant unlimited tablespace to db_owner;
grant administer database trigger to db_owner;
grant create table to db_owner;
grant create view to db_owner;
grant alter any table to db_owner;
grant select any table to db_owner;
grant create sequence to db_owner;
grant create procedure to db_owner;
grant create session to db_owner;
grant create trigger to db_owner;
grant create type to db_owner;
grant select on sys.v_$session to db_owner;
grant execute on sys.dbms_lob to db_owner;
grant execute on dbms_redefinition to db_owner;
grant create any table to db_owner;
grant drop any table to db_owner;
grant lock any table to db_owner;
```

- The owner and the tablespace commonly have the same name.
- The *grant unlimited tablespace* command sets the quota for all tablespaces to unlimited. To set the quota for only the UIM database, execute the following statement in place of *grant unlimited tablespace*. This configuration has not been tested.

```
alter user db_owner quota unlimited on ts_name
```

5. Start the UIM Server installer. When you are prompted, enter the following information:

- – **Service Name:** Name of the pluggable database instance, *pdb_name*, you created
- **Port:** Port of the Oracle database
- **Username:** Username for the local user, *non_admin_user*

Your database server is ready.

Oracle Real Application Clusters (Oracle RAC)

You can install CA UIM against Oracle RAC. This is a clustered version of Oracle Database based on a comprehensive high-availability stack that can be used as the foundation of a database cloud system as well as a shared infrastructure, ensuring high availability, scalability, and agility for any application.

Follow these steps:

1. Install Oracle Instant Client
2. Set Configuration Parameters
3. Configure Settings for Oracle Shared Server
4. Manually create the tablespace and user.
5. During the CA UIM installation, select "Use Existing Database". Ensure that you keep only one Oracle RAC node alive during the CA UIM installation time. If you have multiple Oracle RAC nodes running during the CA UIM installation, the installation fails. Check the log to review the error messages.

Install Oracle Instant Client

The Oracle Instant Client must be installed on the CA UIM system so it can access the Oracle database.

Follow these steps:

1. Go to www.oracle.com and click **Downloads, Instant Client**.
2. Click the link for the operating system and hardware of your system.
3. Download the zip file for the **Instant Client Package - Basic**.
4. Install the Instant Client according to the directions on the web site. The UIM installer asks for the location of the Instant Client.
5. Restart the system.

Set Configuration Parameters

The Oracle administrator must also set the following required configuration parameters before installing CA UIM.

Follow these steps:

1. As the Oracle database administrator, execute:


```
ALTER SYSTEM SET PROCESSES = 300 SCOPE=SPFILE;
ALTER SYSTEM SET SESSIONS = 335 SCOPE=SPFILE; -- 1.1 * PROCESSES +5
ALTER SYSTEM SET OPEN_CURSORS = 500 SCOPE=BOTH;
```
2. Restart the database.

Configure Settings for Oracle Shared Server

If your Oracle database is configured for shared server use, you can increase the total number of allowed shared server sessions using the **SHARED_SERVER_SESSIONS** parameter. Generally, we recommend increasing the **SHARED_SERVER_SESSIONS** to 300 as a starting point.

WARNING

The error message **ORA-00018: maximum number of sessions exceeded** during UIM installation indicates that the number of allowed shared server sessions should be increased.

Manual Creation of the Tablespace and User

The procedure for creating a tablespace manually depends on the version of Oracle that you are using.

Oracle 12c or higher(for Multi-tenant databases)

Create a pluggable database using the files of a seed database. See the Oracle documentation for details about the options available when you create a database from a seed.

Follow these steps:

1. Log in to the desired Oracle database as the administrator (sys as sysdba).
2. Create a pluggable database. Execute the following statement, where <pdb_name> is the name of a pluggable database, <ts_name> is a tablespace name of your choice (for example, uim_ts), <dg_name> is an ASM Disk Group Name (for example, +data):


```
create pluggable database <pdb_name> admin user <db_owner> identified by
  <owner_password>
  default tablespace <ts_name>
  datafile '<dg_name>' size 500m autoextend on
  file_name_convert = ('<location_of_db_to_be_cloned>', '<dg_name>');
alter pluggable database <pdb_name> open;
```
3. Preserve PDB Startup State (CDB - Container Database, PDB - Pluggable Database).
 - **Prior to 12.1.0.2:** Create a system trigger on the CDB to start some or all of the PDBs. Use the following command:


```
CREATE OR REPLACE TRIGGER open_pdb
  AFTER STARTUP ON DATABASE
BEGIN
  EXECUTE IMMEDIATE 'ALTER PLUGGABLE DATABASE ALL OPEN';
END open_pdb;
/
```
 - **12.1.0.2 onwards:** Use the following command:


```
ALTER PLUGGABLE DATABASE <pdb_name> SAVE STATE;
```
4. Connect to the pluggable database using 'sys as sysdba'. The service name for the pluggable database is the <pdb_name> as created in Step 2.
5. Create a non-administrator user in the CA UIM pluggable database. Execute the following statement, where <non_admin_owner> is the name of the user to be created:


```
create user <non_admin_user> identified by <user_password>;
```
6. Grant the necessary privileges to the local user <non_admin_user>.


```
grant unlimited tablespace to <non_admin_user>;
grant administer database trigger to <non_admin_user>;
grant create table to <non_admin_user>;
grant create any table to <non_admin_user>;
grant create view to <non_admin_user>;
grant alter any table to <non_admin_user>;
grant select any table to <non_admin_user>;
grant create sequence to <non_admin_user>;
grant create procedure to <non_admin_user>;
grant create session to <non_admin_user>;
grant create trigger to <non_admin_user>;
grant create type to <non_admin_user>;
grant drop any table to <non_admin_user>;
grant lock any table to <non_admin_user>;
grant select on sys.v_$session to <non_admin_user>;
grant execute on sys.dbms_lob to <non_admin_user>;
```



```
grant execute on dbms_redefinition to <non_admin_user>;
```

7. Start the UIM Server installer. When prompted, enter the following information:

- **Service Name:** Name of the pluggable database instance <pdb_name> you created
- **Username:** Username for local user <non_admin_user>
- **Port:** Port of the Oracle database

WARNING

Pluggable database does not always open correctly when hard failover happens (for example, reboot the primary Oracle RAC node). In this case we need to bring it back to open by executing:

```
alter pluggable database <pdb_name> open;
```

Your database is ready.

Support for TLS v1.2 (Oracle)

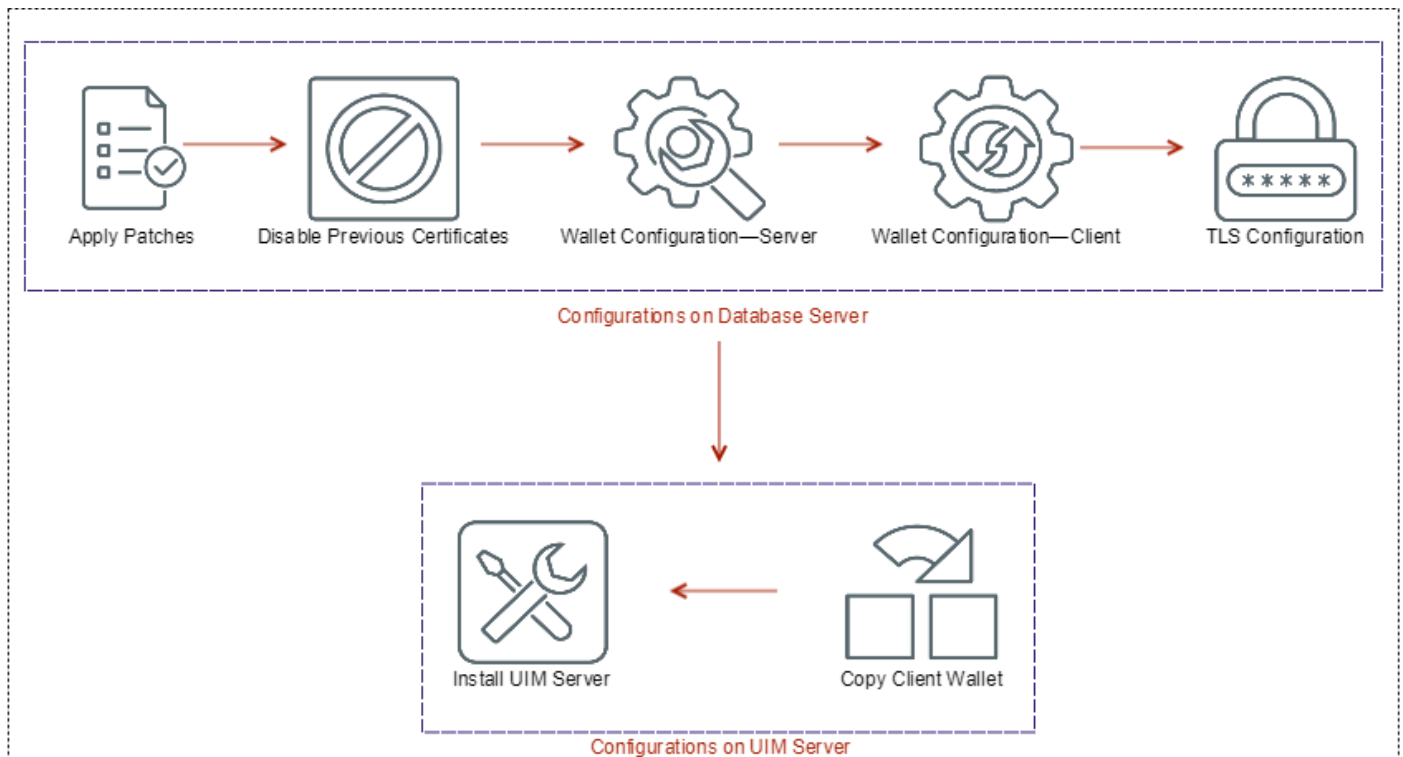
CA UIM supports Transport Layer Security (TLS) v1.2 when communicating with the UIM database: Oracle. This support enables the UIM Server to establish secure communication with the UIM database. To enable TLS v1.2 support for Oracle, ensure that you perform the required configurations on the Oracle computer (database server) and UIM Server (client computer).

The following Oracle versions are supported:

- 12c
- 19c

The following diagram shows the high-level process:

Figure 5: Oracle TLS Support



NOTE

- The cabi 4.10 probe supports TLS v1.2 when communicating with the UIM database: Oracle.
- The cabi 3.40, available with UMP 9.0.2 HF2, probe supports TLS v1.2 when communicating with the UIM database: Oracle. For more information about how to apply the UMP 9.0.2 HF2 for CABI TLS functionality, see [UMP 9.0.2 HF2](#).
- The cabi 3.32 probe does not support TLS v1.2 when communicating with the UIM database: Oracle. As a result, you cannot view the Operator Console home page, OOTB CABI dashboards, and OOTB CABI reports.
- TLS v1.2 support is not enabled by default when you install CA UIM 9.0.2.

Configurations on Database Server

Perform the following tasks on the database server.

1. Verify FQDN Requirement
2. Verify and Apply Patches for Oracle
3. Disable Previous Certificates
4. Perform Wallet Configuration for Server
5. Perform Wallet Configuration for Client
6. Set TLS Configuration on Database Server

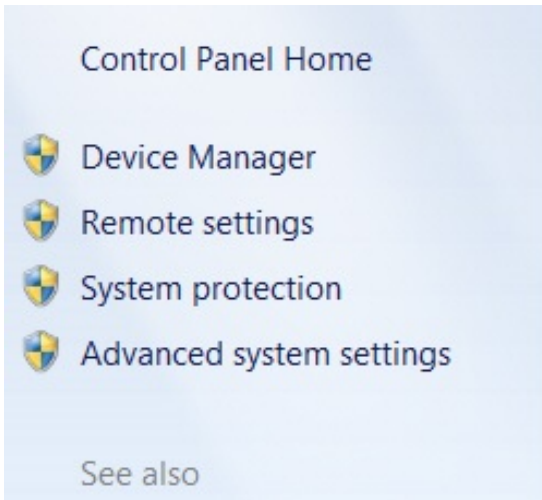
Verify FQDN Requirement

Verify that your full computer name is FQDN (for example, VI02-E74.ca.com). If not, add the domain name (for example, ca.com) to the computer name.

Follow these steps:

1. Access the properties panel of your computer (for example, right-click the Computer icon on your desktop and select **Properties**).
2. Click **Advanced system settings** in the left pane.
3. Click the **Computer Name** tab.
4. Click **Change**.
5. Click **More**.
6. Enter your domain name in the **Primary DNS suffix of this computer** field.
7. Click **OK** and restart the computer.
8. Verify that your full computer name is now FQDN.

The following example screenshot shows that the full computer name is FQDN:



Support hours: 24 hours on support URL
 Website: [Online support](#)

Computer name, domain, and workgroup settings

Computer name: VI02-E74
 Full computer name: VI02-E74.ca.com
 Computer description:
 Domain: ca.com

Disable Previous Certificates

Change the registry keys to disable all the previous versions of certificates on the database server. Verify the following registry keys on the database server:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server

For the Client and Server entries, enter the following Word and Value entries:

- DisabledByDefault=00000000
- Enabled=00000001

For more information, see the TLS 1.2 section on [TLS/SSL Settings](#).

Perform Wallet Configuration for Server

Use the Oracle Wallet Manager user interface or the orapki utility (command line) to perform the wallet configuration, which includes the following tasks:

1. Create a server wallet.
2. Set auto-login to true.
3. Create a certificate request.
4. Export the certificate request into a file and send it to certification authority.
5. Get the certificate from certification authority.
6. Import the user certificate into the server wallet.

NOTE

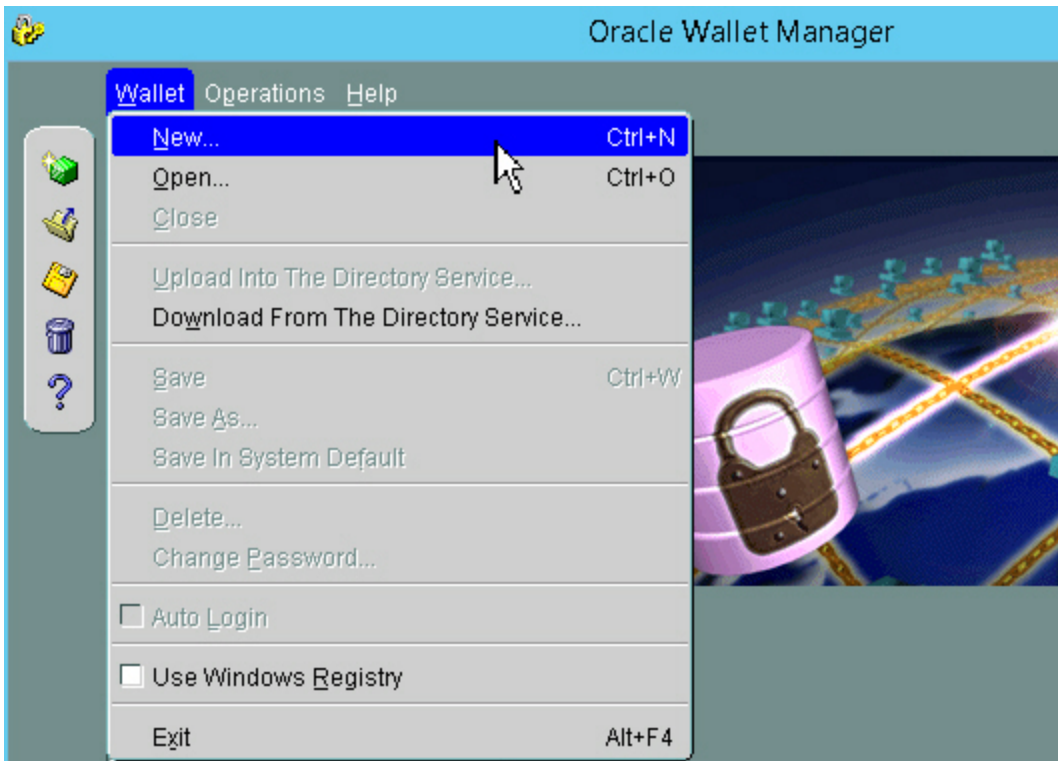
When using certificates, the certificate must be issued to FQDN (Fully Qualified Domain Name) of the computer, not the host name. Also, ensure that the database server name must also be FQDN. If both (certificate name and server name) are not FQDN, you will encounter connection issues.

Using the Oracle Wallet Manager UI

To complete the above tasks, follow these steps in the Oracle Wallet Manager UI:

1. Open the Oracle Wallet Manager UI.

2. Click **Wallet, New** as shown in the following example screenshot:



3. Click **Yes** on the directory creation dialog (if prompted).
4. Enter the wallet password, and click **OK**.
A message appears prompting you to specify whether you want to create a certificate request.
5. Click **Yes**.
The **Create Certificate Request** dialog opens.
6. Enter the required information to create the certificate, and click **OK**. Ensure that you use the FQDN when entering information in the **Common Name** field as shown in the following screenshot:

Please enter the following information to create an identity.

Common Name: VI-074.ca.com

Organizational Unit: LOD

Organization: CA

Locality/City: Boulder

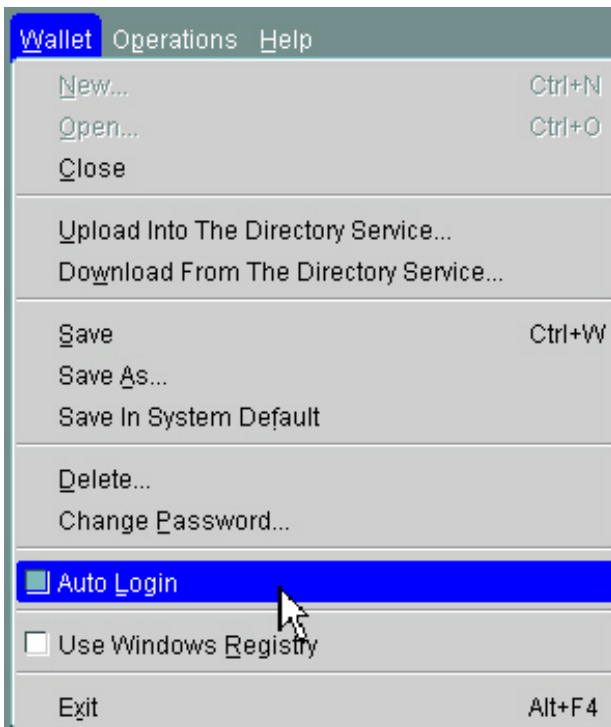
State/Province: Colorado

Country: United States Key Size: 1024

DN: CN=VI-074.ca.com, OU=LOD, O=CA, L=Boulder, ST=

Advanced OK Cancel

7. Click **OK** on the confirmation dialog.
8. Click **Wallet, Save** in the main menu to save the wallet.
9. Click **Wallet** in the main menu and enable the **Auto-Login** option to enable the auto-login for the wallet.



10. Right-click the created wallet and select **Export Certificate Request** from the context menu.
11. Browse to the location where you want to export the certificate request, enter a name for the file, and save the file.
12. Send the exported certificate request to the certification authority (CA).
The CA shares the signed user certificate.
You receive the signed user certificate, perhaps with some CA certificates or a link to the required CA website, from the CA. The standard Oracle wallet must include the root CA certificate. If the intermediate CA has signed the certificate, you must find the correct root CA certificate and then the intermediate certificates to establish the complete certificate chain. Import all the required certificates in the sequence. That is, first, import the root CA certificate, then other intermediate certificates (if applicable). You perform this import operation only if the root CA certificate or other required intermediate certificates are not already available in the wallet. Use the **Import Trusted Certificate** option to perform this step.
13. To import the signed user certificate into the server wallet, right-click the created wallet (under **Wallet**) and select **Import User Certificate** from the context menu.
The signed user certificate is imported into the specified location.

For more information, see [Using Oracle Wallet Manager](#). For more information about the orapki utility, see [Oracle Wallet Manager and orapki](#).

Using the orapki Utility

You can also use the orapki utility to perform wallet-related tasks:

1. Create a new auto-login wallet

Syntax: `orapki wallet create -wallet <Wallet Location> -pwd <Wallet Password> -auto_login`

Example: `orapki wallet create -wallet C:\Server_Wallet -pwd Abc@123 -auto_login`

2. Add a certificate request to the wallet

Syntax: `orapki wallet add -wallet <Wallet Location> -pwd <Wallet Password> -dn "CN=<FQDN>" -keysize 2048`

Example: `orapki wallet add -wallet C:\Server_Wallet -pwd Abc@123 -dn "CN=VI-074.ca.com" -keysize 2048`

3. Export the certificate request

Syntax: `orapki wallet export -wallet <Wallet Location> -pwd <Wallet Password> -dn "CN=<FQDN>" -request <Certificate Request>`

Example: `orapki wallet export -wallet C:\Server_Wallet -pwd Abc@123 -dn "CN=VI-074.ca.com" -request C:\Server_Wallet_Cert_Requests \certificate_request_filename.txt`

4. Send the certificate request to the CA

Send the certificate request to the appropriate CA in your organization.

5. **Add the root CA certificate (if required)** The CA shares the signed user certificate. You receive the signed user certificate, perhaps with some CA certificates or a link to the required CA website, from the CA. The standard Oracle wallet must include the root CA certificate. If the intermediate CA has signed the certificate, you must find the correct root CA certificate and then the intermediate certificates to establish the complete certificate chain. Import all the required certificates in the sequence. That is, first, add the root CA certificate, then other intermediate certificates (if applicable). You perform this import operation only if the root CA certificate or other required intermediate certificates are not already available in the wallet. Use the following command to perform this step:

Syntax: `orapki wallet add -wallet <Wallet Location> -pwd <Wallet Password> -trusted_cert -cert <Trusted Certificate Location>`

Example: `orapki wallet add -wallet C:\Server_Wallet -pwd Abc@123 -trusted_cert -cert C:\certificate_request_filename.crt`

6. Add the user certificate issued by the CA

Syntax: `orapki wallet add -wallet <Wallet Location> -pwd <Wallet Password> -user_cert -cert <User Certificate Location>`

Example: orapki wallet add -wallet C:\Server_Wallet -pwd Abc@123 -user_cert -cert C:\user_certificate_filename.crt

Perform Wallet Configuration for Client

Use the Oracle Wallet Manager user interface or the orapki utility (command line) to perform wallet configuration.

1. Create a client wallet.
2. Set auto-login to true.
3. Create a certificate request.
4. Export the certificate request into a file and send to certificate authority.
5. Get the certificate from certificate authority.
6. Import the user certificate into the client wallet.

NOTE

When using certificates, the certificate must be issued to FQDN (Fully Qualified Domain Name) of the computer, not the host name. Also, ensure that the database server name must also be FQDN. That is, the certificate and the server name must be FQDN. Otherwise, you will encounter connection issues.

Follow the same steps that you followed for the server wallet.

After you import the required certificates into server and client wallets, add the server certificate file as a trusted certificate to the client wallet and the client certificate file to the server wallet. As mentioned previously, you can also use the orapki utility commands to perform all the wallet-related tasks. For example, the command to perform this operation is as follows:

To add the server certificate as a trusted certificate to the client wallet:

- **Syntax:** orapki wallet add -wallet <Client Wallet location> -pwd <Client Wallet Password> -trusted_cert -cert <server_certificate_file_location>

Example: C:\orapki wallet add -wallet "C:\Client_Wallet" -pwd Dau@456 -trusted_cert -cert C:\Wallet_Store\server-certificate.crt

To add the client certificate as a trusted certificate to the server wallet:

- **Syntax:** orapki wallet add -wallet <Server Wallet location> -pwd <Server Wallet Password> -trusted_cert -cert <client_certificate_file_location>

Example: orapki wallet add -wallet C:\Server_Wallet -pwd Abc@123 -trusted_cert -cert C:\Wallet_Store2\client-certificate.crt>

Set TLS Configuration on Database Server

Use Oracle Net Manager to set the TLS configuration details. This configuration includes the following tasks:

- Enter the location of the server wallet.
- Specify that the configuration is for the server.
- Set the TLS version for the server.
- Add listener for TLS.

To complete the above tasks, follow these steps in the Oracle Net Manager UI:

1. Open Oracle Net Manager.
2. Expand **Oracle Net Configuration**.
3. Expand **Local** and click **Profile**.
4. Select **Network Security** from the drop-down list.
5. Click **SSL**.
6. For wallet directory location, browse to the location where you have saved the server certificates.
7. Select **Server** for the **Configure SSL for** option.

8. Select **Any** from the **Require SSL Version** drop-down list as shown in the following example screenshot:

The screenshot displays the Oracle Enterprise Manager console. On the left, a tree view shows the hierarchy: Local > Profile > Service Naming > Listener > LISTENER. The right pane shows the configuration for the selected listener, with the 'SSL' tab active. The configuration includes:

- Credential Configuration:** Configuration Method: File System; Wallet Directory: C:\app\Administrator\product11.2; Encryption Wallet Directory: (empty).
- Configure SSL for:** Client (unselected), Server (selected).
- Cipher Suite Configuration:** A table with columns for Authentication, Encryption, and Data Integrity. Two cipher suites are listed: RSA/AES_256_CBC/SHA and RSA/3DES_EDE_CBC/SHA.
- Revocation Check:** None.
- Require SSL Version:** Any.
- Require Client Authentication:** (unchecked).

Note: In order to use SSL for server connections, you must choose the protocol, TCP/IP with SSL, when configuring the Listener.

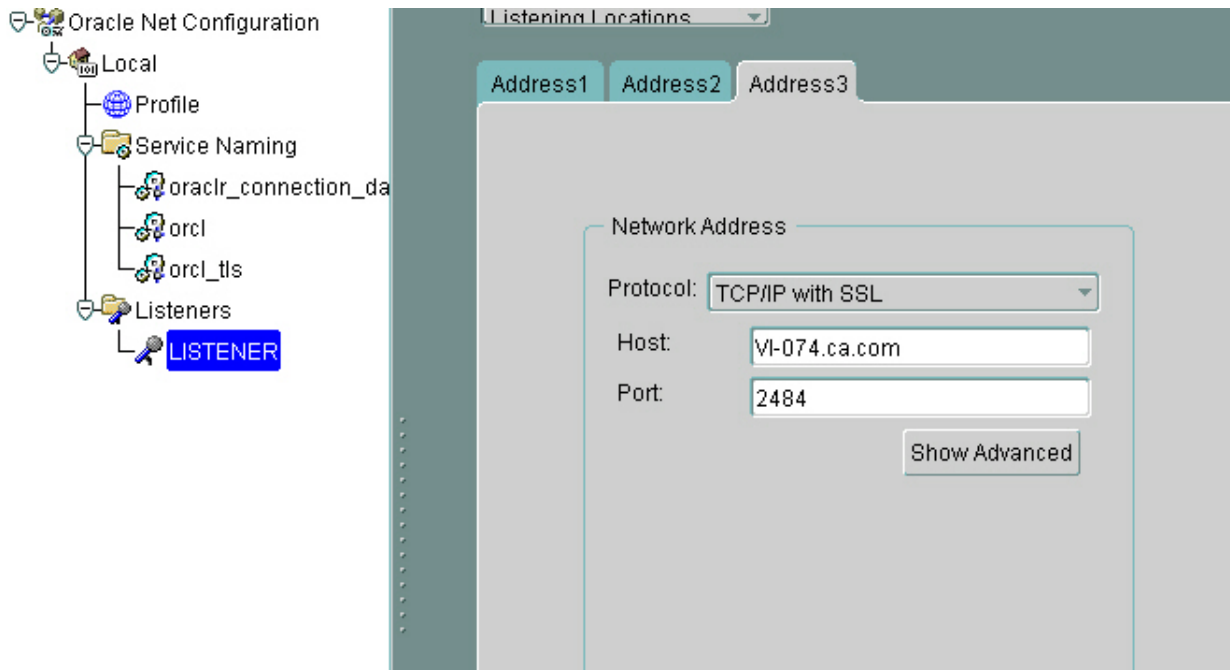
9. Expand **Listeners** and click **LISTENER**.

10. Select the location of the listener from the drop-down list.

11. Add address with the following information:

- **Protocol:** TCP/IP with SSL
- **Host:** Server host name
- **Port:** 2484 (default)

The following example screenshot shows the settings:



12. Click **File, Save Network Configuration** to save all the changes.
13. Restart the listener (Insrctl stop and Insrctl start).

The sqlnet.ora file is updated with the following entries:

```
wallet_location =
(SOURCE=
(METHOD=File)
(METHOD_DATA=
(DIRECTORY=server_wallet_location)))
```

This file is available at `<Oracle_Home>\network\admin.`

Also, you can enable or disable client authentication, as required. The following entry is available in sqlnet.ora to do so:

```
SSL_CLIENT_AUTHENTICATION = TRUE
```

For more information, see [Configuring Secure Sockets Layer Authentication](#).

Configurations on UIM Server

You must perform the following steps on the computer where you want to install the UIM Server:

1. Verify that Oracle Instant Client (version 12.1.0.2.0) is available on the UIM Server.
2. Copy the client wallet folder from the database server to the computer where you plan to install the UIM Server.
3. Note that you need to provide the required client wallet location, wallet password, wallet type, and whether client authentication is needed when you install the UIM Server. The UIM Server installer copies the required wallet files from the provided location and places them in the `<Nimsoft>\security` folder. For more information about the UIM Server installation, see [Install UIM Server](#) and [Installation Parameters](#). The following screenshot shows the TLS v1.2 options (**Enable TLS, Wallet Location, Wallet Type, Wallet Password, and Authenticate Client**) during the UIM Server installation:

CA UIM Server 9.0.2

Database Configuration

Select your database provider, enter the field data, and click Test. Any modifications require the test to be performed again.

Oracle

SYS Password: ?

Database Username: ?

Database Password: ?

Confirm Database Password: ?

Database Tablespace Name: ?

Enable TLS:

Wallet Location: Browse ?

Wallet Type: ?

Wallet Password:

Authenticate Client:

NOTE

Ensure that the ppm probe version is 3.48 or later and robot version is 7.96 or later to display TLS v1.2 configuration options in Admin Console. Otherwise, TLS v1.2 options are not displayed in Admin Console.

The TLS v1.2-related options are as follows:

- **Enable TLS:** Select the option to enable TLS v1.2 in CA UIM, which lets the UIM Server to establish a secure communication with the UIM database (Oracle in this case).
 - **Wallet Location:** Specify the location of the wallet where your security certificates are available. This location includes your trusted security certificates. The same security certificate must be available on the database server.
 - **Wallet Type:** Select the wallet type from the drop-down list. The selected wallet type takes the precedence. Note that both SSO and PKCS12 are copied to the UIM Server (`<Nimsoft>\security`) irrespective of the wallet type you select.
 - **Wallet Password:** Specify the password to access the wallet information.
 - **Authenticate Client:** Select the option to specify whether you want to enable client authentication.
4. After you complete the UIM Server installation, ensure that the following entries are present in the `sqlnet.ora` file that is available in the `<Nimsoft>\security` folder:
- ```
SSL_CLIENT_AUTHENTICATION = TRUE
wallet_location =
(SOURCE=
(METHOD=File)
(METHOD_DATA=
(DIRECTORY=client_wallet_location)))
```

**Additional Information**

Review the following additional information:

- In upgrade scenarios and in situations where you want to enable TLS v1.2 support after the UIM Server installation, perform the following tasks on the UIM Server:
  - a. Verify the availability of Oracle Instant Client.
  - b. Copy the client wallet.
  - c. Use the data\_engine [Admin Console](#) or [Infrastructure Manager](#) to configure the TLS v1.2-related parameters. Provide the required TLS v1.2 information; for example, client wallet location, wallet password, wallet type, and whether client authentication is needed. data\_engine copies the required wallet files from the provided location and places them in the <Nimsoft>\security folder.

After you provide the information, restart the data\_engine probe. The data\_engine probe is successfully configured to support TLS v1.2. You can now deploy other probes and use the secure communication when interacting with the UIM database. Also, review the impacted probes and packages list. These items have been updated to support TLS v1.2. Ensure that you use the latest version of these items if you want them to work in the TLS v1.2 environment. The following screenshot shows the TLS v1.2 options (**Enable TLS, Wallet Type, Wallet Location, Wallet Password, and Need Client Authentication**) in Admin Console:

The screenshot displays the 'Database Vendor' configuration window in the Admin Console. The 'Database Vendor' is set to 'Oracle'. The 'Connection Information' section includes fields for Hostname, Port (1521), Username, Password, and Service name. Below this, there are several configuration options: 'Partition data tables (CAUTION)' (unchecked), 'Index Maintenance' (unchecked), 'Online mode' (Dynamic), and 'Fragmentation level (%)' (30). The 'Enable TLS' checkbox is checked. The 'Wallet Type' is set to 'PKCS12', and the 'Wallet Location' and 'Wallet Password' fields are present. The 'Need Client Authentication' checkbox is unchecked.

- d. Ensure that the sqlnet.ora file is created and placed it in the <Nimsoft>\security folder. Verify that the following entries are present in the file:

```
SSL_CLIENT_AUTHENTICATION = TRUE
wallet_location =
(SOURCE=
(METHOD=File)
(METHOD_DATA=
(DIRECTORY=client_wallet_location)))
```

- e. Open the raw configuration for the controller probe, navigate to the environment section, enter the value as `<Nimsoft>\security` for the `TNS_ADMIN` variable, save the changes, and restart the robot.
- Additionally, for upgrade scenarios, the CA UIM system can be either TLS v1.2 enabled or disabled for all components; it cannot be a partial TLS v1.2-enabled system. That is, all the infrastructure components across layers (for example, primary hub, secondary hub, probes) should be upgraded to the TLS v1.2-supported version.
  - When you want to update a certificate (for example, older certificate has expired), specify the wallet location that includes the new certificate in the `data_engine` UI. The `data_engine` UI uses that information to place the new wallet files on the primary hub in a specific location (`<Nimsoft>\security` folder). Restart the `data_engine` probe. Also, restart the affected probes on other robots.
  - You can enable or disable the TLS v1.2 mode by configuring the `data_engine` UI. Also, restart of `data_engine` is needed whenever TLS v1.2 mode is changed.
  - If you upgrade from a previous version of CA UIM to this version, the state of the system remains in non-TLS v1.2 mode. To enable TLS v1.2 mode, perform all the required manual steps that are mentioned above and use the `data_engine` UI to enable TLS v1.2.
  - If you encounter any database-connectivity issue in a TLS v1.2-enabled environment, the most probable reason for this issue might be that your certificate is not using FQDN.
  - Before you deploy CABI External version 3.4 on a secondary robot, copy the wallet file (SSO or PKCS12) from the UIM Server (`<Nimsoft>\security`) to the CABI External secondary robot (`<Nimsoft>\security`).

### **Probes and Packages Updated for TLS v1.2**

TLS v1.2-related updates have been made to the following items so that they can work in a TLS v1.2 environment. These are the minimum versions with TLS v1.2 related updates:

- ace 9.03

**NOTE**

The ace probe has been deprecated in [UIM 20.3.3](#).

- alarm\_routing\_service 10.20
- apmgwtw 3.20
- audit 9.03
- axagateway 1.32
- cisco\_ucm 2.00
- cm\_data\_import 9.02
- data\_engine 9.02
- discovery\_agent 9.02
- discovery\_server 9.02
- ems 10.20
- hub 7.96
- maintenance\_mode 9.02
- mon\_config\_service 9.02
- mpse 9.03
- nas 9.03
- nis\_server 9.03
- qos\_processor 9.02
- robot 7.96
- sla\_engine 9.02
- telemetry 1.20
- trellis 9.02
- udm\_manager 9.02
- usage\_metering 9.11
- wasp 9.02
- webservices\_rest 9.02

**Troubleshooting**

The following topic provides information about how you can troubleshoot TLS v1.2 related issue:

**Unable to Change "Need Client Authentication" in the data\_engine UI**

**Symptom:** This issue occurs when TLS v1.2 is enabled for Oracle (UIM database) and you try to change the **Need Client Authentication** option. In the data\_engine AC or IM interface, when you try to change the **Need Client Authentication** option, the appropriate value for this option is not set in the sqlnet.ora file. The sqlnet.ora file is available in the < Nimsoft>\security folder on the UIM Server computer.

**Solution:** As a workaround, you must manually update the value of the SSL\_CLIENT\_AUTHENTICATION parameter. To do so, follow these steps:

1. On the UIM Server computer, navigate to the < Nimsoft>\security folder.
2. Locate and open the sqlnet.ora file.
3. Update the SSL\_CLIENT\_AUTHENTICATION parameter in the sqlnet.ora file based on whether the **Need Client Authentication** option is selected or not (in the data\_engine IM interface).

For example, if the option is selected in the IM interface, the parameter must be set as follows:

```
SSL_CLIENT_AUTHENTICATION = TRUE
```

If the option is not selected, the parameter must be set as follows:

```
SSL_CLIENT_AUTHENTICATION = FALSE
```

4. Restart the data\_engine probe.

## Facing Issues with the UIM Database (Oracle)

**Symptom:** I am facing issues with the Oracle database in my TLS v1.2 environment.

**Solution:** To identify the problem, install SQL\*Plus Instant Client and use the following command:

```
Sqlplus DatabaseUser@ "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS) (HOST=DatabaseHost)
(PORT=DatabasePort)) (CONNECT_DATA=(SERVICE_NAME=Servicename))) "
```

## Pre-Installation Considerations

Review the following pre-installation considerations:

- Separate logins are required for logging into [support.nimsoft.com](http://support.nimsoft.com) and [support.broadcom.com](http://support.broadcom.com). In case of any issue, contact Customer Assistance.
- Microsoft Visual C++ 2008 Redistributable Package is no longer deployed as part of the UIM installation. If you need this package, you can download it from [support.nimsoft.com](http://support.nimsoft.com). For example, the Infrastructure Manager (IM) required the Microsoft Visual C++ 2008 version of `vc_redist_x86.exe` and `vc_redist_x64.exe`.
- Access to the Internet is required for successful installation of UIM as it helps in downloading required packages from the web archive. If you cannot have it on the primary hub server, use IM on an operating system that can get the Internet access. Or, install Admin Console on a computer that has the Internet access.
- Ensure that the UIM Server installer (`setupCAUIMServer` executable) and UIM Server packages (`uimserverpackages.zip` file) are in the same location.
- We recommend that you do not install IM or OC on the cluster nodes. Install them on a separate server.
- Oracle Instant Client must be installed on the UIM system to access the Oracle database.
- Microsoft SQL Server is supported only for Windows UIM Server installation.
- You can have many instances of the same probe in a UIM domain, but only one instance of a specific probe per robot.
- Robots for Windows systems must be deployed from hubs running Windows.
- UIM does not support the use of native installers to perform robot upgrades. To upgrade your robots, you must use the `robot_update` package that is available in either the Admin Console or IM archive. For the first-time robot installations, the native robot installers are still supported.
- Hub parameters (domain and hub name, specifically) modified after installation will severely impact your environment. Changing these fields without updating the rest of the hub and robot configuration files (`hub.cfg` and `robot.cfg`) in your environment will cause a disconnect from those components.

## Configure Installation on IPv6 Environment

CA UIM 20.3.0 can be deployed in a pure IPv6 mode environment using IPv6 address. Installing CA UIM does not impact any existing feature and functionality.

### Software Requirements

Before you deploy CA UIM, you must consider the following software requirements:

- Deploy CA UIM on a Linux or Windows 2012 system with Oracle, MySQL, or Microsoft SQL Server as the database.
- The probes which are IPv6 compliant can monitor the systems with the following operating systems:
  - Windows 2012
  - RHEL 6.x
  - HP-UX
  - AIX
- The secondary robot can be configured on any of the following operating systems:

- Windows 2012
- RHEL 6.x
- HP-UX
- AIX

### **Pre-Installation Considerations**

Consider the following points before deploying CA UIM:

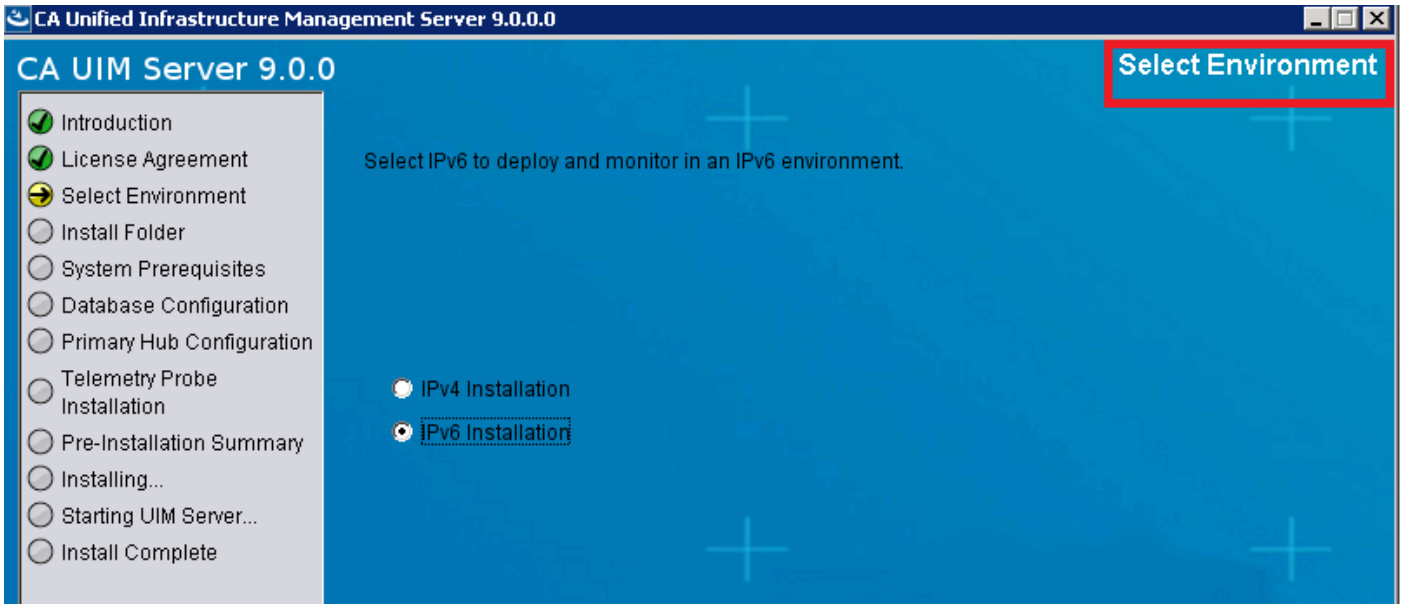
- For IPv6, regular Nimbus Manager.exe does not work as expected. You must use a different Infrastructure Manager interface (**Nimbus ManagerIPv6.exe**) which is bundled with the IPv6 UIM Package. This package can be found at same location as **Nimbus Manager.exe**.
- If you install the robot using the native installers, add the “ip\_version” key with value “ipv4 ipv6” in the robot configuration file.
- Ensure that IPv6 interface is enabled on the machine where you want to install UIM/Operator Console (OC).
- Before you deploy a robot and secondary hub, you must add the environment variable, **NIM\_ROBOT\_IP** and must set the value as **0:0:0:0:0:0:1** on the machine where UIM is installed. Similarly, you must add this environment variable and set its value before deploying CA Operator Console (OC). Setting this variable is required for the installer to connect to the primary hub.
- To install the robot in a pure IPv6 environment, run the installer as follows, on the UNIX system:  

```
./nimldr -R <ipv6 address of hub to connect to>
```
- **(Optional)** We recommend using hostname instead of IP address for robot installation through OC using an xml file.
- **(Optional)** We recommend adding IPv6 entries in the host files before using discovery wizard and deploying the secondary robot.
- For IPv6 environment, you cannot specify an IP address range for scope. You must specify a single IP address at a time.
- With IPv6 UIM installer, addition of any key in hub.cfg is not required. However to manually configure IPv6 environment, add the key **IPV6\_HANDLING\_ENABLED**, and set the value as **Yes**. To add the key:  
**Follow these steps:**
  - a. Stop the Robot/UIM
  - b. Change IPv4 address to IPv6
  - c. Add the key **IPV6\_HANDLING\_ENABLED** and set the value as **Yes** in the **Setup** section of the hub.cfg using Raw Configuration
  - d. Start UIM

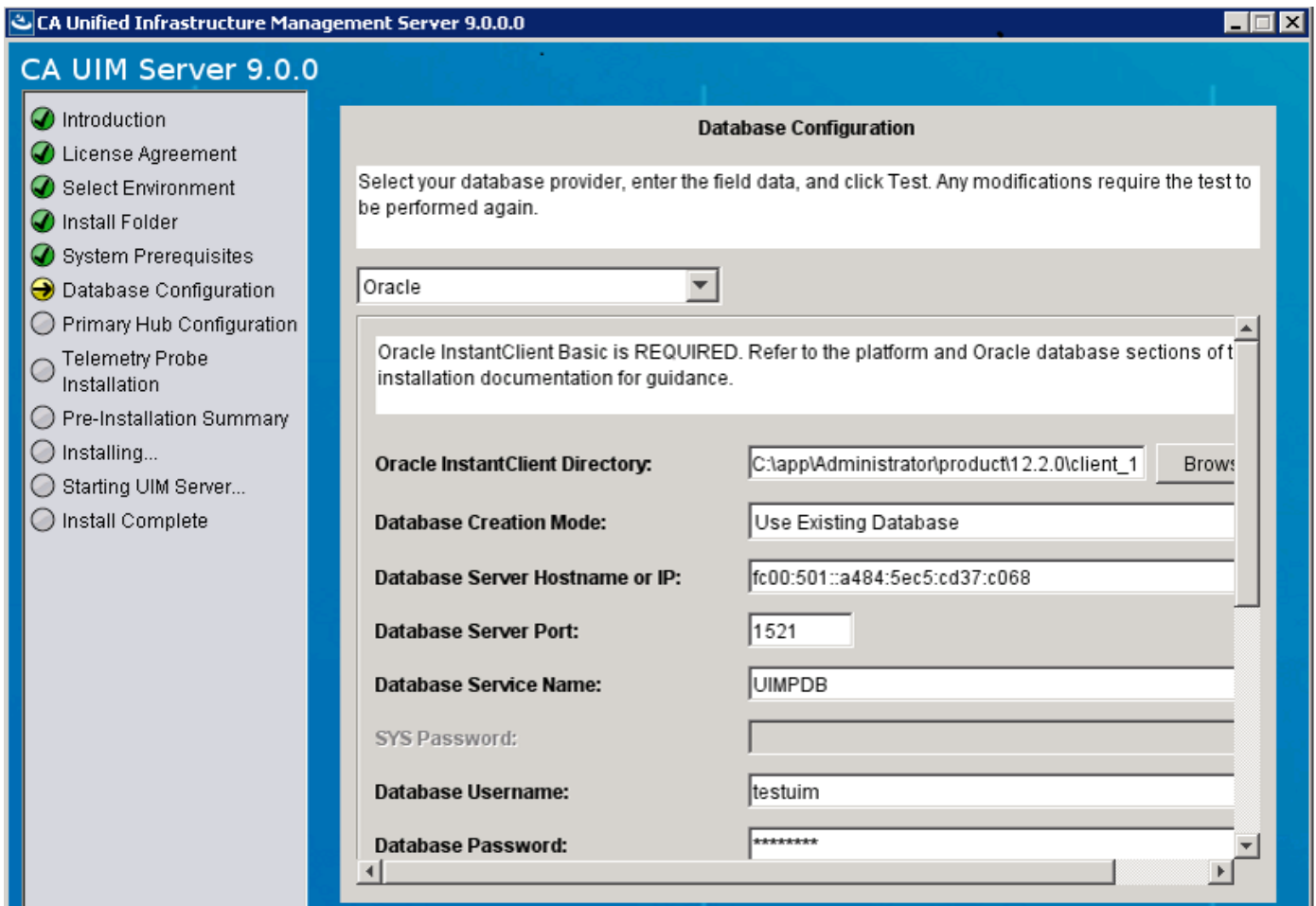
### **Instal UIM on an IPv6 Environment**

To install UIM on an IPv6 environment, follow these steps:

1. Review the pre-installation considerations and meet the requirements.
2. Run the installer following the prompts.
3. Select the **IPv6 installation** option on the **Select Environment** screen.

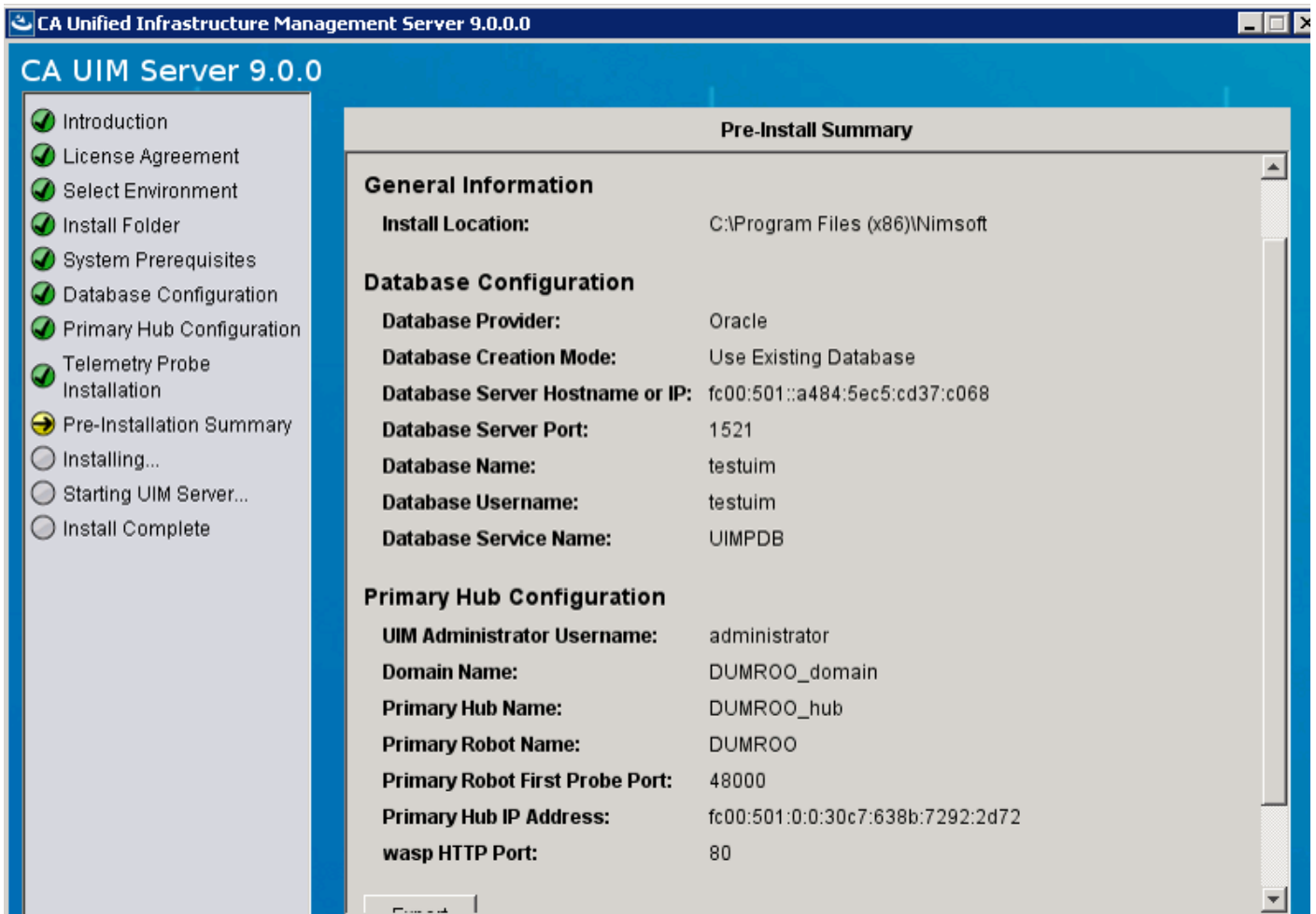


4. Specify/select the Install Folder and check System Prerequisites.
5. Select the database and test the connection. You can install UIM with an IPv6 database server. Installation of UIM on IPv6 supports Oracle, MySQL, and Microsoft SQL databases.





6. Follow the prompts to complete the installation and review Pre-Installation Summary to verify your configuration.



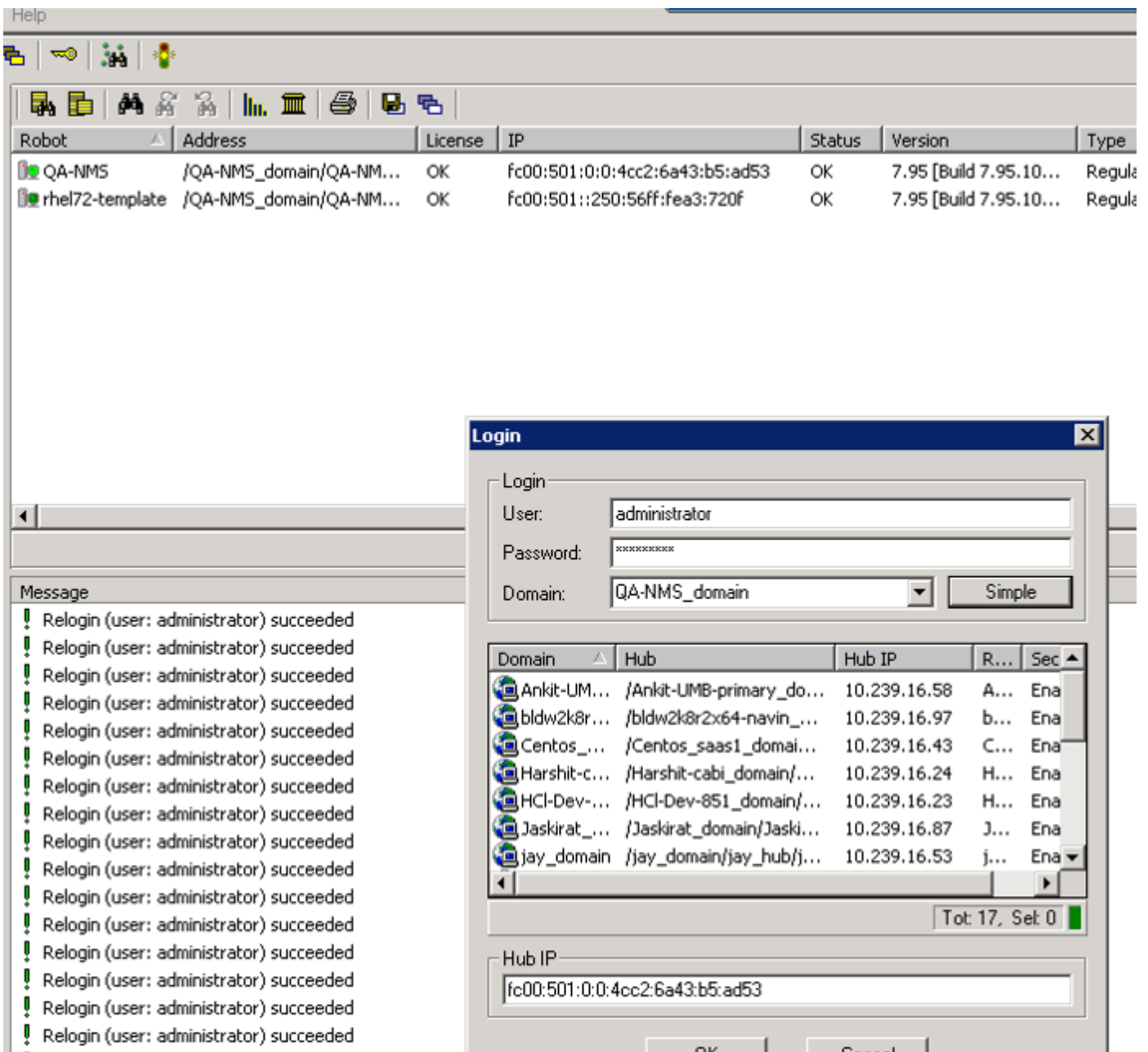
### Install Secondary Robot

To install a secondary robot on the Windows IPv6 system using the Nimbus Robot.exe, select **Choose to connect to the network interface through IP address**.



#### **Access UIM, adminconsoleapp, and OC on an IPv6 Environment**

- Enter the IPv6 address or hostname of the hub in the **Advanced** field to access UIM on an IPv6 environment using Infrastructure Manager.



- **Admin Console GUI:** On an IPv6 environment, to deploy and configure probes on robots from Archive, use the following URL: IPv6 address should be in square brackets **adminconsoleapp**: `https://[<IPv6 address>]:<port>/adminconsoleapp`
- **Example:** `[fc00:416::1c87:2358:a822:1c6b]:80/adminconsoleapp` and OC
- **OC:** Enter the IPv6 address or hostname of the OC robot enclosed in square brackets followed by port name: `https://[<IPv6 address>]:<oc port>/`

## Probes Certified on IPv6 Environment

The following probes are certified on IPv6 environment:

| System     | Application      | Gateway   | Network           | Database  | Services |
|------------|------------------|-----------|-------------------|-----------|----------|
| cdm        | ad_server        | adogtw    | interface_traffic | db2       | nexec    |
| dirscan    | adevl            | emailgtw  | net_connect       | oracle    |          |
| fsmounts   | exchange_monitor | snmpgtw   | ntp_response      | sqlserver |          |
| logmon     | lync_monitor     | snmptd    | snmpget           |           |          |
| ntevl      | tomcat           | sysloggtw |                   |           |          |
| ntperf     | weblogic         |           |                   |           |          |
| ntservices |                  |           |                   |           |          |
| perfmon    |                  |           |                   |           |          |
| printers   |                  |           |                   |           |          |
| processes  |                  |           |                   |           |          |
| reboot     |                  |           |                   |           |          |
| rsp        |                  |           |                   |           |          |

## Password Policies

This article provides information about password policies:

### CA UIM User Password Policy

All passwords are installed in an encrypted format. The UIM Server administrator account password must meet the following requirements:

- Be at least six characters
- Not exceed a maximum of 254 characters
- Cannot be the same as the username (For example, administrator)

We recommend that you configure your user accounts to follow your own internal policy.

### OC User Password Policy

All passwords are installed in an encrypted format. CA does not have a policy for OC users. We recommend that you adhere to your organization's internal policy for the creation of account passwords.

### Database User Password Policy

CA does not have a policy for database users. We recommend that you adhere to your organization's internal policy for the creation of account passwords.

### Logging of Failed Login Attempts

#### Admin Console

Set the log level on the service\_host probe to level 4 or higher to have the system log failed login attempts. Log levels lower than 4 do not report when a failed login attempt occurs. Failed login attempts result in a log entry in service\_host.log indicating a severe error. The following message is an example of a service\_host.log entry for a failed login:

```
Dec 02 11:12:59:179 [tomcat, service_host] SEVERE: Login Error 2: Received status (12)
on response (in sendRcvLogin) for cmd = 'login'
```

**OC**

Set the log level on the wasp probe to level 3 or higher to have the system log failed login attempts. Log levels lower than 3 do not report when a failed login attempt occurs. Failed login attempts result in a log entry in wasp.log. The following message is an example of a wasp.log entry for a failed login:

```
Dec 02 14:00:00:778 INFO [http-bio-80-exec-7,
com.nimsoft.nimbus.probe.service.wasp.auth.LoginModule] Login failed: Wrong username
and/or password.
```

**Firewall Port Reference**

The following table describes the port assignments for various CA UIM components and configurations. These port assignments apply to single-hub installations and to multiple-hub installations with and without a firewall.

The following topics cover the complete information:

**Considerations**

Review the following considerations:

- All installations require:
  - Robot controller
  - Robot spooler
  - Robot-to-hub and manager-to-hub communications
  - A port for each probe
  - wasp probes to access Admin Console or OC through HTTP
- Multiple-hub installations for tunnels that are NOT SSL tunnels also require:
  - Tunnel server
- Multiple-hub installations for tunnels that ARE SSL tunnels also require:
  - service\_host to tunnel client
- Installations that enable discovery across a firewall without a hub and tunnel require the port for the appropriate protocol to be open in the discovery\_agent probe.

**NOTE**

Protocols for all components are TCP except for controller, hub, and spooler, which also require UDP. UDP broadcast is used for the discovery of the hub, spooler, and controller components. All other core communications are done via TCP.

**Firewall Port Reference Table**

In the following table, Firewall Rules define the ports and directions that must be open through the firewall.

| CA UIM Component                 | Ports              | Direction | Firewall Rules                                       | Details                                   |
|----------------------------------|--------------------|-----------|------------------------------------------------------|-------------------------------------------|
| <b>CABI Server, UIM database</b> | 1433, 1521 or 3306 | Inbound   | Allow inbound on respective port to database server. | Inbound from CABI to the chosen database. |

|                               |                                |                          |                                                          |                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------|--------------------------------|--------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>CABI Server, OC</b></p> | <p>80 or 443; configurable</p> | <p>Inbound, outbound</p> | <p>Allow inbound on 80 or 443 to OC and CABI Server.</p> | <p>This connection provides browser and customer client connectivity to CABI and OC. Port 80 by default, or port 443 or another configured port for HTTPS. The port can vary from client/browser to CABI and OC. The value depends on your choice during the CABI and OC installation. For example, port 80 or port 443. The configurable range of ports is 1 through 65535.</p> |
|-------------------------------|--------------------------------|--------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                          |                            |                          |                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|----------------------------|--------------------------|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Controller</b></p> | <p>48000; configurable</p> | <p>Inbound, outbound</p> | <p>Allow inbound on 48000+ for probe access on all robots.</p> | <p>The controller listening port.</p> <p>For an enterprise, enable communication both ways on port 48000 through a firewall. Communication both ways allow CA UIM to contact and control hubs, robots, and probes. This port also receives status from BUS components.</p> <p>The hub spooler and the spooler for robots transmit alarm and QoS data. A port must be set in the controller configuration for Infrastructure Manager (IM) and Admin Console to connect to remote tunnels through the tunnel server and client IPs: for example, 192.168.1.10:50003.</p> <p>For tunnel hubs, set the <b>First Probe port number</b> in Setup &gt; Advanced for the controller to 50000 or higher. If necessary, open the same port and higher in the firewall.</p> <p><b>Note:</b> You only need ports 48000 for the controller and 48002 for the hub open between the primary hub and the OC hub. You don't need these ports open between every hub in the domain and the OC server as the hub controllers will talk to the primary hub controller.</p> |
| <p><b>Spooler</b></p>    | <p>48001; configurable</p> | <p>Inbound, outbound</p> | <p>Allow inbound on 48001 on all robots.</p>                   | <p>Enable inbound communication from robot to hub so that probes can send messages to hubs through the spooler port. Probes send messages to hubs using the spooler port 48001. This port must be enabled from the robot to the hub.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|                   |                            |                          |                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|----------------------------|--------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Hub</b></p> | <p>48002; configurable</p> | <p>Inbound, outbound</p> | <p>Allow inbound on 48002 to the hub.</p> | <p>The hub listening port. This connection allows robot-to-hub and manager-to-hub communications.</p> <ul style="list-style-type: none"> <li>• Allow outbound traffic on all hub and robot ports.</li> <li>• All hubs must have port 48002 open inbound and outbound for robot-to-hub and manager-to-hub communications.</li> <li>• All hubs must have port 48000 open inbound and outbound for communication with the robot controller.</li> <li>• All child robots must also have port 48000 open inbound.</li> <li>• Open port 48001 on the hub for spooler communications.</li> </ul> <p>We recommend that you have ports 48000 through 48099 open inbound to all robots.</p> <p><b>Note:</b> You only need ports 48000 for the controller and 48002 for the hub open between the primary hub and the OC hub. You don't need these ports open between every hub in the domain and the OC server as the hub controllers will talk to the primary hub controller.</p> |
|-------------------|----------------------------|--------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



|                       |                                       |  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|---------------------------------------|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Tunnels</b></p> | <p>48003 or 443;<br/>configurable</p> |  |  | <p>Tunnels using tunnel-server-to-tunnel-clients model or tunnel-client-to-tunnel-servers need port 48003, 443, or another configured port for incoming traffic. For example, a port must be open for the enterprise data center and MSP firewall.</p> <p><b>Note:</b> Port 443 is the default port for <b>https</b> but can be used for other purposes.</p> <p>Multi-hub infrastructures can use a tunnel with or without SSL. For tunnels that are NOT SSL tunnels, ports use the same assignment as for single-hub installations.</p> <p><b>Note:</b> You only need ports 48000 for the controller and 48002 for the hub open between the primary hub and the OC hub. You don't need these ports open between every hub in the domain and the OC server as the hub controllers will talk to the primary hub controller.</p> |
|-----------------------|---------------------------------------|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                             |                                                                                                                    |                |                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------|----------------|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secure (SSL) Tunnels</b> | 48003; configurable                                                                                                | Unidirectional | Allow inbound, outbound through a firewall.             | <p>If you are using a CA UIM SSL tunnel, you need the tunnel port open between tunneled hubs. All other CA UIM traffic flows over the tunnel. For tunnels that are SSL tunnels:</p> <ul style="list-style-type: none"> <li>• The controller port must be set to 48000.</li> <li>• The hub port must be set to 48002.</li> <li>• The tunnel client port must be set to 48003 to allow access to the tunnel server.</li> <li>• The wasp probe must be set to port 80 to access Admin Console and the CA UIM web page.</li> </ul> <p>All other UIM ports, other than the configured SSL tunnel port, must be blocked.</p> |
| <b>Discovery_agent</b>      | DNS - port 53<br>NetBIOS - port 137<br>SSH - port 22<br>SNMP - port 161; configurable<br>WMI - port 135 and others | Outbound       | Allow outbound on ports for the protocol                | Discovery_agent makes calls, as a client, to the services hosted on target machines.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Probes</b>               | 48004-48050; configurable                                                                                          | Inbound        | Allow inbound on 48004-48050 (or higher) on all robots. | <p>Probes listen on their respective ports and await incoming connections from other clients. The inbound port for each probe must be open so that outside clients and hubs can communicate. Ports are assigned to probes sequentially as available beginning with the first probe port number. For information about probe-specific port requirements, refer to the probe documentation at <a href="#">CA Unified Infrastructure Management Probe Space</a>.</p>                                                                                                                                                      |

|                                             |                                                                                                                 |                          |                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Distribution Server (distsrv)</b></p> | <p>48005 or automatically assigned</p>                                                                          | <p>Inbound, outbound</p> | <p>See Details</p>                 | <p>The distsrv probe on the hub must have its TCP port open on the hub for licensing of probes on the robots. Without this port open, probes fail to start on the robots. Unlike the controller, spooler, and hub, the distsrv probe does not have a reserved port. The port can change each time the hub restarts.</p>                                                                                                                                                                                                                                                             |
| <p><b>UIM database</b></p>                  | <p>1433 (Microsoft SQL Server); configurable<br/>1521 (Oracle); configurable<br/>3306 (MySQL); configurable</p> | <p>Inbound</p>           | <p>Allow inbound for database.</p> | <p>The primary hub (data_engine) to UIM database is preferably local/on the same subnet as CA UIM. If the database for the primary hub is behind an internal firewall, then the appropriate port has to be open from the UIM Server to the CA UIM database, outbound from hub server, and inbound on the CA UIM database server. Responses from the database server to the primary hub come back over the same connection/port.</p> <p><b>Tip:</b> Port information for your UIM database is located in the <b>Database Configuration</b> section of the data_engine probe GUI.</p> |

|                           |                           |                 |                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|---------------------------|-----------------|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>ADE</b></p>         | <p>22</p>                 | <p>Outbound</p> |                                               | <p>The automated_deployment engine probe uses port <b>22</b> to deploy robots using SSH file transfer to the target system. If you cannot open port 22 on the primary hub:</p> <ul style="list-style-type: none"> <li>• a. Deploy the automated_deployment_eng a secondary hub where port 22 is not blocked.</li> <li>b. Log in to Infrastructure Manager directly from the secondary hub.</li> <li>c. Drag and drop the robot packages that you want to deploy into the archive on the secondary hub.</li> <li>d. Deploy the robots to the secondary hub through an XML file. For more information, see the topic <a href="#">Bulk Robot Deployment with an XML File</a>.</li> </ul> |
| <p><b>udm_manager</b></p> | <p>4334; configurable</p> | <p>Inbound</p>  | <p>Allow inbound on 4334 for UDM Manager.</p> | <p>UDM clients (Datomic peer), including OC, Trellis, and the Discovery Server, must connect to the SQL database and also to UDM Manager on this port.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                              |                                                                |                   |                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|----------------------------------------------------------------|-------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OC server</b>             | 8080, 80, or 443;<br>configurable range: 1–65535               | Inbound, outbound | Allow inbound on 8080, 80, or 443 on OC server.      | The port assignment for the OC server can vary by client/browser to OC and depends on your choice during the OC installation.<br>If you are using a configuration with multiple OC servers, the servers communicate through multicasting on the following IP address and ports: <ul style="list-style-type: none"> <li>IP addresses <b>239.255.0.1</b> through <b>239.255.0.5</b></li> <li>Ports <b>23301</b> through <b>23305</b></li> </ul> |
| <b>OC (Tomcat connector)</b> | 8009                                                           | Inbound, outbound | Allow inbound on 8009 on OC server.                  | The OC engine.<br>Allow inbound on port 8009 from the UIM Server to the OC instance (wasp probe).                                                                                                                                                                                                                                                                                                                                             |
| <b>OC database</b>           | 1433 (Microsoft SQL Server);<br>1521 (Oracle);<br>3306 (MySQL) | Inbound           | Allow inbound on respective port to Database server. | Inbound from OC to the chosen database.<br>The wasp probe requires a connection to the UIM database. Ensure that the database ports between the OC and database servers are open.                                                                                                                                                                                                                                                             |
| <b>UIM Server home page</b>  | 80; configurable                                               | Inbound           | Allow inbound to port 80 (internal enterprise).      | The UIM Server home page is typically internal-access only. Open the port in the firewall for any systems that must be able to contact the primary hub to run applications or download and install the client software.                                                                                                                                                                                                                       |
| <b>SMTP</b>                  | 25; configurable                                               | Outbound          | Allow outbound                                       | Report Scheduler creates output in PDF and CVS that is transmitted via email to users. Email transmission requires a designated server with this SMTP port open.                                                                                                                                                                                                                                                                              |
| <b>SNMP</b>                  | 161; configurable                                              |                   |                                                      | SNMP is an internet-standard protocol for managing devices on IP networks. The snmpcollector probe uses port <b>161</b> by default to communicate with the SNMP port on a device.                                                                                                                                                                                                                                                             |

|                                                |                                     |                   |                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------|-------------------------------------|-------------------|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hub to LDAP/AD server</b>                   | 389, 686; configurable              | Outbound          | Allow outbound to LDAP/AD server.               | Allow outbound to any custom port set in wasp probe configuration.                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Web clients, browsers to OC, OC clients</b> | 80, 443; configurable               | N/A               | Allow inbound on port 80 or 443.                | Portal access over the Internet.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Admin Console</b>                           | 80, 443; configurable<br>wasp probe | Inbound           | Allow inbound on port 80 or 443 on primary hub. | Admin Console is hosted on the primary hub with <code>service_host</code> . <ul style="list-style-type: none"> <li>80 is the default port to access Admin Console and CA UIM web page through HTTP.</li> <li>443 is the default port to access Admin Console and CA UIM web page through HTTPS.</li> </ul>                                                                                                                                                            |
| <b>Log Analytics</b>                           | 9200, 9092                          | Inbound, Outbound | See Details                                     | Open the following ports to allow communication between CA UIM and CA App Experience Analytics: <ul style="list-style-type: none"> <li>AXA Elasticsearch port (default 9200) - Open this port between CA App Experience Analytics and the location of the <code>log_monitoring_service</code> probe</li> <li>AXA Kafka Port (default 9092) - Open this port between CA App Experience Analytics and the location of the <code>axa_log_gateway</code> probe</li> </ul> |

## UIM Sizing Recommendations

Review the following reference material to understand the architecture and typical deployment of UIM. The recommendations and specifications that are listed below are based on the scale of deployment.

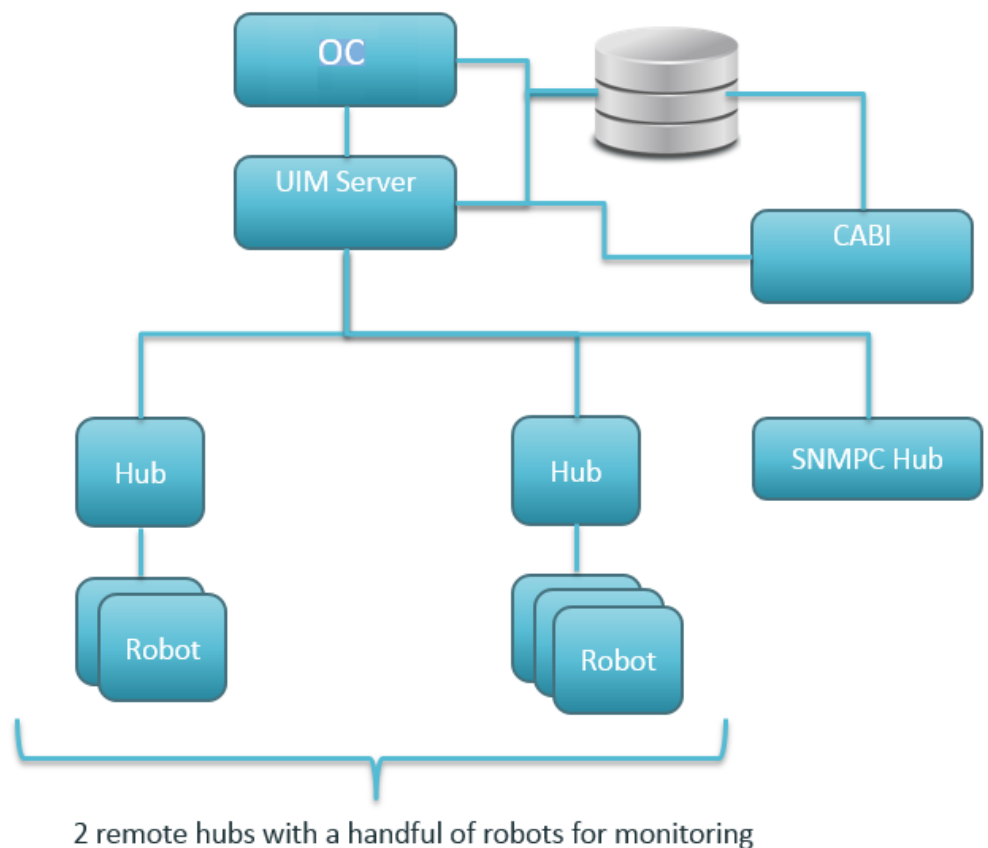
## Small Scale Reference Deployment Architecture

### High-Level Description

- A small company or individual team
- <500 devices monitored
- <5 hubs
- <200 robots
- A few concurrent users

### Architecture

## Small Scale Customer Representative Environment



### Specifications and Information

- Systems
  - Database
    - 8 cores x 2.8 Ghz
    - 12 GB RAM
    - One file system on 10k SAN
    - Disk Size: 100 GB (data storage that is expected to reach ~30-40 GB with retention settings below)
  - UIM

- 8 cores x 2.8 Ghz
- 12 GB RAM
- One filesystem on 10k SAN
- Disk Size: 100 GB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- OC
  - 8 cores x 2.8 Ghz
  - 12 GB RAM
  - One filesystem on 10k SAN
  - Disk Size: 50 GB
- CABI
  - 8 cores x 2.8 Ghz
  - 12 GB RAM
  - One filesystem on 10k SAN
  - Disk Size: 100 GB
- SNMPC hub
  - 4 cores x 2.8 Ghz
  - 8 GB RAM
  - One file system on 10k SAN
  - Disk Size: 100 GB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- General hubs
  - 4 cores x 2.8 Ghz
  - 8 GB RAM
  - One filesystem on 10k SAN
  - Disk Size: 50 GB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- Configuration
  - 100 robots
  - 1 SNMPC (100 devices)
- Performance
  - Sustained insert rate (used in example test environment):
    - Non-secure bus environment: 1500 msgs/sec
    - Secure bus environment: 1000 msgs/sec
  - Max insert rate:
    - Non-secure bus environment: 3500 msgs/sec
    - Secure bus environment: 2500 msgs/sec
- Recommended Configuration Parameters
  - Data\_engine insert threads that are increased by setting thread\_count\_insert=24 in data\_engine.cfg
  - Increase bulk size for data\_engine queue: hub\_bulk\_size = 2000
  - Data\_engine retention/maintenance settings – 7 days raw, 30 days hourly, 1 year daily
  - SNMPC – can use default max heap settings for javaopts (2G)



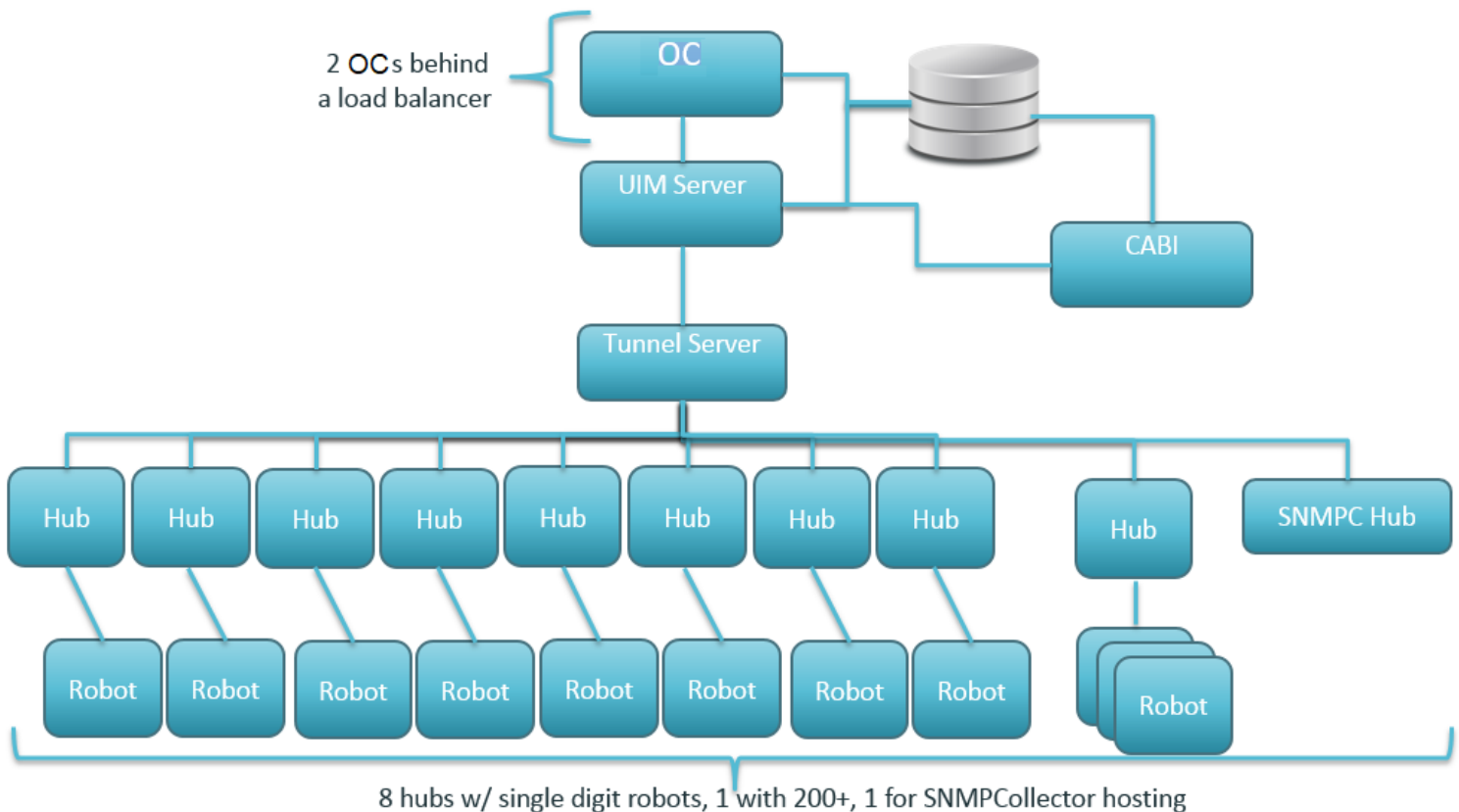
## Medium Scale Reference Deployment Architecture

### High-Level Description

- A medium-sized company or medium-sized lab/datacenter
- 500-1000 of devices monitored
- 5-20 hubs
- 200-1000 robots
- A dozen concurrent users

### Architecture

## Medium Scale Customer Representative Environment



### Specifications and Information

- Systems
  - Database
    - 16 cores x 2.8 Ghz
    - 16 GB RAM
    - One filesystem on 15k SAN
    - Disk Size: 500 GB (data storage that is expected to reach ~300 GB with retention settings below)
  - UIM

- 16 cores x 2.8 Ghz
- 16 GB RAM
- One filesystem on 15k SAN
- Disk Size: 100 GB for main drive and 100-300 GB for hub queues (as desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- OC
  - 16 cores x 2.8 Ghz
  - 16 GB RAM
  - One filesystem on 15k SAN
  - Disk Size: 50 GB
- CABI
  - 16 cores x 2.8 Ghz
  - 16 GB RAM
  - One filesystem on 15k SAN
  - Disk Size: 100 GB
- Tunnel Server hub
  - 8 cores x 2.8 Ghz
  - 8 GB RAM
  - One filesystem on 15k SAN
  - Disk Size: 200 GB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- SNMPC hub
  - 8 cores x 2.8 Ghz
  - 8 GB RAM
  - One filesystem on 10k SAN
  - Disk Size: 100 GB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- General hubs
  - 8 cores x 2.8 Ghz
  - 8 GB RAM
  - One filesystem on 10k SAN
  - Disk Size: 100 GB/1 TB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- Configuration
  - 200 robots
  - One snmpc (1,000 devices)
  - Ten groups
- Performance
  - Sustained insert rate (used in example test environment):
    - Non-secure bus environment: 5000 msgs/sec
    - Secure bus environment: 3500 msgs/sec
  - Max insert rate:
    - Non-secure bus environment: 10,000 msgs/sec
    - Secure bus environment: 7000 msgs/sec
- Recommended Configuration Parameters

- Data\_engine insert threads that are increased by setting thread\_count\_insert=24 in data\_engine.cfg
- Increase bulk size for data\_engine queue: hub\_bulk\_size = 2000
- Data\_engine retention/maintenance settings – 7 days raw, 30 days hourly, 1 year daily
- SNMPC – change default max heap settings for javaopts from 2G to 4G

**Recommendations**

- 15,000 drives in RAID 10 configuration recommended. If you expect high reporting needs, use SSD drives.

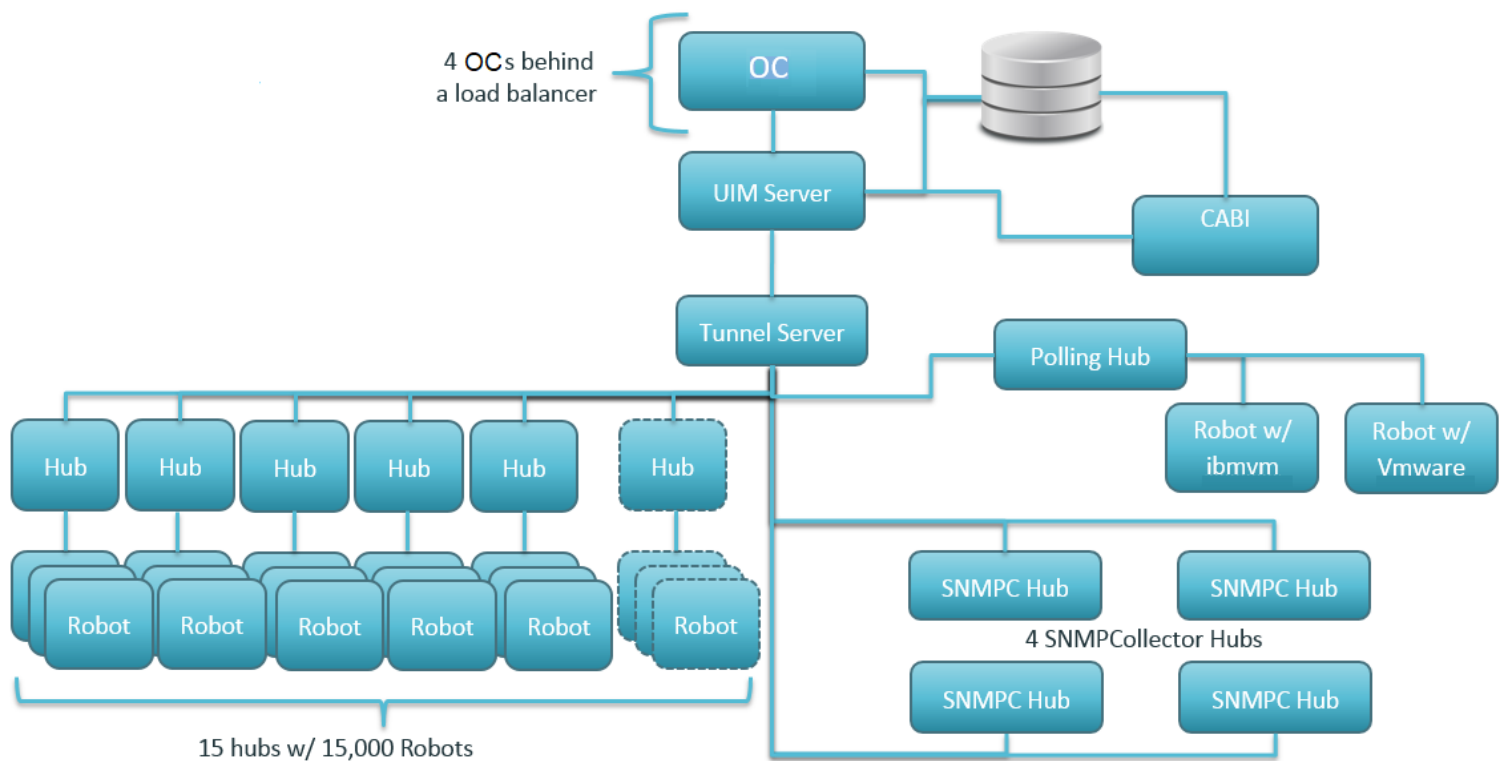
**Large-Scale Reference Deployment Architecture**

**High-Level Description**

- A large company or large datacenters
- 5-10K+ devices monitored
- 20+ hubs
- >1000 robots
- Dozens of concurrent users

**Architecture**

## Large Scale Customer Representative Environment



**Specifications and Information**

- Systems
  - Database

- 16 cores x 2.7 Ghz
- 32 GB RAM
- SSD SAN
- Log and Data on separate filesystems
- Disk Size: 2-3 TB (data storage that is expected to reach ~1.5 TB with retention settings below)
- UIM
  - 16 cores x 2.5 Ghz
  - 32 GB RAM
  - SSD SAN
  - Disk Size: 200 GB for main drive and 200-500 GB for hub queues (as desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- OC
  - 16 cores x 2.5 Ghz
  - 24 GB RAM
  - One filesystem on 15k SAN
  - Disk Size: 100 GB
- CABI
  - 16 cores x 2.8 Ghz
  - 32 GB RAM
  - One filesystem on 15k SAN
  - Disk Size: 100 GB
- Tunnel Server hub
  - 16 cores x 2.8 Ghz
  - 16 GB RAM
  - SSD SAN
  - Disk Size: 200 GB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows and additional drive that is dedicated to hub queues for resiliency)
- SNMPC hubs
  - 16 cores x 2.8 Ghz
  - 16 GB RAM
  - One filesystem on 10k SAN
  - Disk Size: 100 GB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- General hubs
  - 16 cores x 2.8 Ghz
  - 16 GB RAM
  - One filesystem on 10k SAN
  - Disk Size: 100 GB (more if desired to enable queues to fill up on disk in the case of extended outages or maintenance windows)
- Configuration
  - 15,000 robots
  - 4 SNMPC (8,000 devices)
  - 2.6 m metrics
  - 9,000 groups
- Performance
  - Sustained insert rate (used in example test environment):

- Non-secure bus environment: 15,000 msgs/sec
- Secure bus environment: 10,000 msgs/sec
- Max insert rate (tuned):
  - Non-secure bus environment: 35,000 msgs/sec
  - Secure bus environment: 25,000 msgs/sec
- Active alarm count:
  - Non-secure bus environment: 70,000
  - Secure bus environment: 70,000
- Max rate of alarm:
  - Non-secure bus environment: 100 alarms/sec
  - Secure bus environment: 70 alarms/sec
- Recommended Configuration Parameters
  - spooler\_inbound\_threads = 50 and check\_spooler\_session = 1 in primary hub.cfg
  - bulk\_size to 1500 for data\_engine queue
  - bulk\_size to 1000 for baseline engine queue
  - Data\_engine insert threads that are increased by setting thread\_count\_insert = 24 in data\_engine.cfg
  - Data\_engine queue limit increase: queue\_limit\_total = 1000000
  - Increase bulk size for data\_engine queue: hub\_bulk\_size = 2000
  - Data\_engine retention/maintenance settings – 7 days raw, 30 days hourly, 1 year daily
  - SNMPC – change default max heap settings for javaopts from 2G to 8G for each SNMPC probe
  - nas probe changes:
    - nis\_batch\_mode = 1
    - nis\_batch\_size = 5000 (default is 1000)

**NOTE**

The total number of QoS messages that are supported in the database are to a maximum of 2000000.

**Recommendations**

- SSD drives should be used when deploying environments this large for better reporting and DB performance.

**Additional Sizing Considerations and Information**

- Plan to leave enough headroom for expansion and ability to catch up after planned outages.
  - For example, if your environment has a max message rate of 50,000 messages/sec and typically runs at a steady state of 15,000 messages/sec then a one-hour outage window will accumulate 54,000,000 messages.
- High volume hub Disk speed/IO capacity (primary hub, tunnel server) can aid in processing - that is, SSD drive for queues.
- Database disk speed/IO capacity can help insert rate and report processing speed – SSDs for the database is highly recommended.
- Database platform/version can improve performance or can enable additional scale capability.

- Partitioning is recommended for large deployments and is supported by Oracle, MySQL, and MSSQL Enterprise.
- MSSQL 2014 supports per-partition online rebuild of indexes – minimizes table locks during partitioning making data maintenance more efficient.
- Reserve CPU/Memory for UIM/tunnel server/database virtual machines to increase speed and dedicated resources.
- An intermediate proxy/concentrator hub is often used to offload metric processing and tunnel termination from the primary UIM server (see medium and large environment recommendations).
- To minimize firewall configuration and enable a cleaner architecture, tunnel can be used to connect UIM hub components in a distributed customer environment.
- Linux tunnel server hubs are known to scale the best in terms of raw message rate and number of subscribers supported.
- For optimal hub/robot performance, it is recommended that no more than 2000 robots be deployed per hub. For more information, refer [KB article](#).
- For extensive monitoring, a maximum of 150 QoS metrics per device is recommended.
- If CABI is deployed on the Operator Console, you must add 8 GB RAM and 8 CPU cores to your OC environment.

## Product Compatibility

The articles in this section help you to plan and prepare your UIM Installation by listing the supportability for all UIM components:

Once you review this information, you can proceed to the article [Install UIM Server](#).

## Supported Install/Upgrade Paths

This section highlights installation/migration paths that are supported for UIM components.

### Unified Infrastructure Management (UIM)

- UIM 20.3.1 to UIM 20.3.3
- UIM 20.3.0 to UIM 20.3.3

**NOTE**

For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.

- UIM 20.3.0 to UIM 20.3.1

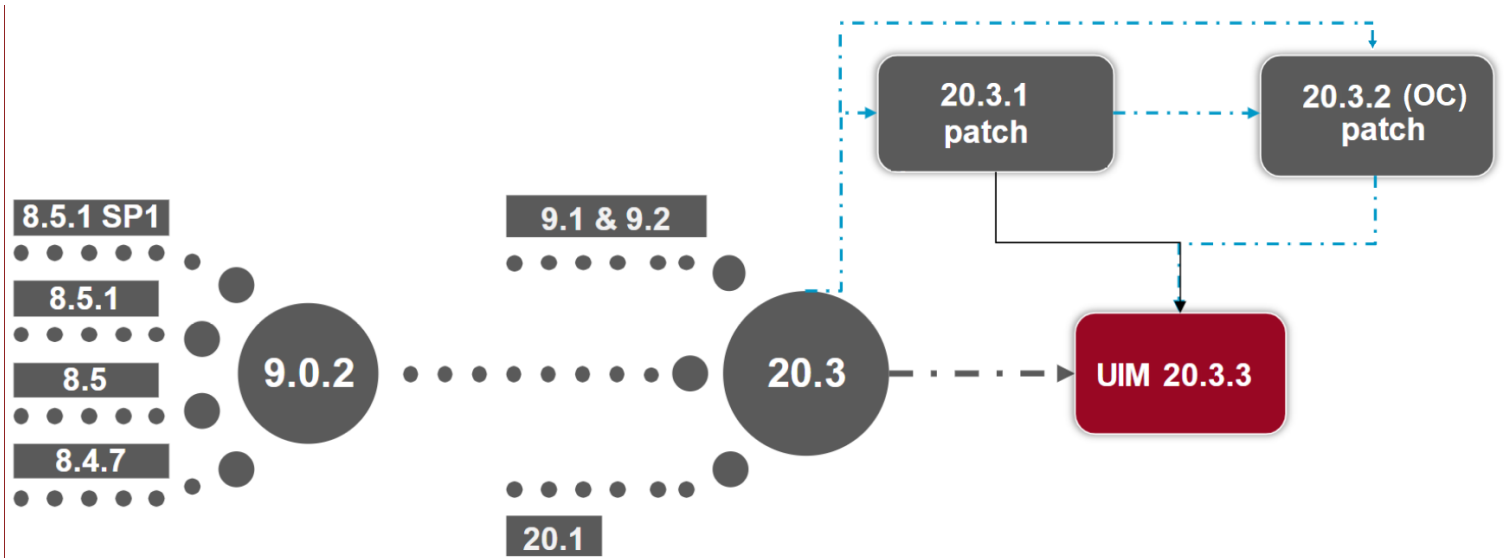
**NOTE**

UIM 20.3.1 is a patch release over UIM 20.3.0. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes the OC upgrade installer along with the separate standalone artifacts that you can use to upgrade the respective components to 20.3.1. For more information about the artifacts that are available as a part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.

- UIM 20.1.0 to UIM 20.3.0
- UIM 9.x.x to UIM 20.3.0

**NOTE**

If you are using any older version of UIM that is prior to UIM 9.0.2, you must first upgrade to UIM 9.0.2 and then can upgrade to UIM 20.3.0.

**NOTE**

- Direct installation of UIM 20.3.3 is not supported; that is, you cannot directly install UIM 20.3.3. You must follow the proper upgrade path as shown in the diagram.
- For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.
- OC 20.3.2 is a patch release. For more information about the OC 20.3.2 patch, see the [OC 20.3.2 Patch](#) article.
- UIM 20.3.1 is a patch release over UIM 20.3.0. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes the OC upgrade installer along with the separate standalone artifacts that you can use to upgrade the respective components to 20.3.1. For more information about the artifacts that are available as a part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.

**Operator Console (OC)**

- OC 20.3.2 to OC 20.3.3
- OC 20.3.1 to OC 20.3.3
- OC 20.3.0 to OC 20.3.3

**NOTE**

For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.

- OC 20.3.1 to OC 20.3.2
- OC 20.3.0 to OC 20.3.2

**NOTE**

OC 20.3.2 is a patch release. For more information about the OC 20.3.2 patch, see the [OC 20.3.2 Patch](#) article.

- OC 20.3.0 to OC 20.3.1

**NOTE**

UIM 20.3.1 is a patch release over 20.3.0. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes the OC upgrade installer along with the separate standalone artifacts that you can use to upgrade the respective components to 20.3.1. For more information about the artifacts that are available as a part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.

- UMP 20.1.0 to OC 20.3.0
- UMP 9.x.x to OC 20.3.0

**NOTE**

If you are using any older version of UMP that is prior to UMP 9.0.2, you must first upgrade to UMP 9.0.2 and then can upgrade to OC 20.3.0.

## UIM Compatibility Matrix

### Compatibility Matrix

This section highlights the compatibility for the UIM components.

| Component  | OC 20.3.3  | OC 20.3.2  | OC 20.3.1  | OC 20.3    | UMP 20.1   | UMP 9.0.2  |
|------------|------------|------------|------------|------------|------------|------------|
| UIM 20.3.3 | <b>yes</b> | <b>x</b>   | <b>x</b>   | <b>x</b>   | <b>x</b>   | <b>x</b>   |
| UIM 20.3.1 | <b>x</b>   | <b>yes</b> | <b>yes</b> | <b>x</b>   | <b>x</b>   | <b>x</b>   |
| UIM 20.3   | <b>x</b>   | <b>x</b>   | <b>x</b>   | <b>yes</b> | <b>x</b>   | <b>x</b>   |
| UIM 20.1   | <b>x</b>   | <b>x</b>   | <b>x</b>   | <b>x</b>   | <b>yes</b> | <b>x</b>   |
| UIM 9.0.2  | <b>x</b>   | <b>x</b>   | <b>x</b>   | <b>x</b>   | <b>x</b>   | <b>yes</b> |

**NOTE**

- UIM 20.3.1 is a patch release over UIM 20.3.0. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes the OC upgrade installer along with the separate standalone artifacts that you can use to upgrade the respective components to 20.3.1. For more information about the artifacts that are available as a part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.
- OC 20.3.2 is a patch release. For more information about OC 20.3.2, see the [OC 20.3.2 Patch](#) article.
- For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.

### Component Support Matrix

|                      | Operating Systems         |                                                                                                                          | Browsers <sup>2</sup> |                      |                      | Databases |            |                                                                             | Java JRE |
|----------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------|-----------------------|----------------------|----------------------|-----------|------------|-----------------------------------------------------------------------------|----------|
|                      | Windows (64-bit)          | Linux (64-bit)                                                                                                           | Edge                  | Firefox              | Chrome               | Oracle    | MySQL      | MSSQL                                                                       |          |
| <b>UIM/OC 20.3.3</b> | 2012, 2012 R2, 2016, 2019 | SLES 11, SLES 12.x, SLES 15, OpenSuse 12, OpenSuse 13, Red Hat 6, Red Hat 7.x, Red Hat 8, CentOS 6, CentOS 7, CentOS 8.x | 79 <sup>2</sup>       | Version 80 or higher | Version 85 or higher | 12<br>19  | 5.6<br>5.7 | 2012 <sup>4</sup><br>2014 <sup>4</sup><br>2016 <sup>4</sup><br>2017<br>2019 | Java 8   |



|                                                           |                           |                                                                                                                          |                 |                      |                      |            |            |                                                                     |        |
|-----------------------------------------------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------|-----------------|----------------------|----------------------|------------|------------|---------------------------------------------------------------------|--------|
| <b>UIM/OC 20.3.1 (and OC 20.3.2) (Patch)</b> <sup>5</sup> | 2012, 2012 R2, 2016, 2019 | SLES 11, SLES 12.x, SLES 15, OpenSuse 12, OpenSuse 13, Red Hat 6, Red Hat 7.x, Red Hat 8, CentOS 6, CentOS 7, CentOS 8.x | 79 <sup>2</sup> | Version 80 or higher | Version 85 or higher | 12<br>19   | 5.6<br>5.7 | 2012 <sup>4</sup><br>2014 <sup>4</sup><br>2016 <sup>4</sup><br>2017 | Java 8 |
| <b>UIM/OC 20.3</b>                                        | 2012, 2012 R2, 2016, 2019 | SLES 11, SLES 12.x, SLES 15, OpenSuse 12, OpenSuse 13, Red Hat 6, Red Hat 7.x, Red Hat 8, CentOS 6, CentOS 7, CentOS 8.x | 79 <sup>2</sup> | Version 80 or higher | Version 85 or higher | 12<br>19   | 5.6<br>5.7 | 2012 <sup>4</sup><br>2014 <sup>4</sup><br>2016 <sup>4</sup><br>2017 | Java 8 |
| <b>UIM/UMP 20.1</b>                                       | 2012, 2012 R2, 2016, 2019 | SLES 11, SLES 12.x, SLES 15, OpenSuse 12, OpenSuse 13, Red Hat 6, Red Hat 7.x, Red Hat 8, CentOS 6, CentOS 7             | 79 <sup>2</sup> | Version 60 or higher | Version 65 or higher | 12<br>19   | 5.6<br>5.7 | 2012 <sup>4</sup><br>2014 <sup>4</sup><br>2016 <sup>4</sup><br>2017 | Java 8 |
| <b>UIM/UMP 9.2.0</b>                                      | 2012, 2012 R2, 2016       | SLES 11, SLES 12.x, OpenSuse 12, OpenSuse 13, Red Hat 6, Red Hat 7.x, CentOS 6, CentOS 7                                 | 79 <sup>2</sup> | Version 35 or higher | Version 45 or higher | 11.2<br>12 | 5.6<br>5.7 | 2012 <sup>4</sup><br>2014 <sup>4</sup><br>2016 <sup>4</sup><br>2017 | Java 8 |

|                      |                     |                                                                                          |                 |                      |                      |            |            |                                                                     |        |
|----------------------|---------------------|------------------------------------------------------------------------------------------|-----------------|----------------------|----------------------|------------|------------|---------------------------------------------------------------------|--------|
| <b>UIM/UMP 9.0.2</b> | 2012, 2012 R2, 2016 | SLES 11, SLES 12.x, OpenSuse 12, OpenSuse 13, Red Hat 6, Red Hat 7.x, CentOS 6, CentOS 7 | 79 <sup>2</sup> | Version 35 or higher | Version 45 or higher | 11.2<br>12 | 5.6<br>5.7 | 2012 <sup>4</sup><br>2014 <sup>4</sup><br>2016 <sup>4</sup><br>2017 | Java 8 |
|----------------------|---------------------|------------------------------------------------------------------------------------------|-----------------|----------------------|----------------------|------------|------------|---------------------------------------------------------------------|--------|

## NOTE

1. UIM supports the minor version for a supported major version.
2. The Operator Console is certified on Chromium based Microsoft Edge.
3. The CABI TLS v1.2 feature available with cabi probe 4.10 bundled supports TLS v1.2 when communicating with the CA UIM database: Microsoft SQL Server - 2012, 2014, 2016<sup>7</sup>, and Oracle - 11.2 and 12.1. Note that UIM 20.1 (and later) do not support Oracle 11.2.
4. The CABI TLS v1.2 feature is not supported for Microsoft SQL Server 2012, 2014, and 2016 when installed on Windows Server 2016.
5. UIM 20.3.1 is a patch release over UIM 20.3.0. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes the OC upgrade installer along with the separate standalone artifacts that you can use to upgrade the respective components to 20.3.1. For more information about the artifacts that are available as a part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.
6. OC 20.3.2 is a patch release. For more information about OC 20.3.2, see the [OC 20.3.2 Patch](#) article.
7. For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.

## Robot Support Matrix

| Supported Operating Systems | Robot 7.96     | Robot 7.97 | Robot 9.20 | Robot 9.20S | Robot 9.30 | Robot 9.30S | Robot 9.31 | Robot 9.31S | Robot 9.32 | Robot 9.32S | Robot 9.33 | Robot 9.33S |     |
|-----------------------------|----------------|------------|------------|-------------|------------|-------------|------------|-------------|------------|-------------|------------|-------------|-----|
| AIX                         | PowerPC 64 6.1 | yes        | yes        | yes         | x          | yes         | x          | yes         | x          | yes         | x          | yes         | x   |
|                             | PowerPC 64 6.2 | yes        | yes        | yes         | x          | yes         | x          | yes         | x          | yes         | x          | yes         | x   |
|                             | PowerPC 64 7.0 | yes        | yes        | yes         | x          | yes         | x          | yes         | x          | yes         | x          | yes         | x   |
|                             | PowerPC 64 7.1 | yes        | yes        | yes         | x          | yes         | x          | yes         | x          | yes         | x          | yes         | x   |
|                             | PowerPC 64 7.2 | yes        | yes        | yes         | x          | yes         | x          | yes         | x          | yes         | x          | yes         | x   |
| HPUX                        | 11.3 (IA64)    | yes        | yes        | yes         | x          | yes         | x          | yes         | x          | yes         | x          | yes         | x   |
|                             | 11.3 (PA-RISC) | yes        | yes        | yes         | x          | yes         | x          | x           | x          | x           | x          | x           | x   |
| Linux                       | Amazon Linux 2 | x          | yes        | yes         | yes        | yes         | yes        | yes         | yes        | yes         | yes        | yes         | yes |

|                      |     |     |     |     |     |     |     |     |     |     |     |     |
|----------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| CentOS 6<br>x86_32   | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| CentOS 6<br>x86_64   | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| CentOS 7<br>x86_32   | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| CentOS 7<br>x86_64   | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| CentOS 8<br>x86_32   | x   | x   | x   | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| CentOS 8<br>x86_64   | x   | x   | x   | x   | yes | yes | yes | yes | yes | yes | yes | yes |
| Debian 7<br>x86_64   | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| Debian 8<br>x86_64   | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| Debian 9<br>x86_64   | x   | x   | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| OpenSuse19<br>x86_32 | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| OpenSuse19<br>x86_64 | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| OpenSuse19<br>x86_32 | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| OpenSuse19<br>x86_64 | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| RHEL 5<br>x86_32     | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| RHEL 5<br>x86_64     | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| RHEL 6<br>x86_32     | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| RHEL 6<br>x86_64     | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| RHEL 7.x<br>x86_32   | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| RHEL 7.x<br>x86_64   | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |

|                                 |     |     |     |     |     |     |     |     |     |     |     |     |
|---------------------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| RHEL 8 x86_32                   | x   | x   | x   | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| RHEL 8 x86_64                   | x   | x   | x   | x   | yes | yes | yes | yes | yes | yes | yes | yes |
| SLES 11 x86_32                  | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| SLES 11 x86_64                  | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| SLES 12.x x86_32                | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| SLES 12.x x86_64                | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| SLES 15 x86_32                  | x   | x   | x   | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| SLES 15 x86_64                  | x   | x   | x   | x   | yes | yes | yes | yes | yes | yes | yes | yes |
| SUSE 11 x86_64                  | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| SUSE 12 x86_64                  | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| SUSE 12.x x86_32                | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| SUSE 12.x x86_64                | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| Ubuntu 12 x86_32                | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |
| Ubuntu 14 x86_64                | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| Ubuntu 16 x86_64                | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| Ubuntu 18.04 x86_64 LTS         | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| Ubuntu 20.04 LTS (Intel 64-bit) | x   | x   | x   | x   | x   | x   | x   | x   | x   | x   | yes | yes |

|                                                 |                                                            |     |     |     |     |     |     |     |     |     |     |     |     |     |
|-------------------------------------------------|------------------------------------------------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| PowerPC<br>64<br>Little-<br>endian<br>(ppc64le) | RHEL<br>7.x                                                | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |     |
|                                                 | SUSE<br>12.x                                               | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |     |
| Solaris                                         | SPARC64<br>10                                              | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |     |
|                                                 | SPARC64<br>11                                              | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |     |
|                                                 | x86 10                                                     | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |     |
|                                                 | x86 11                                                     | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |     |
|                                                 | x86_64<br>10                                               | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |     |
|                                                 | x86_64<br>11                                               | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |     |
| Windows                                         | 7 32-bit                                                   | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | x   |     |
|                                                 | 7 64-bit                                                   | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | 8 32-bit                                                   | yes | yes | yes | x   | yes | x   | yes | x   | yes | x   | yes | yes |     |
|                                                 | 8 64-bit                                                   | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | 10 64-<br>bit                                              | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | 2012<br>64-bit                                             | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | 2012<br>R2 64-<br>bit                                      | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | 2016<br>64-bit<br>(Essentials,<br>Standard,<br>Datacenter) | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
|                                                 | 2019<br>64-bit<br>(Essentials,<br>Standard,<br>Datacenter) | x   | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |
| zLinux                                          | RHEL 6                                                     | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | RHEL<br>7.x                                                | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | RHEL 8                                                     | x   | x   | x   | x   | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | SLES<br>11                                                 | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | SLES<br>12.x                                               | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes | yes |     |
|                                                 | SLES<br>15                                                 | x   | x   | x   | x   | yes | yes | yes | yes | yes | yes | yes | yes |     |

**NOTE**

- Secure robot is supported only on Linux x64-bit and Windows x64-bit environments.

2. UIM supports the minor version for a supported major version.
3. In CA UIM 20.3.0, robot installation on ppc64le through ADE is not supported.

| Supported Operating System                            |              | Robot 5.50 | Robot 5.71 | Robot 5.73 | Robot 5.77* |
|-------------------------------------------------------|--------------|------------|------------|------------|-------------|
| IBM i (Previously known as OS/400, AS/400, and i5/OS) | V5R3 iSeries | yes        | yes        | yes        | x           |
|                                                       | V5R4 iSeries | yes        | yes        | yes        | x           |
|                                                       | V6R1 iSeries | yes        | yes        | yes        | yes         |
|                                                       | 7.1          | yes        | yes        | yes        | yes         |
|                                                       | 7.2          | yes        | yes        | yes        | yes         |
|                                                       | 7.3          | yes        | yes        | yes        | yes         |

**NOTE**

1. IBM iRobot 5.77 contains only the robot\_update. It does not contain the robot.

**Automated Deployment Engine**

Robot deployment using the Automated Deployment Engine (ADE) probe.

|                         |                                                  | Deploy from ADE |         |         |
|-------------------------|--------------------------------------------------|-----------------|---------|---------|
| Deploy to Target System |                                                  | Linux           | Solaris | Windows |
|                         | <b>POSIX (AIX, HPUX, Linux, Solaris, zLinux)</b> | Yes             | Yes     | Yes     |
|                         | <b>Windows</b>                                   | Yes*            | Yes*    | Yes     |

\*A Linux primary NMS hub can deploy Windows robots if the hub is a Windows hub. This enables the ADE to run Windows to Windows commands.

**CA UIM Probes Support Matrix**

[Platform Support Availability - PDF](#)

[Platform Support Availability - Spreadsheet](#)

**Install UIM Server**

This article explains how to install UIM Server for the first time. After you have completed pre-installation, you can run the installer for UIM Server. The following topics cover the complete information:

**Tasks Performed**

The UIM Server is the foundation of the CA UIM solution and consists of:

- The Message Bus
- The Domain
- The Primary Hub
- A robot and core probes
- The UIM Server web page, which contains links to installers for client systems
- The UIM Database
- The required UIM Server and Database user accounts

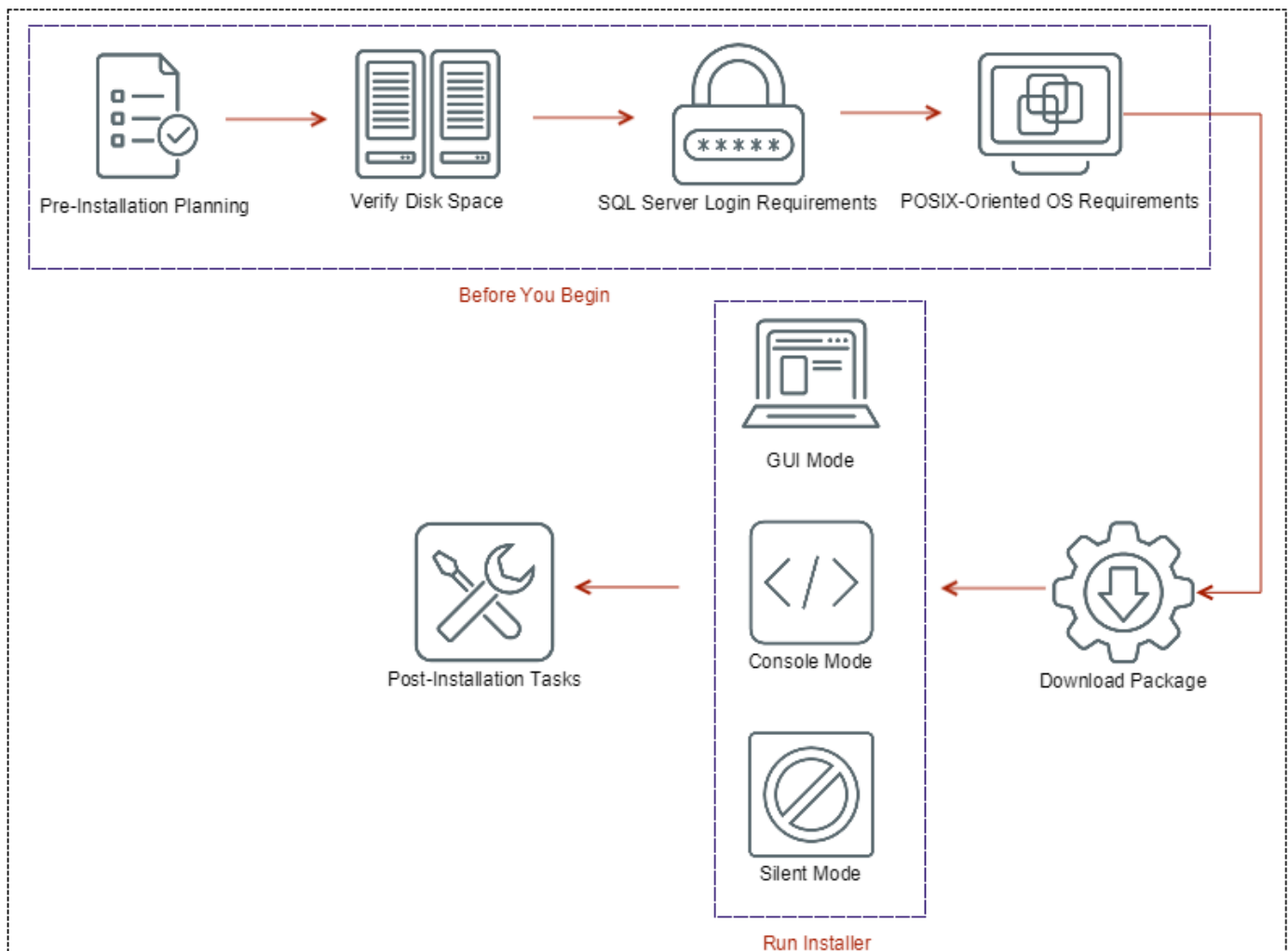
The UIM Server installer performs the following tasks:

- Installs the Primary Hub, the core of the UIM message bus.
- Creates your database (if not created during database software installation).
- Creates your UIM domain.
- Installs your UIM Server Home Page, which provides access to administrative consoles and UIM component install packages.
- Installs your local archive, which contains probes and packages.

### High-Level Process

The following diagram shows the high-level steps that are required for the UIM Server installation:

**Figure 6: Install UIM Server Process**



### Before You Begin

Complete the following tasks before you install UIM Server:

1. Perform Pre-Installation Planning

2. Verify Required Disk Space
3. Microsoft SQL Server Log in Requirements
4. POSIX-Oriented Operating System Requirements

**NOTE**

If you are installing on Windows 2008 R2 64-bit, ensure that you have the Microsoft Visual C++ 2008 64-bit runtime libraries already installed; otherwise, installer will fail.

**Perform Pre-Installation Planning**

Read and understand the prerequisites that are detailed in [Pre-Installation Planning](#). Pre-Installation planning covers the hardware, operating system, and database software requirements for CA UIM.

**NOTE**

To configure CA UIM in a pure IPv6 environment review [Configure IPv6 Support](#).

**Verify Required Disk Space**

Ensure that you have the necessary disk space:

- 15-GB available disk space is recommended for UIM Server.
- The installer requires 2.1 GB of temporary space to unpack the files.

**NOTE**

: On Linux, the installer unpacks to /tmp/install.dir.xyz, where xyz is a random number. If /tmp does not have 2.1 GB available, the installer uses the home directory of the user running the installer (root).

**Microsoft SQL Server Log in Requirements**

If you are using Microsoft SQL Server for the UIM database, log in to the system using the database account that you designated during [Pre-Installation Planning](#). If you are using Microsoft SQL Server with Windows authentication, verify that a domain administrator has permission to **log on as a service** on both the primary hub server and the database server, and that SQL Server is configured to use Windows authentication. For more information about the **log on as a service** right, see the Microsoft article [https://technet.microsoft.com/en-us/library/cc739424\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc739424(v=ws.10).aspx).

**POSIX-Oriented Operating System Requirements**

Root access is required to run the UIM Server installer.

**Download the UIM Server Install Package****Follow these steps:**

1. Log in to the UIM server as administrator.
2. Log in to [support.broadcom.com](http://support.broadcom.com) and locate the installation packages in [Download Management](#).

**NOTE**

A CA support login is required.

3. Download the following installation packages for your operating system:
  - The UIM Server Installer (**setupCAUIMServer** executable)
  - The UIM Server Packages (**uimserverpackages** zip file)

**WARNING**

Both files are required on the system that hosts the UIM server. If the uimserverpackages zip file is not present, the installation fails.



4. **(Silent Mode Only)** Download the **Silent Install Templates for UIM Server** zip package.
5. **(Linux Only)** Run the **chmod 755** command on the setupCAUIMServer executable file.

### **Run the UIM Server Installer**

You can run the installer in one of the following modes:

- GUI Mode
- Console Mode
- Silent Mode

The installer log file is located in /tmp/ca\_uim.

#### **GUI Mode**

Graphical user interface (GUI) mode walks you through the installation process.

#### **Follow these steps:**

1. Follow the prompts to complete the installation. Database server parameters and hub configuration values are case-sensitive. For help, you can hover over the tooltip buttons next to the fields or refer to the article [Installation Parameters](#).
2. Allow the process to complete. Note the following items:
  - Post configuration can take several minutes.
  - A warning that one or more probes did not activate before the installer finished does not necessarily represent an issue. Some probes might not finish their startup sequence before the installer displays its final screen.

#### **Console Mode**

Console mode provides an interactive command-line interface.

#### **Follow these steps:**

1. From a command line, execute the appropriate command:
 

```
setupCAUIMServer.exe -i console (Windows systems)
setupCAUIMServer.bin -i console (Linux systems)
```
2. Follow the prompts to set up your database and specify your hub and robot information. Database server parameters and hub configuration values are case-sensitive. The parameters are defined in the article [Installation Parameters](#).
3. Allow the process to complete. Note the following items:
  - Post configuration can take several minutes.
  - **(Linux Only)** To see the progress of the installation in detail, execute:
 

```
$ tail -f /tmp/ca_uim/uimserver_ia_install.log
```
4. UIM Server launches. If for some reason it does not, execute:
  - Windows: **net start "Nimsoft Robot Watcher"**

#### **NOTE**

The NT service named 'Nimsoft Robot Watcher' can also be administered through the 'Services' Administrative Tools control panel application.

- Linux: **/etc/init.d/nimbus start**

#### **Silent Mode**

If you do not want to monitor your product installation for GUI inputs, you can use a silent mode installation. During a silent-mode installation, the UIM installer reads your defined installation parameters from **installer.properties** file. A silent-mode installation:

- Does not display configuration options.
- Does not require any customer interaction after the creation of the properties file.

### Follow these steps:

1. Prepare your response file:
  - a. Extract the silent install template zip file.
  - b. Locate the **uimserver\_silentinstall\_master.properties** file that corresponds to your system setup, and save the file as **installer.properties** in the same directory as the UIM Server installation executable binary file.
  - c. In **installer.properties**, enter or change the parameter values as needed. All lines that do not begin with a **#** symbol must have a value. For more information, refer to the article [Installation Parameters](#).
  - d. Save the file, ensuring the file type is still **PROPERTIES**. If the file type is **Text Document**, remove the **.txt** extension (which might not be displayed in the folder).
2. Run the installer. From a command line, execute the appropriate command:

```
setupCAUIMServer.exe -i silent (Windows systems)
```

```
setupCAUIMServer.bin -i silent (Linux systems)
```

3. The installer unpacks the files and completes the installation. This process can take several minutes or more. To see the progress of the installation, execute:

```
tail -f /tmp/ca_uim/uimserver_ia_install.log
```

4. UIM Server launches. If for some reason it does not, execute:
  - Windows: **net start "Nimsoft Robot Watcher"**

#### TIP

The NT service named 'Nimsoft Robot Watcher' can also be administered through the 'Services' Administrative Tools control panel application.

- Linux: **/etc/init.d/nimbus start**

#### NOTE

(For Microsoft SQL Server with NT Authentication) After installation, ensure that the **Nimsoft Robot Watcher NT** service Logon User is the same as the one used during UIM Server installation. Since this service starts the robot, the **Nimsoft Robot Watcher** user also requires full permissions to the UIM Server installation folder and logon privileges to the SQL Server. Also, we recommend against changing the logon user value, which could result in the robot either not being able to start or unable to function correctly due to file permission issues. If a change is made, be sure that the login user is specified in the <domain>\<nt\_username> format so that the user has full permissions to the install directory contents.

### Additional Information

Review the following additional information:

- CA UIM 9.0.2 removes dependency on the end-of-life (EOL) Microsoft Visual C++ Redistributables for a [few probes and packages](#). Because of this dependency removal, CA UIM 9.0.2 installation deploys the Microsoft Visual C++ 2017 Redistributables package (for example, vs2017\_vccredist\_x86) by default. With this package deployment, only the listed probes can work. For other probes that use the EOL Microsoft Visual C++ Redistributables or for older versions of the impacted probes, you must download and deploy the required EOL Microsoft Visual C++ Redistributable package (for example, vs2008\_redist\_x86) from the Archive.
- Furthermore, if you want to use the impacted probes with CA UIM releases prior to CA UIM 9.0.2, ensure that you download and deploy the required Microsoft Visual C++ 2017 Redistributables package that is available in the Archive.
- The UIM Server installer creates a .pem file (certificate.pem) in the <Nimsoft>\security folder. The .pem file is a symmetric key that is shared with the required robots, which is then used for communication with the data\_engine probe. You copy this .pem file to the remote OC robot, UR robot, CABI robot, and HA system (if available) and provide the location of the file in the robot.cfg file (cryptkey = <.pem file location> ). Furthermore, if any [impacted probe](#) is not on the same computer where data\_engine is present, copy the generated .pem file to the robot computer

(where `data_engine` is not available) and update the `robot.cfg` file with the `.pem` file location on that computer. For more information about the `robot.cfg` file configuration, see [Configure the robot.cfg File](#).

## Options After Installation

### WARNING

If you shut down any anti-virus software or firewalls before installation, turn them back on now.

Once you have installed UIM Server, you have several options on how to proceed:

- [Log in to Admin Console](#) - The Admin Console application allows you to manage and maintain the hubs, robots, and probes on your CA UIM system.
- [Install Infrastructure Manager](#) - Infrastructure Manager is a thick client console that is required for some UIM infrastructure management tasks.
- [Install Secondary Hubs](#) - Most deployments have at least one extra Secondary Hub for load balancing.
- [Install Operator Console \(OC\)](#) - OC presents the performance and availability data CA UIM collects.

### NOTE

To Upgrade an existing installation, see [Upgrade CA UIM](#).

To reinstall, first, uninstall the software, then restart the installation process. Your server configuration information (domain and hub names, IP addresses, user accounts, and passwords) is not retained.

## Installation Parameters

This article describes the parameters that are used during CA UIM installation. The parameters that are required during your installation vary depending on:

- The installation method that you are using.
- The database software that you are using for the UIM database.

The following topics cover the information:

### GUI and Console Parameters

The GUI and console installation processes prompt you for the parameters that are required for your operating system, database, and secure mode.

- [Port Parameters](#)
- [MySQL Parameters \(GUI/Console\)](#)
- [SQL Server Parameters \(GUI/Console\)](#)
- [Oracle Parameters \(GUI/Console\)](#)
- [Hub Parameters \(GUI/Console\)](#)

### Port Parameters

| Parameter      | Value                                                                           |
|----------------|---------------------------------------------------------------------------------|
| WASP HTTP Port | The port for accessing Admin Console, OC, and the UIM Home Page (default is 80) |

**MySQL Parameters (GUI/Console)**

| Parameter                              | Value                                                                                                                                                |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database Server Hostname or IP         | Database server hostname or IP address. If you have selected IPv6 installation environment, then enter the IPv6 address as database server hostname. |
| Database Server Name                   | Desired name for a new database, or the name of the UIM database that is created before UIM Server installation                                      |
| Database Port                          | Database server port (typically 3306)                                                                                                                |
| Database Name                          | Enter CA_UIM or the name of your choice                                                                                                              |
| Database Username<br>Database Password | Database administrative account (root) and password                                                                                                  |

**SQL Server Parameters (GUI/Console)**

| Parameter                      | Value                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database Server Hostname or IP | Database Server hostname or IP address. If you have selected IPv6 installation environment, then enter the IPv6 address as database server hostname.                                                                                                                                                                                                                         |
| Database Server Port           | <ul style="list-style-type: none"> <li>Database server port if the port is assigned (default is 1433)</li> </ul>                                                                                                                                                                                                                                                             |
| Database Name                  | <ul style="list-style-type: none"> <li>CA_UIM (default) or name of your choice for a new database</li> <li>Actual name of the UIM database that is created before UIM Server installation</li> </ul>                                                                                                                                                                         |
| Database Authentication Mode   | <ul style="list-style-type: none"> <li>SQL Server Authentication to use the database to authenticate credentials</li> <li>Windows Authentication to use Active Directory to authenticate credentials</li> </ul>                                                                                                                                                              |
| Database Username              | <ul style="list-style-type: none"> <li>Username for a SQL Server user account on the database server if you chose SQLServer Authentication (default is sa)</li> <li>Domain/username for a Windows account if you chose Windows Authentication</li> </ul> <p><b>Note:</b> If you chose <b>Create New Database</b> mode, this account must have administrative privileges.</p> |
| Database Password              | <ul style="list-style-type: none"> <li>Password for existing database administrator account</li> <li>Desired password if the account is created during CA UIM installation.</li> </ul>                                                                                                                                                                                       |
| Enable TLS                     | Select the option to enable TLS v1.2 in CA UIM, which lets the UIM Server establish secure communication with the UIM database (Microsoft SQL Server in this case).<br>For more information about TLS v1.2 support, see the Support for TLS v1.2 section in <a href="#">Microsoft SQL Server</a> .                                                                           |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TrustStore Path     | Specify the location of the generated .jks file. The UIM Server installer copies the .jks file from the specified location and places it in the<br><pre>&lt;uim&gt;\Nimsoft\security</pre> folder during the installation. The installer then renames the copied file to truststore.jks. This file includes your database server certificate. For more information about how to create a .jks file, see the Support for TLS v1.2 section (Create a .jks File for Server Certificate) in <a href="#">Microsoft SQL Server</a> . |
| TrustStore Password | Specify the password to access the source .jks file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### Oracle Parameters (GUI/Console)

| Parameter                       | Value                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Oracle Instant Client Directory | Location of Oracle Instant Client (required)                                                                                                                                                                                                                                                                 |
| Database Server Name            | <ul style="list-style-type: none"> <li>• Hostname</li> <li>• IPv4 address</li> </ul>                                                                                                                                                                                                                         |
| Database Server Port            | Database server port (typically 1521)                                                                                                                                                                                                                                                                        |
| Database Service Name           | <ul style="list-style-type: none"> <li>• Oracle service name to use for the database connection (default is ORCL)</li> <li>• (Oracle 12 ONLY) Pluggable database name</li> </ul>                                                                                                                             |
| SYS Password                    | Password for the SYS account on the database server (required only if database is created during installation)                                                                                                                                                                                               |
| Database Username               | <ul style="list-style-type: none"> <li>• Desired name for the UIM database user account that the installer creates (new)</li> <li>• Database user who is created when database was created (existing)</li> </ul>                                                                                             |
| Database Password               | Password for the UIM database administrator account                                                                                                                                                                                                                                                          |
| Database Tablespace Name        | Tablespace name to associate with the database username schema. Valid characters are: a-z, A-Z, 0-9 and underscore (_)                                                                                                                                                                                       |
| Enable TLS                      | Select the option to enable TLS v1.2 in CA UIM, which lets the UIM Server establish secure communication with the UIM database (Oracle in this case). For more information about TLS v1.2 support, see the Support for TLS v1.2 section in <a href="#">Oracle</a> .                                          |
| Wallet Location                 | Specify the location of the wallet where your security certificates are available. This location includes your trusted security certificates. The same security certificate must be available on the database server. For more information, see the Support for TLS v1.2 section in <a href="#">Oracle</a> . |
| Wallet Type                     | Select the wallet type from the drop-down list. The selected wallet type takes the precedence. Note that both SSO and PKCS12 are copied to the UIM Server (<uim>Nimsoft\security) irrespective of the wallet type you select.                                                                                |
| Wallet Password                 | Specify the password to access the wallet information.                                                                                                                                                                                                                                                       |
| Need Client Authentication      | Select the option to specify whether you want to enable client authentication.                                                                                                                                                                                                                               |

**Hub Parameters (GUI/Console)****WARNING**

Hub parameters (domain and hub name, specifically) modified after installation will severely impact your environment. Changing these fields without updating the rest of the hub and robot configuration files (hub.cfg and robot.cfg) in your environment will cause a disconnect from those components.

| Parameter                      | Value                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name                    | <ul style="list-style-type: none"> <li>Desired domain name (default is <i>hostname_domain</i>)</li> </ul>                                                                                                                                                                                                                                                                    |
| Primary Hub Name               | <ul style="list-style-type: none"> <li>Desired hub name (default is <i>hostname_hub</i>)</li> </ul>                                                                                                                                                                                                                                                                          |
| Primary Robot Name             | <ul style="list-style-type: none"> <li>Desired robot name (default is <i>hostname</i>)</li> </ul>                                                                                                                                                                                                                                                                            |
| Primary Robot First Probe Port | <ul style="list-style-type: none"> <li>No value or the default (48000)</li> <li>Port assignments start at 48000. Increase by one until a free port is found, then continue to increase for subsequent assignments</li> <li>Any available port if you want to specify an initial port for UIM probes. Subsequent port assignments increase from the specified port</li> </ul> |
| Primary Hub IP Address         | <ul style="list-style-type: none"> <li>IP address that you want to use for UIM traffic (the installer displays all network interfaces attached to the computer). If you have selected IPv6 installation environment then you can chose the interface to install.</li> </ul>                                                                                                  |
| UIM Administrator Username     | <ul style="list-style-type: none"> <li>Administrator by default</li> </ul>                                                                                                                                                                                                                                                                                                   |
| UIM Administrator Password     | <ul style="list-style-type: none"> <li>Desired UIM administrator password (at least six characters)</li> </ul>                                                                                                                                                                                                                                                               |

**telemetry Probe Parameters**

The telemetry probe is installed by the CA UIM installer, unless you choose to not accept the terms of the Telemetry Probe License Agreement and you cancel the installation of CA UIM. You must read and scroll completely to the bottom of the Telemetry Probe License Agreement before you can modify the probe parameters.

| Parameter                                                          | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I accept the terms of the Telemetry Probe License Agreement        | If you accept the terms, click the radio button. If you want the probe to upload data about your CA UIM environment to CA Technologies Support for further troubleshooting purposes, click the button to accept the terms <i>and</i> enter your Support credentials before you click Next. If you click the button to accept the terms and do <i>not</i> enter your Support credentials before you click Next, the probe is installed, is active, and collects data about your CA UIM environment. However, the probe saves this data only to your local system. <b>Note:</b> You cannot go back later to configure the probe to upload data to Support. |
| I do NOT accept the terms of the Telemetry Probe License Agreement | If you do NOT accept the terms, click the radio button. If you want to halt the entire CA UIM installation process, click the button to NOT accept the terms and then click Cancel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| CA Support Username                                                | If you accept the terms and want the probe to upload data about your CA UIM environment to Support, enter your valid CA UIM Support username.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| CA Support Password                                                | If you accept the terms and want the probe to upload data about your CA UIM environment to Support, enter your valid CA UIM Support password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Secure Mode Parameters

This section is applicable only when you are upgrading from CA UIM 9.0.2 to CA UIM 9.2.0.

| Parameter                                             | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Do you want to install secure bus binaries?<br>Enable | <p>The CA UIM 9.2.0 upgrade installer (UIM Server) performs the secure hub- and robot-related configurations in the existing CA UIM 9.0.2 environment when you enable this option. The secure mode option provides enhanced end-to-end security for hub-to-hub and robot-to-hub communication. For more information about the secure hub and robot, see <a href="#">Secure hub and robot</a>.</p> <p>Review the following points:</p> <ul style="list-style-type: none"> <li>You want to use the secure option.<br/>Your existing 9.0.2 setup is already configured with tunnels. In this case, the tunnel configuration options are not displayed in this screen. Because the secure option is enabled, the upgrade uses the secure hub and robot packages.</li> <li>You want to use the secure option.<br/>Your existing CA UIM 9.0.2 setup is not configured with tunnels. In this case, the tunnel configuration options are displayed in this screen. Because the secure option is enabled, the upgrade uses the secure hub and robot packages.</li> <li>You do not want to use the secure option.<br/>When you disable the secure option, no tunnel configuration parameters are displayed in this screen. Because the secure option is not enabled, the upgrade uses the non-secure (normal) hub and robot packages.</li> </ul> |
| Tunnel Server Port                                    | <p>Specifies the tunnel server port that you want to use for the primary hub. Click <b>Test</b> to verify the port availability.</p> <p><b>Default:</b> 48003</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| CA/Tunnel Server Password                             | <p>Specifies the password that you want to use while creating the certificate authority (CA) and * (wildcard) tunnel server certificates.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Confirm CA/Tunnel Server Password                     | <p>Lets you confirm the password entered for the CA and * tunnel server certificates.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Client Certificate Password                           | <p>Specifies the password that you want to use while creating the * tunnel client certificates.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Confirm Client Certificate Password                   | <p>Lets you confirm the password entered for the * tunnel client certificates.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Silent Install Parameters

Silent install parameters are defined in the installer.properties file. You can [download](#) the template file.

## Installing in an Active/Passive Microsoft Cluster

A cluster configuration minimizes the risk of having a single point of failure due to hardware problems or maintenance. Monitoring continues to operate even if the cluster nodes change state. The UIM Server supports failover with the following Microsoft versions:

- Windows Cluster 2012
- SQL Server Cluster 2008, 2012, 2014, and 2019

**NOTE**

**Optional:** You can set up failover using a primary hub and a secondary hub with the HA probe.

- Failover is handled by the cluster when CA UIM is installed on a Microsoft Cluster.
- Failover is handled by the HA probe when CA UIM is installed on the primary and secondary hubs with the HA probe.

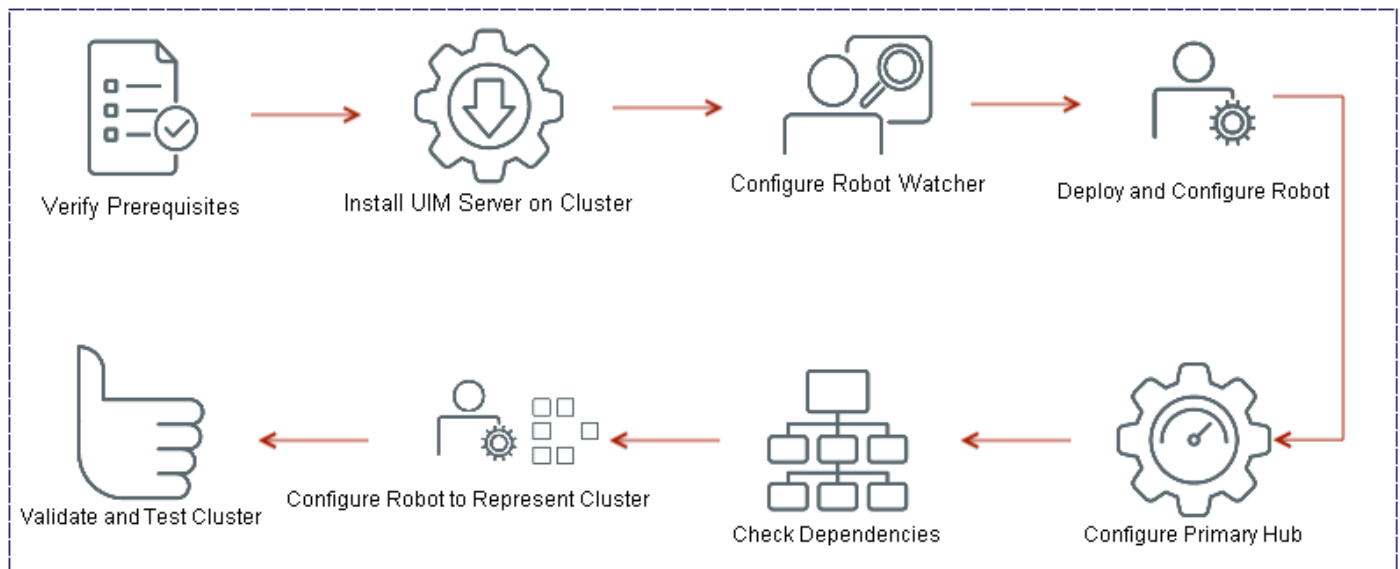
The Windows Cluster method creates a virtual IP address for the cluster nodes running the CA UIM components. Using a virtual IP address means that none of the CA UIM components need to be reconfigured to point to the failover node.

With the HA probe, failover is automated, but the OC components require configuration so that they point to the failover server. Use a LUA script or a probe available from CA UIM Services to configure OC failover.

**Installation Overview**

The following diagram shows the high-level steps:

**Figure 7: Install UIM in Microsoft Cluster**



Follow the steps in each section to install CA UIM in an active/passive Microsoft cluster:

**NOTE**

For database high availability, Microsoft SQL Server is supported. No special database connection or configuration is required.

Cluster configuration is covered in Microsoft documentation, and in the Microsoft Developer Network. Some resources include:

- <http://technet.microsoft.com>
- <http://blogs.msdn.com>

**Verify Prerequisites**

Before you begin, verify the following prerequisites:



- You have administrative access to an active/passive two-node failover cluster.
- A shared disk target, typically a SAN, NAS, or RAID array, for example, drive **S:\**
- All resources are available to both cluster nodes
- An IP address for assignment to the virtual service

### **Install UIM Server on the Cluster**

#### **NOTE**

We recommend that you do *not* install Infrastructure Manager or OC on the cluster nodes. Install them on a separate server.

#### **Follow these steps:**

1. Download the UIM Server installer to the shared disk target drive, for example, **S:\**.
  2. Run the [UIM Server installer](#) on the active node, which has current control of the **S:\** drive.
    - Install to a location on the shared drive, such as **S:\Nimsoft**. Do *not* install to the **C:\Program Files** directory.
    - Specify the network interface as the physical IP address of the system.
    - Make note of the domain name and hub name. You will need this information when you install UIM Server on the second node.
    - Both cluster nodes will share the hub name. To avoid confusion, use a hub name that is different from the default, *hostname*.
    - If the installer warns you that one or more probes did not start, ignore the message.
  3. Reboot the active node. The second node takes over and becomes active.
  4. Log in to the second node and verify that you can access the shared drive, **S:\**.
  5. Install UIM Server on the second node. Take the following steps to ensure that the IP bindings are correctly initialized, and that all required registry entries and DLLs are installed on both nodes of the cluster:
    - Use the *same domain name and hub name* for both nodes.
    - When you are prompted for an IP address, enter the **physical IP address** of the second node.
  6. When installation is complete, reboot the second node and log in to the first node. The first node becomes the active node, and gains control of the shared drive.
- In a non-clustered environment, if the UIM Server stops for any reason, The *Robot Watcher Service* restarts the robot.
  - In a clustered environment, if the robot stops because the primary node goes down, the *Robot Watcher Service* starts the robot on the failover node.

#### **NOTE**

Installing the UIM Server on the two cluster nodes can result in the loss of data in the `security.cfg` file. Take the following steps to avoid losing content.

1. After installing the UIM server on the first node, stop the *Robot Watcher Service* and make a backup copy of the **S:\Nimsoft\hub** directory on the shared drive.
2. After installing the UIM server on the second node, compare the size of the `security.cfg` file in the **S:\Nimsoft\hub** directory with the size of the `security.cfg` file in your backup directory. If the filesize differs, continue with Step 3.
3. Follow the steps in the [document](#). Use the contents of your backup `security.cfg` file to restore any missing content.

### **Configure the Robot Watcher Service**

1. On the active node, launch **Failover Cluster Manager**.
2. Expand the tree in the left frame and select **Services and Applications**.
3. Under **Actions** in the right frame, click **Configure a Service or Application** and select **Generic Service**.

4. In the **Client Access Point** dialog, specify the name that clients use to access the service. If you are asked to provide an IP address, use the available virtual IP address provided by your Network Administrator. In DHCP environments, networking is configured automatically, and you do not need to supply an IP address.
5. In the **Select Storage** dialog, enter the shared drive where the UIM Server is installed, for example, **S:\**. The service is created and brought online with the virtual IP address. You will need this address when you configure the robot.

#### NOTE

If you receive an **Operation Has Failed** error message, take each of the following steps, in order, to resolve the problem.

1. Reboot both cluster nodes.
2. Verify that the latest Windows updates are applied to both nodes.
3. Disable antivirus scanning.
4. Configure the *Robot Watcher Service* with **Windows PowerShell** as follows:
  - a. Go to **Start, Administrative Tools**, and right-click **Windows PowerShell Modules**.
  - b. Select **Run as Administrator** to open the Windows PowerShell command prompt.
  - c. At the **PS>** command prompt, execute the following command:
 

```
Add-ClusterGenericServiceRole -ServiceName NimbusWatcherService -
Name <a unique service name you provide> -
Storage "<name of cluster disk with the shared Nimsoft directory>"
For example: PS> Add-ClusterGenericServiceRole -
ServiceName NimbusWatcherService -Name NimbusService -
Storage "Cluster Disk 2"
```

### Deploy and Configure the Robot

1. Deploy the robot:
  - a. Log in to the active node of the cluster and launch Admin Console or Infrastructure Manager.
  - b. Deploy the new robot package to the existing primary hub robot.

#### NOTE

- Two robots are available, one for each node of the cluster. Ensure that you deploy the robot to the active node.
  - The distribution process can report that the deployment finished with unknown status. The message can be ignored.
2. Edit the robot configuration:
    - a. Navigate to the UIM Server installation folder, **S:\Nimsoft**, and open the **robot** folder.
    - b. Open the robot configuration file, **robot.cfg**, in a text editor and make the following changes. If one or more key-value pairs do not exist, add them.
      - **hubip** = <Nimsoft\_Service\_virtual\_IP> (from Step 5 of *Configuring the Robot Watcher Service*)
      - **robotip**=<Nimsoft\_Service\_virtual\_IP> (from Step 5 of *Configuring the Robot Watcher Service*)
      - **strict\_ip\_binding=no** (default)
      - **local\_ip\_validation=no** (default)
  3. Create the **NIMBUS\_LOCAL\_IP** environment variable on both cluster nodes. Set the variable value to the virtual IP address of the service, from Step 5 of *Configuring the Robot Watcher Service*.

### Configure the Primary Hub

1. Navigate to the UIM Server installation folder, **S:\Nimsoft**, and open the **hub** folder.
2. Open the hub configuration file, **hub.cfg**, in a text editor.
3. Add or modify the following key-value pair in the **<hub>** section of the file:

- `bulk_size_floor=1`

### **Check the Dependencies**

1. Restart the *Robot Watcher Service*:
  - a. Open the **Failover Cluster Manager** on the active node.
  - b. Right-click **NMS Robot Watcher** and select **Take this resource offline**. Right-click the service, and select **Bring this resource online**.
2. Check the dependencies:
  - a. Right-click the *Robot Watcher Service* and click **Properties**.
  - b. On the **Dependencies** tab, set the dependencies for the *Robot Watcher Service*. Before the service starts, ensure that the following cluster resources are online and available:
    - Cluster shared disk
    - Virtual NMS resource
    - Virtual IP address that is assigned to the virtual NMS service

### **Configure One Robot to Represent the Cluster**

1. Log in to Infrastructure Manager. You see two robots, one for each node of the cluster. The robot on the active node is green, the robot on the passive node can be red.
2. Double-click the controller probe on the active node.
3. Under **Setup Options**, click **Set Specific Name**. Specify a unique name for the robot. Use the name of the *Robot Watcher Service*, and not the physical *hostname*.
4. Right-click the robot that is on the second node and select **Remove**. This action:
  - Removes the robot from the list of registered robots for the hub
  - Prevents the generation of alarms from the robot

One robot now represents the cluster.

#### **NOTE**

- If any probe managed by the robot is red, or shows invalid security, right-click the probe and select **Security > Validate**.
- If any components are using an auto-generated license, install a standard license.
- From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).

### **Validate and Test the Cluster**

1. Validate the probe IP address binding:
  - a. In Admin Console or Infrastructure Manager, display the probes on the cluster robot.
  - b. View the **IP Address** column to verify that the controller probe, and any Java probes, report their IP address as the virtual IP address of the UIM service.
  - c. Verify that other probes are using the localIP address of the active node.
2. Test the failover and failback operation of CA UIM within the cluster.
  - a. Launch **Failover Cluster Manager** and expand the tree in the left frame.
  - b. Right-click the virtual hub and select **Move the service or application to another node**.
  - c. Select the other node in the cluster and confirm the operation. As the service moves to the passive node, Infrastructure Manager shows that the hub becomes unavailable by displaying it in red. Failover Cluster Manager shows the status of the cluster as the CA UIM service moves to the failover node.

- d. After a short time, verify the hub status in Admin Console or Infrastructure Manager. A green status indicates that the UIM Server is running successfully on the failover node.
3. Repeat Step 2 to fail the service back to the original node.

## Uninstalling UIM Server

This article describes the procedure for uninstalling UIM Server.

### Windows

To uninstall UIM Server in a Windows environment, follow the instructions in this procedure.

#### Follow these steps:

1. Go to the Control Panel.
2. Choose **Programs and Features (Add/Remove Programs)** on older versions of Windows).
3. Select each UIM component. Some components might be shown as "CA Unified Infrastructure Management Server".
4. Click **Uninstall/Change**, then follow the system prompts.

### Linux

To uninstall UIM Server in a Linux environment, follow the instructions in this procedure.

#### Follow these steps:

1. Go to `<UIM_Server_home> /_ca_uimserver_installation` (the default installation directory is `/opt/nimsoft`).
2. Run the uninstaller. Execute:
3. – **uninstall** to run in GUI mode  
– **uninstall -i console** to run in console mode

#### NOTE

In console mode, you might see a message that says `Some items could not be removed`. This message can be safely ignored.

## Install Infrastructure Manager

Infrastructure Manager is a management console that is required for some UIM tasks. If your primary hub server is a Windows system, CA recommends you install it there. It also can be installed on another Windows system in your environment, and from there you can use it to manage your domain.

#### WARNING

Infrastructure Manager requires the Microsoft Visual C++ 2008 Redistributable Package. Download the package from [support.nimsoft.com](http://support.nimsoft.com).

#### Follow these steps.

1. From the system where you want to install Infrastructure Manager, browse to your UIM Server web page (`http://<servername_or_IP_address>:80`).
2. Click the **Installers** tab. Under **UIM Server Administration**, click **Infrastructure Manager** to download the installer file.
3. Run the installer, following the prompts to complete the installation.

**NOTE**

If you have installed OC, port 80 has been assigned to wasp by default. To access the UIM Server page, browse to `http://<servername_or_IP_address>/uimhome/` to begin the installation.

## Install Secondary Hubs

Most deployments have at least one extra hub. For load balancing, enterprise deployments can have several to hundreds. Secondary hubs are typically dedicated servers. They are used:

- To provide failover capability if the primary hub is unavailable.
- In enterprise deployments, they host services and management consoles, such as Operator Console (OC) and the Alarm Server (nas).
- For data collection in an enterprise deployment. Use tunnels and queues to connect secondary hubs in a hierarchy for securely transporting data to the primary hub.

The topics in this section describe the process for deploying hubs on each supported operating system. For more information about configuring hubs, tunnels and queues, see the [hub](#) probe documentation in Probes Documentation Space.

For more information about how to upgrade existing hubs to a secure state, see [Secure Hub and Robot](#).

## Deploy Secondary Hubs on Windows

To configure a secondary hub as a tunnel client, you need a certificate that is generated by the tunnel server hub. If the tunnel server is not set up, you can install a hub with no tunnel. Later, you can configure the tunnel between the hubs with Admin Console or Infrastructure Manager.

### Follow these steps:

1. On the secondary hub server, browse to your UIM Server home page:  
`http://server_name_or_IP:<wasp_port>/uimhome`
2. Click the **Installers** tab. Under **Infrastructure Installers**, download the **Windows Robot, Hub, Distribution Server** package.
3. Launch the **NimBUS Infrastructure** installer.
4. Select one of the following modes:
  - **Automatic** search for a hub. If a hub is found, only a robot is installed. If a hub is not found, then a hub with no tunnel is installed.
  - **Custom** install the hub in the same network as the primary hub.
  - **DMZ** install a tunnel hub that is separated from the primary hub by a firewall.
5. Follow the prompts to complete the installation. Note the following points:
  - If no other hub is available, select an existing domain. All available domains are shown.
  - Specify the desired hub name.
  - Create a hub user account (the **Initial User**) for the hub. Specify a user name, or use the default, administrator. Supply a password for the account. When prompted to log in, enter the new user name and password.
  - (Recommended) Leave the First probe port field blank, unless you have a reason to specify it. The system assigns the first probe to port **48000** (or the first available subsequent port). The port number increments by 1 for each additional assignment.
6. If you are installing a tunnel server hub, the **Setting up Tunnel Server** dialog prompts you to create an authentication password. This password is required when you set up the tunnel client.

- In the **Generating Client Certificate** dialog, enter the IP address of the primary hub, or the secondary hub tunnel client.
  - Save the generated certificate, and copy the file to the tunnel client server. You need this certificate when you set up the tunnel client.
7. If you are installing a tunnel client hub:
- Enter the IP of the tunnel server, the server port, and the password you created during tunnel server setup.
  - Browse for the certificate file. When the file is found, the certificate text displays.

Hub installation is complete. The hub is in an enabled, or started, status.

### **Next Steps**

- Set up queues and tunnels between hubs. See the [Hub](#) probe documentation on the Probes Documentation Space for more information.
- If you want to use Admin Console to manage this hub, its child robots, or probes, deploy the Probe Provisioning Manager (ppm) probe to the hub. Use either Admin Console or Infrastructure Manager to deploy the probe from your local archive.

## **Deploy Secondary Hubs and Robots on Linux**

This article describes the process for deploying hubs and robots using the nimldr utility.

### **Understand The nimldr Utility**

The **nimldr** utility installs secondary hubs and robots on Linux . You can run nimldr in express mode to perform a silent installation.

#### **WARNING**

Cloud deployment is not supported on AIX.

### **Flags for nimldr**

You can execute nimldr with flags to modify how the installer runs, or to specify information.

| <b>Usage</b>      | <b>Flag</b> | <b>Description</b>                                                                            |
|-------------------|-------------|-----------------------------------------------------------------------------------------------|
| All installations | -?          | Help                                                                                          |
|                   | -d          | Debug level, 0 - 5 (default, 0)                                                               |
|                   | -l          | Installation logfile                                                                          |
|                   | -t          | Location for temporary files during installation; default is<br><code>/opt/nimsoft/tmp</code> |
|                   | -D          | NimBUS domain name                                                                            |
|                   | -H          | NimBUS hub name                                                                               |
|                   | -N          | Override robot name Default,<br><code>robot_hostname</code>                                   |
|                   | -p          | NimBUS installation path; Default,<br><code>/opt/nimsoft</code>                               |

|                                                      |    |                                                                                                                                                                                                                                                        |
|------------------------------------------------------|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                      | -f | Override package file name. The default installation file is detected by the program.<br><b>Note:</b> The file name is case-sensitive. Omit the .zip extension.                                                                                        |
|                                                      | -u | Install as the current user, and not as root ( <i>not</i> recommended).                                                                                                                                                                                |
|                                                      | -o | First probe port<br>If you omit this flag (recommended), the system assigns the first probe to port <b>48000</b> , or the first available subsequent port. Specify any available port. The port number increments by 1 for each subsequent assignment. |
|                                                      | -R | The IP address for the robot. Use this parameter on systems with multiple network cards.                                                                                                                                                               |
|                                                      | -a | Set the automatic unregister flag. Default, <b>no</b>                                                                                                                                                                                                  |
|                                                      | -s | Set the robot to passive mode                                                                                                                                                                                                                          |
|                                                      | -A | set<br>robotip_alias<br>for NAT. This is a special case, use caution.                                                                                                                                                                                  |
|                                                      | -v | Print the version of<br>nimldr.                                                                                                                                                                                                                        |
|                                                      | -h | Print this help text.                                                                                                                                                                                                                                  |
| Installation file is on local system                 | -F | If the installation file is on the local system, specify the directory containing the installation file.                                                                                                                                               |
| Installation file is on a NimBUS Distribution Server | -I | The IP address of the NimBUS hub running a Distribution Server. This parameter overrides the<br>-H<br>flag.                                                                                                                                            |
|                                                      | -U | The username for logging in to the hub.                                                                                                                                                                                                                |
|                                                      | -S | The password for logging in to the hub.                                                                                                                                                                                                                |
|                                                      | -V | Package version Use the specified version of the package, and not the latest one.                                                                                                                                                                      |
| Installation modes                                   | -r | Install only the robot (default)                                                                                                                                                                                                                       |
|                                                      | -i | Install an Infrastructure (robot, hub, nas, and distsrv)                                                                                                                                                                                               |
|                                                      | -E | Express installation This method uses the defaults, or supplied flags. The installation file must be on the local system.                                                                                                                              |
|                                                      | -X | Silent express installation If there is an error, this method fails instead of going to interactive mode. The installation file must be on the local system.                                                                                           |

|                                                                       |    |                                                                 |
|-----------------------------------------------------------------------|----|-----------------------------------------------------------------|
| Cloud installation<br>( <i>option not available for AIX systems</i> ) | -C | The number of restarts until robot is expected to become active |
|                                                                       | -M | DNS name of the system running the hub                          |

### **nimldr Robot and Hub Questions**

During the install process, the nimldr utility prompts you to answer questions. The following table lists all the potential questions. Not all questions are asked. Some questions depend on your answers to previous questions, and some depend on the type of installation you are performing.

In the installer, the default answers are in brackets. Press **Enter** to accept the default.

| <b>Question</b>                                                                                         | <b>Answer</b>                                                                                                     |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Where should nimldr store temporary files?                                                              | <code>opt/nimsoft/tmp</code><br>(default)<br>Directory of your choice                                             |
| Do we have the installation file locally?                                                               | <b>Yes</b><br><b>No</b>                                                                                           |
| Where do we have the installation file(s)?                                                              | <b>Path</b> to installation files                                                                                 |
| Is there a host running a hub we can query for the installation file?                                   | <b>Yes</b><br><b>No</b>                                                                                           |
| What is the IP address of the host running a hub?                                                       | <b>IP address</b>                                                                                                 |
| What is the Domain called?                                                                              | <b>Domain name</b> (if it exists)<br><b>Desired name</b> (if it is created)<br>* (asterisk) to search for domains |
| What is the hub called?                                                                                 | <b>Hub name</b> (if it exists)<br><b>Desired name</b> (if it is created)<br>* to search for hubs                  |
| What is the installation file called?                                                                   | <b>install_ platform</b>                                                                                          |
| Which of these archives would you like to connect to?                                                   | <b>Archive name</b>                                                                                               |
| Enter username and password.                                                                            | <b>Username</b> and <b>password</b> for the administrator account set up during UIM installation                  |
| Where do we have the installation files?                                                                | <b>Install file directory</b> (if local)                                                                          |
| What are we installing?                                                                                 | <b>1</b> (robot only)<br><b>2</b> (robot and hub, tunnel server, or tunnel client)                                |
| Would you like to install the Distribution Server (distsrv)?<br><i>distsrv is the UIM probe archive</i> | <b>Yes</b><br><b>No</b>                                                                                           |
| Where should the software be installed?                                                                 | <code>/opt/nimsoft</code> (default)                                                                               |
| Automatically unregister robot from hub on termination?                                                 | <b>No</b> (default)<br><b>Yes</b>                                                                                 |
| Should this robot run in passive mode?                                                                  | <b>No</b> (default; robot sends data to hub)<br><b>Yes</b> (hub must request data from robot)                     |
| What is this Domain called?                                                                             | <b>Domain</b> set up during UIM installation                                                                      |
| Which hub should this robot connect to?                                                                 | <b>Hub name</b>                                                                                                   |
| What is this hub called?                                                                                | <b>Hub name</b>                                                                                                   |
| What is that hub's IP address?                                                                          | <b>IP address</b>                                                                                                 |



|                                                                 |                                                                                                            |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Are you setting up a tunnel between this hub and another hub?   | <b>Yes</b><br><b>No</b>                                                                                    |
| Would you like to initialize the security settings on this hub? | <b>Yes</b> (default)<br><b>No</b>                                                                          |
| Please specify the administrator user password.                 | <b>Password</b> for the account created during UIM installation                                            |
| Are you setting up a tunnel between this hub and another hub?   | <b>No</b> (default, installation completes and the installer exits)<br><b>Yes</b> (installation continues) |

### **Nimldr Tunnel Client Questions**

Answer the following questions to set up a tunnel client hub.

| Question                                             | Answer                                                                                                    |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| What is the IP address of the tunnel server hub?     | Tunnel server hub IP address                                                                              |
| What port is the server listening on?                | Port number assigned during UIM installation; typically 48000 (default)                                   |
| What password was used to generate this certificate? | Password that is defined when the tunnel client certificate was created during tunnel server setup        |
| What file is the client certificate in?              | Path and file name for the client certificate that was copied from the tunnel server to the tunnel client |

### **Run the nimldr Utility**

Run the nimldr utility to install secondary hubs and robots.

#### **Follow these steps:**

1. If UIM software is installed and running on the system, turn off all UIM processes and remove the software. Execute:

```
/opt/Nimsoft/bin/niminit stop
/opt/Nimsoft/bin/inst_init.sh remove
```

2. Verify that the system `/etc/hosts` file maps 127.0.0.1 to localhost, and its own IP address to its hostname.
3. Download and unpack the installers:

- a. On the client computer, browse to your UIM Server home page:  
`http://server_name_or_IP:<wasp_port>/uimhome`

#### **NOTE**

The default wasp port number is 80.

Click the **Installers** tab. Under **Infrastructure Installers**, select **UNIX installation utility (nimldr) for all platforms**, and save the archive on the client. If the client system does not have a browser, download the installer to another computer and copy it to the client. Ensure the file is named **nimldr.tar.Z**.

- b. Uncompress and extract the file, **nimldr.tar.Z**, using the tar command:

```
tar -xzf nimldr.tar.Z
```

This command creates the subdirectories that contain nimldr installers for various Linux platforms.

#### **NOTE**

On certain non-Linux UNIX platforms, the tar command does not contain the `-z` option. In such cases, follow these steps:

1. Use `uncompress nimldr.tar.Z` or `gunzip nimldr.tar.Z` to uncompress nimldr.tar.Z file.
2. Use `tar -xf nimldr.tar` or `tar -xvf nimldr.tar` to extract the contents of the nimldr.tar file.

4. Enter the appropriate subdirectory for your platform. For example, **LINUX\_23\_64**.

5. Change the file permissions to add executable permissions for the file owner:

```
chmod 755 nimldr
```

6. Launch the installer. If the client is on the:

- Same network segment as the primary hub, execute:

```
./nimldr
```

- Different network segment, execute:

```
./nimldr -I NMS_server_name_or_IP_address
```

7. Answer the nimldr questions to install the hub.

8. If you are installing a tunnel server hub:

- a. Answer the nimldr tunnel server questions. The values are used to generate the tunnel client certificate, and save it to a file.
- b. Copy the certificate file to the tunnel client hub. After installation, install the certificate on the tunnel client hub.

9. If you are installing a tunnel client hub:

- a. Ensure that the certificate file resides on the hub.
- b. Answer the nimldr tunnel client questions.

### TIP

Installation progress is logged in the **nimldr.log** file, typically located in **opt/nimsoft/tmp**. To view it, execute:

```
tail -f /opt/nimsoft/tmp/nimldr.log
```

### Example: Perform an Installation with a Local File

This example provides high-level steps to perform an installation with a local file.

#### Follow these steps:

1. Copy **install\_LINUX\_23\_64-7\_93.zip** to a directory on the computer, such as `/opt`.
2. Rename the version information from the install file **install\_LINUX\_23\_64-7\_93.zip** to **install\_LINUX\_23\_64.zip**.
3. Run `./nimldr` from the **LINUX\_23\_64** directory.
4. Specify `y` when the installer prompts you to specify whether the installation file is available locally (*Do we have the installation file locally?*).
5. Specify `/opt` when the installer prompts you to specify the installation file location (*Where do we have the installation file(s)?*).
6. Continue with the remaining installation steps.

#### Next Steps

- Set up queues and tunnels between hubs. See the [Hub](#) probe documentation on the Probes Documentation Space for more information.
- If you want to use Admin Console to manage this hub or its child robots or probes, deploy the Probe Provisioning Manager (ppm) probe to the hub. Use either Admin Console or Infrastructure Manager to deploy the probe from your local archive.

## Configure the robot.cfg File

The UIM Server installer creates a `.pem` file (certificate.pem) in the `<Nimsoft>\security` folder. The `.pem` file is a symmetric key that is shared with the required robots, which is then used for communication with the `data_engine` probe. You copy this `.pem` file to the remote OC, and CABL robots and provide the location of the file in the `robot.cfg` file (`cryptkey = <.pem file location>`). Furthermore, if any **impacted probe** is not on the same computer where `data_engine` is present, copy the generated `.pem` file to the robot computer (where `data_engine` is not available) and update the `robot.cfg` file with the `.pem` file location on that computer.

To configure the robot.cfg file, follow these steps:

1. Navigate to the <nimsoft>\robot folder.
2. Open the robot.cfg file in a text editor.
3. Add the following parameter to the file:  

```
cryptkey = <location of the .pem file>
```

 For example, cryptkey = c:\Certificate\certificate.pem
4. Save your changes.  
**Note:** You do not need to restart the robot.

You have successfully configured the robot.cfg file.

### **Create a .pem File**

Though the UIM Server installer automatically generates a .pem file (certificate.pem) in the <Nimsoft>\security folder, you can generate your own .pem file, if you want. You then need to copy the same .pem file to all the required places (OC robot, CABI robot) and configure the robot.cfg file as explained. You can use [OpenSSL](#) to create a .pem file.

**Note:** data\_engine does not consider the .pem file expiry though the automatically generated .pem file has a validity of 365 days. However, as a best practice, we recommend that you keep regenerating your .pem file based on your security requirements.

### **Follow these steps:**

1. For Windows, you can download OpenSSL from <http://gnuwin32.sourceforge.net/packages/openssl.htm>. Then, create a new system environment variable OPENSSL\_CONF with the value C:\Program Files (x86)\GnuWin32\share\openssl.cnf. For Linux, use appropriate package manager to install OpenSSL.
2. Open the command prompt and navigate to the location where the OpenSSL executable file is available.
3. Run the following command:  

```
openssl req -nodes -new -x509 -days <number of days the certificate is valid for> -out <certificate_filename>.pem
```

**Note:** Ensure that your certificate filename does not include spaces.
4. Enter the following information when prompted:
  - Country Name (2 letter code) [AU]:
  - State or Province Name (full name) [Some-State]:
  - Locality Name (eg, city) []:
  - Organization Name (eg, company) [Internet Widgits Pty Ltd]:
  - Organizational Unit Name (eg, section) []:
  - Common Name (e.g. server FQDN or YOUR name) []:
  - Email Address []:
 The .pem file is generated in the same location where the OpenSSL executable is available.
5. Copy the .pem file to the location that is accessible only to the appropriate users in your CA UIM environment. You provide this location while configuring the robot.cfg file.

## **Install Operator Console (OC)**

CA UIM features an Operator Console (OC) that presents the performance and availability data CA UIM collects. OC contains several modules, which are webapps. Operator Console Installer installs Operator Console and supporting Webapps that presents:

- **Account Admin** - for managing accounts and users
- **Dashboard Designer** - for creating and editing custom dashboards
- **SLM** - for creating, monitoring, and validating SLAs for internal or external customers
- **Alarm Viewer** - for monitoring, and managing alarms
- **CABI**- for custom/out-of-box dashboards

**NOTE**

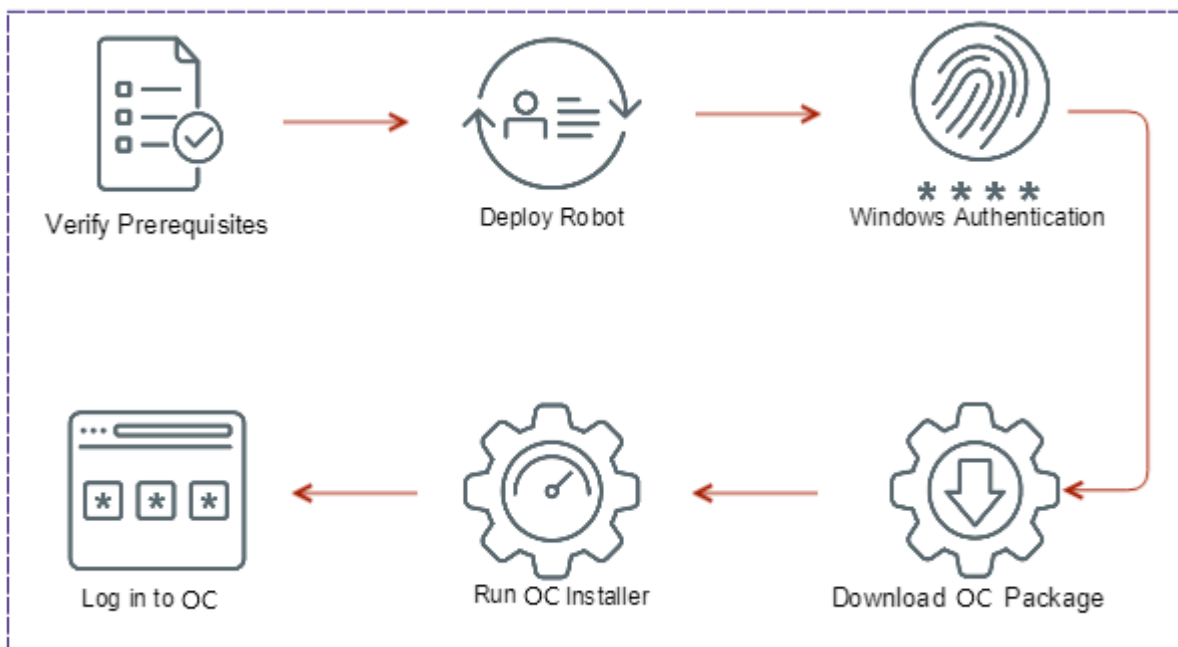
UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

**NOTE**

For a full list of the webapps available for Operator Console, see [Operator Console](#) in the Configuring and Viewing Monitoring Data page.

**Installation Overview**

The following diagram shows the high-level steps for Operator Console Installation:

**Figure 8: Install Operator Console****NOTE**

(For UMP) The OC installer must be used to upgrade UMP, as UMP is no longer available in UIM 20.3.0 (and later). The OC installer will uninstall deprecated components and upgrade valid components.

**NOTE**

- In an upgrade scenario, if you are upgrading UMP/OC to Operator Console in a secure setup, ensure that you bring your UMP/OC robot to the secure state by deploying the appropriate certificates and then updating

the robot version to the secure state (9.20S or later). After that, you upgrade UMP/OC to OC. For more information about the secure setup and how to deploy certificates, see [Secure Hub and Robot](#).

- To upgrade from a previous version of OC to OC 20.3.3, use the OC 20.3.3 upgrade installer that is released as part of the UIM 20.3.3 release. For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.
- To upgrade from a previous version of OC to OC 20.3.2, use the OC 20.3.2 upgrade installer. OC 20.3.2 is a patch release. For more information about the OC 20.3.2 patch, see the [OC 20.3.2 Patch](#) article.
- To upgrade from a previous version of OC to OC 20.3.1, use the upgrade installer for OC that the UIM 20.3.1 patch contains. Note that UIM 20.3.1 is a patch release over UIM 20.3.0. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes the OC upgrade installer along with the separate standalone artifacts that you can use to upgrade the respective components to 20.3.1. For more information about the artifacts that are available as part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.

### **Installation Steps**

The following steps help you install OC:

Your UIM environment contains the following components before you install OC:

- **Database Server:** The database server is the location of the UIM database. The QoS data and other required system information is written to the database server.
- **Primary Hub Server:** The primary hub server is the location of the robot that controls the UIM primary hub.
- **(Optional) Secondary Hub Servers:** Your UIM environment can also have extra servers for load-balancing and failover capability.

You have several options for the location of OC in your environment.

- A new server, which is known as the *OC server*. All of the probes that are required for basic OC functionality are installed on the OC server.
- An existing secondary hub server that has services such as `nas` or `discovery_server` located on a different secondary hub. In such a scenario, you can configure OC to connect to the service probes on a secondary hub.
- On the primary hub server. Only install OC on the primary hub server if you have a small environment to monitor. Generally, a small environment is classified as one that has 1 hub and fewer than 100 robots. See the article [Pre-Installation Planning](#) for more information about deployment size classifications.

### **Verify Prerequisites**

Complete the following tasks before running the OC installer.

#### **Verify Administrator Privileges for a User**

OC can be installed successfully only by a user with administrator privileges. This user setting can be changed in Windows with the following steps.

#### **Follow these steps:**

1. Open **Administrative Tools > Services**
2. Right click on the Nimsoft Robot Watcher and select **Properties**.
3. Select the **Log On** tab.
4. Select the **This account** radio button.
5. Enter the account and password for an administrator.

### **Verify the Requirements in the Pre-Installation Articles**

OC has specific requirements that will impact both the server hardware and database software that you are using in your CA UIM environment. Ensure that you have met all of the OC-specific requirements in [Pre-Installation Planning](#) before you continue with your OC installation.

### **Verify the Required Probes on the Primary Hub Server**

Verify that the following probes are installed, active, and responsive on your primary hub server when the OC installer runs:

- ace

#### **NOTE**

The ace probe has been deprecated in 20.3.3.

- automated\_deployment\_engine (ade)
- data\_engine
- discovery\_server
- ems
- maintenance\_mode
- mpse
- nas
- sla\_engine
- cdm

#### **NOTE**

The OC installer attempts to launch the cdm probe to gather system specifications for the robot you select. If the cdm probe is not installed or fails to start, a warning message displays. If this warning occurs, you can proceed with the OC installation. However, the installer cannot inform you that the robot does not meet the minimum recommended specifications for running OC. Therefore, before you install OC, it is recommended you verify that the cdm probe is installed, active, and responsive.

### **Download the UIM JRE Package**

Verify that the JRE package for your OS is present in the Archive folder in Admin Console or Infrastructure Manager. For Windows and Linux, the package is named **java\_jre package**. If necessary, right-click on the package for your OS, and download it before installing OC. If the JRE package for your OS is not present at installation, the OC installer prompts you to download it. If the installer cannot contact these probes, an error message appears. Use Infrastructure Manager or Admin Console to activate, restart, or download and deploy these probes as necessary.

### **Deactivate distsrv Forwarding**

If you have package forwarding set up for the distsrv probe, deactivate it before installing OC. The distsrv probe can be configured to forward packages to other hubs. By default, forwarding is activated but no hubs are specified, so packages are not forwarded.

#### **Follow these steps:**

1. In Admin Console, click the black arrow next to the distsrv probe, select **Configure**.
2. Click the **Forwarding** folder. If any Forwarding records have **All** in the **Type** column, deactivate forwarding. For other types of records (**Specific**, **Update**, or **Licenses**) you do not need to deactivate forwarding.
3. Deselect **Forwarding active**.

#### **NOTE**

From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 (or later) to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).

**Set the OC Server Locale**

The locale on the server that hosts OC must match the locale set on the UIM database server. For example, if the database server locale is set to Spanish, the OC server locale must also be set to Spanish.

**Turn off Anti-Virus Scanning on the Primary Hub Server**

Active anti-virus scanners slow down OC installation significantly. Before you begin installation, turn off any anti-virus scanning on the primary hub server.

**(Optional) Secure Hub and Robot**

The secure hub and robot provide robust hub-to-hub and robot-to-hub communication. To upgrade OC from UMP/OC in a secure setup, upgrade the UMP/OC robot to a secure state and then perform the OC upgrade. For more information about the secure setup and how to deploy certificates, see [Secure Hub and Robot](#).

**Deploy a Robot to the OC Server**

If you are installing OC on a new server, deploy a robot. For more information about robot deployment, see the article [Deploy Robots](#). Once the robot is deployed, you can continue with OC installation.

**NOTE**

The UIM Server installer creates a .pem file (certificate.pem) in the <Nimsoft>\security folder. The .pem file is a symmetric key that is shared with the required robots, which is then used for communication with the data\_engine probe. You copy this .pem file to the remote OC and CABI robots and provide the location of the file in the robot.cfg file (cryptkey = <.pem file location>). Furthermore, if any [impacted probe](#) is not on the same computer where data\_engine is present, copy the generated .pem file to the robot computer (where data\_engine is not available) and update the robot.cfg file with the .pem file location on that computer. For more information about the robot.cfg file configuration, see [Configure the robot.cfg File](#).

**(Microsoft SQL Server Windows Authentication Only) Set up Windows Authentication in OC****WARNING**

If you are using Microsoft SQL Server with Windows authentication, ensure that the UIM, OC, and CABI Servers are on Windows servers.

Windows authentication must be set up both in UIM and OC.

**Follow these steps:**

1. After the OC robot is installed, go to **Administrative Tools > Services** and double-click on **Nimsoft Robot Watcher**.
2. Select the **Log On** tab.
3. Use Windows "SYSTEM" user to login to your DB from the data\_engine.

**NOTE**

For MS SQL with AD Authentication, Change the logon account to the same account and password used in the data\_engine and the primary UIM server.

4. Click **OK**.
5. Right-click on **Nimbus Robot Watcher** and select the **Restart** option.
6. Close the windows.
7. Restart the wasp.

**Download the OC Install Package to the Primary Hub Server**

Log in to [support.broadcom.com](http://support.broadcom.com) and locate the OC installation package in [Download Management](#).

**Run the OC Installer from the Primary Hub Server**

The following description is for a first-time installation of OC. By default, the OC installer runs as a wizard with a GUI. You can also run the installer in console mode.

**NOTE**

Once OC has been installed, the system IP address cannot be changed.

**GUI Mode**

Graphical user interface (GUI) mode walks you through the installation process.

**Follow these steps:**

1. Run the installer from the primary hub server.
2. Select the language to use.
3. Select the installation folder location.
4. Enter the user name and password to log in to the primary hub. The user name can be any user with administrative rights.
5. Follow the required steps based on your requirements:
  - a. (For 20.3.3) Specify the IP address of the required robot, where you want to install OC, in the **Specify IP** field. This robot must be reporting to the primary hub. Alternatively, you can also use the **Choose** option to select the robot that you deployed for your OC installation

**NOTE**

- It is recommended to use the **Specify IP** field if you have a large number of robots connected to the primary hub.
  - If you try to perform the installation on the primary hub, you receive a message prompting you to confirm whether you want to proceed with the installation on the primary hub. It is not recommended to install OC on a primary hub.
  - The OC installer displays an error message if you do not provide the valid IP address or the robot is not connected to the primary hub.
  - If wasp is down or cryptkey is not configured, the OC installer displays the appropriate error.
  - If the same OC version is already installed, the OC installer prompts you to reinstall or uninstall the instance.
  - If a previous version of OC is detected, the OC installer prompts you to upgrade to the latest OC version.
  - If the cdm probe fails to gather system specifications, or if the specifications do not meet requirements, a warning message is displayed. In either case, you can proceed with the installation.
- b. (Prior to 20.3.3) Choose the robot that you deployed for your OC installation. Systems in the list appear by host name.

**NOTE**

If the cdm probe fails to gather system specifications, or if the specifications do not meet requirements, a warning message is displayed. In either case, you can proceed with the installation.

6. Confirm or update the locations of the probes that are listed on the screen.
7. Specify the ports for OC to use.
  - **HTTP/Web port** - The port that is used by the browser when sending requests to OC. The default is 80 for new installations.
  - **AJP DMZ port** - This port is used by the OC Server to receive requests from the Apache web server in a DMZ implementation. The default is 8009 for new installations. For more information about DMZ implementations with OC, see [Set up Access to OC through a DMZ](#).
8. (**Windows only**) Choose where you want shortcuts to be created.
9. Review the information on the screen and click **Install**. The installer updates the archive (copies the files to the system) and installs OC. While it installs OC, a status bar displays progress for each phase. Each phase is validated before the installer continues. If there are errors, you can try that phase again, ignore the errors and continue, or cancel the installation.
10. Click **Done** to exit the installer.



11. Turn any anti-virus scanners back on.
12. Reactivate distsrv forwarding if you disabled it prior to installation.

### **Console Mode**

Console mode provides an interactive command-line interface.

**Follow these steps:** From a command line or terminal, add the following parameter when running the installer:

```
-i console
```

For example, the Linux command is:

```
./oc-installer_linux.bin -i console
```

The installer asks for the same information in console mode as in GUI mode.

### **Log in to OC**

Before you log in to OC, ensure that:

- Cookies are enabled in your browser.

To access OC, open a supported web browser and enter the IP address or the host name of the OC Server. See the [Unified Infrastructure Management Compatibility Matrix](#) for the current list of supported browsers.

After a user is authenticated, OC opens the default home page.

## **Configure Multiple OC Servers**

This article describes how to set up an initial multiple-OC configuration. If you are upgrading a multiple-UIMP/OC to OC configuration, see [Upgrade a Multiple OC Configuration](#).

### **NOTE**

- To upgrade from a previous version of OC to OC 20.3.3, use the OC 20.3.3 upgrade installer that is released as part of the UIM 20.3.3 release. For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.
- To upgrade from a previous version of OC to OC 20.3.2, use the OC 20.3.2 upgrade installer. OC 20.3.2 is a patch release.. For more information about the OC 20.3.2 patch, see the [OC 20.3.2 Patch](#) article.
- To upgrade from OC 20.3.0 to OC 20.3.1, use the upgrade installer for Operator Console that the UIM 20.3.1 patch contains. Note that UIM 20.3.1 is a patch release over UIM 20.3.0. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes the OC upgrade installer along with the separate standalone artifacts that you can use to upgrade the respective components to 20.3.1. For more information about the artifacts that are available as part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.
- Ensure that you deploy the `wasp_alarmviewer_api` package to the secondary OC.

### **Configure a Secondary OC Server**

Use the steps in this section to configure a secondary OC server. Repeat these steps to configure additional OC servers.

### **NOTE**

No steps are required for configuring the primary OC server.

Review the following points:

- A secondary OC server can only be installed on a robot. Do not attempt to install a secondary OC server on a hub.
- All probe addresses, for example, `/domain/hub/robot/<probe_name>`, are case sensitive.
- Before wasp is started on the secondary OC server, import the `.pem` file to the secondary OC server and add the cryptkey path for that `.pem` file in the `robot.cfg` file. For more information, see [Configure the robot.cfg File](#).
- Verify that robot 9.31 (or later) is running on the secondary OC robot (without this the wasp will not start).

**Follow these steps:**

1. Deploy a robot to the host that you plan to use as the secondary OC server.
  - The robot you choose must report directly to the primary hub, and must be on the same network subnet.
  - Installing a secondary OC instance on a robot that reports to a secondary hub is not supported.
  - Do not run the OC installer on the secondary OC server.
2. For 20.3.3
  - a. Launch the OC installer on the primary hub and navigate to the **Select Robot** dialog.
  - b. Specify the IP address of the required robot, where you want to install the OC, in the **Specify IP** field. This robot must be reporting to the primary hub. Alternatively, you can also use the **Choose** option to select the robot that you deployed for your OC installation

**NOTE**

- It is recommended to use the **Specify IP** field if you have a large number of robots connected to the primary hub.
  - If you try to perform the installation on the primary hub, you receive a message prompting you to confirm whether you want to proceed with the installation on the primary hub. It is not recommended to install OC on a primary hub.
  - The OC installer displays an error message if you do not provide the valid IP address or the robot is not connected to the primary hub.
  - If wasp is down or cryptkey is not configured, the OC installer displays the appropriate error.
  - If the same OC version is already installed, the OC installer prompts you to reinstall or uninstall the instance.
  - If a previous version of OC is detected, the OC installer prompts you to upgrade to the latest OC version.
- c. Follow the remaining steps to complete the installation. For more information about the steps, see the [Install Operator Console \(OC\)](#) article.
3. Prior to 20.3.3
    - a. In Admin Console or Infrastructure Manager, distribute the following OC server packages from the Archive to the secondary OC server in the below order. Ensure that you drag each of the `ump_portlet_name` packages that are required for your environment from the archive.
      - `java_jre`
      - `wasp`
      - `wasp_service_wrapper`
      - `nisapi_wasp`
      - `ump`
      - `ump_operatorconsole`
      - `wasp_alarmviewer_api`
      - `policy_management_ws`
      - `mcsuiapp_portlet`
      - `ump_cabi`
      - `ump_accountadmin` (Optional)
      - `ump_dashboard` (Optional)

- b. Configure the wasp probe to use the correct data\_engine probe address. For example, */domain/hub/robot/data\_engine*
- c. Use Raw Configure to modify the `<ump_common>` section of the wasp configuration to specify the following probe addresses:

- `ace: /domain/hub/robot/ace`

**NOTE**

The ace probe has been deprecated in [UIM 20.3.3](#).

- `automated_deployment_engine: /domain/hub/robot/automated_deployment_engine`
  - `discovery_server: /domain/hub/robot/discovery_server`
  - `nas: /domain/hub/robot/nas`
  - `service_host: /service_host` Functionality for the service\_host probe has been moved to wasp, and the probe is no longer installed as part of CA UIM v8.47 or later. The address key for the probe still exists in wasp but is not functional.
  - `sla_engine: /domain/hub/robot/sla_engine`
- d. Add the following keys with addresses as follows:
    - `maintenance_mode = /domain/hub/robot/maintenance_mode`
    - `udm_manager = /domain/hub/robot/udm_manager`
    - `mpse = /domain/hub/robot/mpse`
  - e. Activate the wasp probe on the secondary OC server. When the wasp probe is activated, the probes create database tables.

**NOTE**

These manual steps will work for 20.3.3 also. However, it is recommended that you use the 20.3.3 OC installer as explained in the previous step (Step 2) while configuring multiple OC servers in 20.3.3.

4. Repeat the same steps on other robots to implement more OC servers.

### **Configure a Load Balancer**

This section provides the high-level steps for configuring a load balancer for a multiple OC server configuration. Use the steps in this section after you install and configure the primary and secondary OC server.

**NOTE**

Load balancers and the terms that vendors use to describe them vary. Refer to the documentation for your load balancer for specific configuration details. You may need to perform the high-level steps in this section in a different order than shown.

**Follow these steps:**

1. Deploy the load balancer:
  - a. Configure the load balancer with IP addresses for each OC server.
2. Create a node/device for each OC server.
  - a. Enter the name and IP address of each OC server in your configuration.
3. Create a pool/server farm:
  - a. Provide a unique name for the pool/server farm.
  - b. Add one or more health monitors, such as the gateway\_icmp and http\_head.
  - c. Select a load balancing algorithm. The most common load balancing algorithm is round robin, where one connection is sent to each server on the list in turn.
  - d. Add the nodes you created previously to the pool for port 80. Use port 443 for an HTTPS connection.
4. Create a virtual server/context:
  - a. Provide a unique name for the virtual server/context.
  - b. Provide an IP address for the virtual server/context.
  - c. Configure additional settings for the virtual server as follows:

- Protocol = tcp
- HTTP Profile = https or http
- Source Port = preserve strict
- Default Persistent Profile = cookie.

#### NOTE

Regardless of the load balancer, setting the Default Persistent Profile setting to *cookie* is required.

5. Verify the load balancer was successfully configured by entering the IP of the virtual server/context in a web browser.

The load balancer is now configured for a multiple OC server configuration.

## Uninstall OC

This article describes the procedure for uninstalling OC.

### Considerations

Review the following points before you start the uninstall process:

- You do not need to delete wasp to complete a OC uninstall. The uninstall routine will delete wasp if appropriate. Wasp is not deleted if the uninstall routine detects other web applications running in wasp. For example, both CABI and Admin Console have wasp dependencies, and deleting wasp from a hub where they have been deployed will disable them. If no web applications are detected in wasp, the uninstall routine will delete wasp.
- A user name and password for an administrative user is required to uninstall OC.
- Do not attempt to uninstall OC using oc-installer-20.3.0-linux-x64.bin. If you attempt to uninstall OC using this binary file, the uninstall fails and you will see the following error in the uninstall log:

```
Installer: No 'sea_loc' in working directory, could not define $EXTRACTOR_EXECUTABLE$
```

### Windows

To uninstall OC in a Windows environment, follow the steps in this procedure.

#### Follow these steps:

1. (For 20.3.3) Go to **<UIM\_Server\_home>\Operator Console<IP\_address>** (the default installation directory is **C:\Program Files (x86)\Nimsoft\Operator Console<IP\_address>**).
2. (Prior to 20.3.3) Go to **<UIM\_Server\_home>\Operator Console** (the default installation directory is **C:\Program Files (x86)\Nimsoft\Operator Console**).
3. Run the **Uninstall\_Operator Console** executable file.
4. Follow the prompts and confirm the uninstall.

#### NOTE

You can find the OC installation/uninstallation logs at **<UIM\_Server\_home>\Operator Console<IP\_address>** or **<UIM\_Server\_home>\Operator Console**, as appropriate.

You can also uninstall OC using the Windows Control Panel. However, it is recommended that you use the above method for uninstallation:

1. Go to the Control Panel.
2. Click **Uninstall or change a program**.
3. Select OC from the list of programs to uninstall

### Linux

To uninstall OC in a Linux environment, follow the steps in this procedure.

**Follow these steps:**

1. (For 20.3.3) Go to **<UIM\_Server\_home>/Operator Console<IP\_address>** (the default installation directory is **/opt/nimsoft/Operator Console<IP\_address>**).
2. (Prior to 20.3.3) Go to **<UIM\_Server\_home>/Operator Console** (the default installation directory is **/opt/nimsoft/Operator Console**).
3. Run the Uninstall\_Operator Console binary file. You can use the **-i console option** to run the installer in console mode.
4. Follow the prompts and confirm the uninstall.

**NOTE**

You can find the OC installation/uninstallation logs at **<UIM\_Server\_home>\Operator Console<IP\_address>** or **<UIM\_Server\_home>\Operator Console**, as appropriate.

## Discover Systems to Monitor

Before you can deploy probes to your devices, you must run CA UIM Discovery. Discovery is performed by either:

- Running the Discover Devices Wizard in OC.
- Importing an XML file that contains your device and profile data.

This article contains the following topics:

### Introduction

#### Discovery Architecture

A critical part of IT monitoring is creating and maintaining an accurate list of the devices in your IT environment. Finding and listing all addressable devices and computers within a managed IT environment is the job of automated *discovery*.

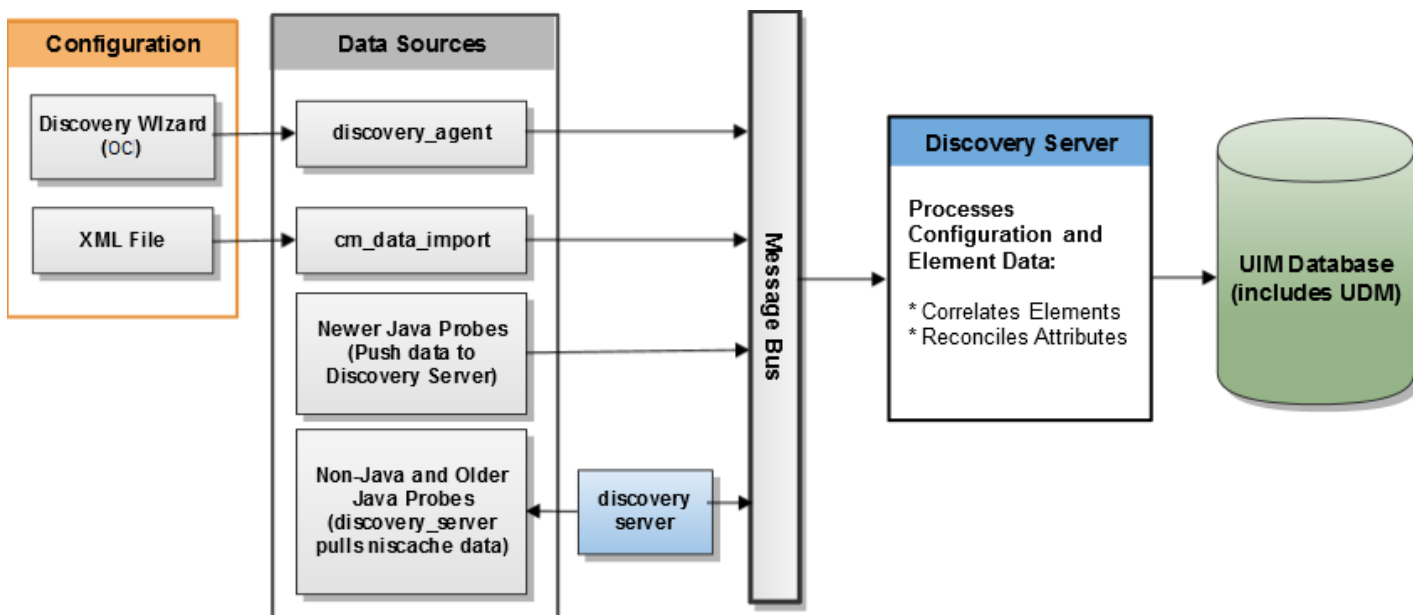
Once the Operator Console (OC) is installed, the Discovery Wizard can be opened from the Settings and prompts you to configure and run discovery. The wizard allows you to specify authentication credentials and define IP address ranges to scan. Discovery finds virtually all connected resources on the network and provides detailed information about device type, configuration, and asset/inventory data. By using ICMP, ARP, DNS, SNMP (v1, v2, and v3), WMI, SSH, and NetBIOS, discovery finds a wide range of devices and device information.

The list of devices, referred to as your *Inventory*, can be augmented by XML file-based device import. When multiple discovery records correspond to a single device, device correlation and reconciliation is performed to ensure that the device is only listed once.

To maintain current inventory, re-run discovery through the wizard at any time, modifying the credentials and scopes as needed. You can schedule discovery to run on regular intervals.

This diagram illustrates the flow of data among the key components of discovery:

Figure 9: Discovery Architecture



## Discovery Components

All discovery components are included in a basic installation of CA Unified Infrastructure Management.

### Discovery Wizard

The Discovery Wizard lets you easily configure discovery scans. To launch the wizard, open the Operator Console(OC) and select **Setup Wizard**. You can open the Discover Devices wizard by clicking on the tile. The wizard lets you specify authentication profiles and the range of addresses you want to search. Discovery then uses this information to scan the network and populate the device inventory.

### Discovery Server probe

In most installations, the `discovery_server` probe runs on the primary hub. The probe performs these major tasks:

#### NOTE

Starting with UIM 20.3.3, a new parameter (`using_datomic`) has been introduced. This parameter lets you decide whether you want `discovery_server` to use the `udm_manager` probe (Datomic). If you do not want `discovery_server` to use `udm_manager`, you can specify the value as `false`. The `discovery_server` probe then does not try to perform any Datomic transactions, and all the data is stored in the relational database. You can set this parameter by using the raw configuration or by updating the `discovery_server.cfg` file (under `setup/udm/`). If you are integrating with DX NetOps Spectrum or Network Flow Analysis (NFA), then it is recommended that you allow `discovery_server` to continue using the `udm_manager` probe.

- Configures discovery agents and collects status from them.
- Collects information about the UIM Server infrastructure: hubs, robots, probes, packages, monitored systems or devices, monitored subsystems or items and monitored metrics.
- Collects device data from probes that publish discovery information.
- Applies correlation rules to associate new device records, where appropriate, with any already-existing master device records. One example is to represent multi-homed devices (devices with multiple network interfaces) accurately.

**NOTE**

Beginning with CA UIM 8.51, device correlation is configurable. You can turn correlation rules on and off, reorder rules, alter existing rules, and create and add new rules. For more information, see [Device Correlation Configuration](#) page.

The information that is collected by the `discovery_server` probe is stored in both UDM and the CM\* tables within the UIM database and used by other UIM Server components. The `discovery_server` probe also helps maintain the database by expiring inactive systems that don't have any associated QoS data.

**NOTE**

Even without any `discovery_agent` probes deployed, the `discovery_server` probe is still needed to generate the data required by other components.

**Discovery Agent probe**

The `discovery_agent` probe scans the IT network, pinging and querying devices according to subnet masks/ranges, credential profiles, and selected profiles. These scanning parameters are configured within the Discovery Wizard.

**CM Data Import**

This probe processes an XML file that describes devices and authentication profiles. Device information is added to your inventory. Authentication profiles are accessible in the Discovery Wizard. The `cm_data_import` probe is usually co-located with `discovery_server`, typically on the primary hub. When you run file-based import from the Discovery Wizard, `cm_data_import` does the work.

**Additional Components**

Additional components that play a role in discovery:

**probeDiscovery queue**

This queue on the primary hub collects discovery data that is processed by the discovery server. On secondary hubs, you will configure `probe_discovery` queues to collect data and route it to the primary hub. See [Configure Discovery Queues](#).

**UIM Database**

The UIM Database is the database that holds all persistent data, including discovery data.

**WARNING**

Some data in the UIM database is stored in parallel in the UDM database. Manually deleting these entries from the UIM database can cause UDM data to be out of sync if not performed correctly. Use the **`remove_master_device`** callbacks to ensure that entries are deleted cleanly from both the UIM and UDM databases. See [Remove Master Devices through Discovery Server](#) for more information.

**Other monitoring probes**

All monitoring probes provide information about systems that are monitored to the Discovery Server. Several of these probes publish directly to the probe Discovery queue. These monitoring probes help supplement auto-discovery.

**Discovery Considerations**

This article describes general use of Discovery:

- Starting with UIM 20.3.3, a new parameter (`using_datomic`) has been introduced. This flag is intended to make the `discovery_server` probe function without having `udm_manager`. In this release of 20.3.3, the default value of this flag is true and users can set it to false if they want to stop using `udm_manager` or `Datomic`. You can set this parameter by using the raw configuration or by updating the `discovery_server.cfg` file (under `setup/udm/`). The `discovery_server` probe then does not try to perform any `Datomic` transactions, and all the data is stored in the relational database. This flag mainly impacts the way how device interfaces are processed within `discovery_server`. When using `udm_manager` or `Datomic`, the device interfaces information is stored in `Datomic` first and then ported to the relational database. When `udm_manager` is disabled and `discovery_server` is configured with `using_datomic = false`, then the device interfaces information is stored only in the relational database. No data is propagated to `Datomic`. So, if there are any other probes that read information from `Datomic`, you must run `discovery_server` with `using_datomic = false` and enable `udm_manager`.  
If `using_datomic` is changed from true to false, then the `Datomic` is not updated further.  
If `using_datomic` is changed from false to true, it takes awhile to populate `Datomic` with all the inventory information. During the course of the inventory graph processing, `Datomic` is filled with the inventory information. The time to re-populate depends on the frequency at which probes publish the full graphs to `discovery_server`.

**NOTE**

If you are integrating with DX NetOps Spectrum or Network Flow Analysis (NFA), then it is recommended that you allow `discovery_server` to continue using the `udm_manager` probe.

- In version 8.1, `discovery_server` began using `log4j` as its logger to capture UDM logging. Use of `log4j` results in the following changes to logging:
  - Settings in the new `log4j.xml` replace `logsize` in the `.cfg` file.
  - The 8.1 `discovery_server.cfx` removes `logsize` from the `.cfg` file.
  - The logging mechanism in previous versions would always log some messages. Beginning with v8.1, messages are logged by default only if there are errors. This may result in an empty log file when discovery proceeds without errors. You can change this behavior by modifying the root priority value in the `log4j.xml` file.
- `Discovery_server` and UDM Manager are coupled beginning with UIM Server v8.1, and `udm_manager` and `discovery_server` probes must have the same major UIM release versions (8.2x, 8.3x, etc.). Some data in the UIM database is stored in parallel in the UDM database, and manually deleting these entries from the UIM database can cause UDM data to be out of sync. Use the **`remove_master_device`** callbacks to ensure that entries are deleted cleanly from both the UIM and UDM databases. See [Remove Master Devices through Discovery Server](#) for more information.
- `Discovery_server` functions as a `Datomic` transaction peer for populating UDM. When there is a heavy load on the system and `discovery_server` is processing large graphs, the transaction timeout interval can be exceeded prior to returning all data. An error message appears in the log file when this occurs. The timeout can be reset to another value by configuring the config file or through raw configuration of the probe. See [Set the Probe Transaction Timeout Value](#) under Advanced Configuration for more information.
- Discovery supports subnets with a CIDR notation number of /16 or larger only. Entering range scopes larger than 65,536 addresses when defining a discovery range might result in one of the two following behaviors:
  - When using the `snmpcollector` probe to query for a list of devices, defining a range greater than /16 will generate an exception with an error message indicating that the query is not supported.
  - When using the Discovery Wizard to define one or more subnets using the same CIDR notation, defining a range greater than /16, or entering multiple /16 ranges will generate an out of memory exception.

**Prerequisites and Supported Platforms****NOTE**

Discovery Agent uses password authentication to connect to a target device over SSH. Discovery Agent cannot communicate with a device where SSH is configured for other authentication methods, such as keyboard-interactive. Discovery Agent also does not support public key authentication or challenge-response authentication.



Discovery\_server 8.40 or later requires CA Unified Infrastructure Management 8.4.

- Discovery\_server 8.40 only works with 7.x and later discovery agents. The discovery\_server raises an alarm for any pre-v7.0 discovery\_agent it finds.
- Discovery\_server 8.40 does not collect any discovery results from pre-7.0 discovery agents.

#### NOTE

Although discovery\_server can run with an older version of discovery\_agent, it is best to use a discovery\_agent version that matches the discovery\_server version. For example, if you are running discovery\_server 8.40, then use the discovery\_agent 8.40. This will give you the latest enhancements and fixes.

The UDM Manager probe must be active for discovery server to function. From CA Unified Infrastructure Management version 8.1 forward, discovery functionality requires version compatibility between UDM clients, the UDM Manager probe, and the discover\_server probe. In upgrading components of CA UIM, if UDM clients, UDM Manager, and discovery\_server do not have the same version number, the installation will fail and error messages will appear in the log. If there is a mismatch between the schema version and the discovery\_server probe, the probe will be disabled on initialization. To reestablish proper functionality, upgrade all components to the same version and rerun discovery.

#### NOTE

Only bus users with the Discovery Management permission in their ACL can perform discovery.

For supported system platforms, see the [Compatibility Support Matrix](#).

## Configuring Discovery

Here is how the discovery process works.

1. The components that are required for discovery are deployed when you install UIM Server. See [Discovery Probe Deployment](#) for deployment considerations.
2. If your installation includes secondary hubs, configure *probeDiscovery* queues so that messages with the *probe\_discovery* subject reach the primary hub. See [Configure Discovery Queues](#).
3. You install OC, which includes the Discovery Wizard.
4. After you install OC, the Discovery Wizard can be launched in Setup Wizard and leads you through the process of configuring discovery. You will:
  - a. [Create authentication profiles](#).
  - b. [Define ranges](#) of IP addresses and IP masks that define and bound the scope of discovery.
  - c. [Schedule discovery](#).

#### NOTE

If you don't want to create your inventory now or if you want to create it solely with file-based import, cancel the wizard. You can run discovery or import devices at any time.

5. To augment automated discovery, you can prepare an XML file with device information and can import this information into the device inventory. See [Run File-based Import](#).

#### NOTE

If desired, you can create your inventory solely with file-based import.

6. When discovery is complete, you can view computers and devices that have been discovered on your network. See [View Discovered Systems](#).
7. You can schedule discovery to update the list of system components automatically in the Discovery Wizard in the Schedule tasks.

## Discovery Probe Deployment

The components (probes) required for discovery are deployed on the primary hub with a basic install of UIM Server:

- Discovery Server
- Discovery Agent
- CM Data Import

Consider the following points if you want to modify the default discovery probe deployment:

- For minimal discovery, only the `discovery_server` probe is required. No network scanning is performed.
- A domain should have a single instance of `discovery_server`. Deploying multiple `discovery_server` probes is not supported and results in adverse behavior.
- To add network scanning, configure the `discovery_agent` probe on the UIM primary hub or deploy and configure a discovery agent at another location.

### NOTE

The alternative location can be any robot. The hub robot is a reasonable default, but another robot may be chosen for load balancing purposes.

A hub is often a convenient location for the discovery agent because hubs are often installed in different parts of the network. The most important consideration is that the target IP addresses can be reached from the installed discovery agent location.

- For optimal discovery in larger environments, more than one discovery agent can be deployed. Some users, particularly service providers and those with very large networks, find it useful to deploy multiple discovery agents in various locations. Discovery of a large network can be divided across administrative boundaries with no direct connectivity to devices at a remote site because of firewall constraints or network-address translation (NAT). For efficient discovery and to avoid duplicate device entries, deploy discovery agents such that each one discovers an exclusive part of the network.
- The WMI protocol is only supported for `discovery_agent` probes running on Windows systems.

### NOTE

Discovery Agent requires read-only SNMP access to network devices. To simplify discovery configuration, consider setting up network devices to use a "universal" read-only community string (SNMP v3 recommended over v1 or v2c). For example, you could define read-only (get-only) credentials to be **"uim\_get\_only"**. Set up every device possible to allow read-only SNMP access via those credentials: this minimizes the number of SNMP authentication credentials that must be attempted on network nodes and vastly simplifies your discovery configuration.

The `discovery_agent` probe installation must include the applicable `java_jre` package. Appropriate `java_jre` versions are:

- CA UIM 8.51 and later: `java_jre` package 1.8
- CA UIM 8.5 and earlier: `java_jre` package 1.7

Recommended minimum hardware requirements for deploying Discovery Agent on a server are given in [Prepare Your Server Hardware](#).

## Configure Discovery Queues

If all discovery process probes are deployed on a single hub, communication of discovery data is automatically configured. However, if discovery probes are deployed to hubs *other* than the hub that hosts the `discovery_server` probe, ensure that discovery data can flow from those hubs up to the primary hub.

Flow is accomplished by setting up queues that handle the `probe_discovery` subject:

- You can use a combination of *attach* and *get* queues. An *attach* queue creates a permanent queue on a downstream hub. A corresponding *get* queue set up on the upstream hub is paired with each *attach* queue to retrieve messages from the downstream hub.
- Alternatively, you can use *post* queues. A *post* queue set up on a downstream hub sends a directed stream of messages to the upstream hub.

An *attach* queue is automatically set up on the primary hub to collect discovery data. Set up additional queues to collect discovery data from downstream hubs that host *discovery\_agent* or any CTD-publishing probes. This list includes (but is not limited to):

- *discovery\_agent*
- vmware 5.10 or later
- *cm\_data\_import* (typically deployed with *discovery\_server* on the primary hub)
- *snmpcollector*
- *vcloud*
- *rhev* (Red Hat Virtualization)

Then set up a corresponding *get* queue (which retrieves messages from the *attach* queue) on the primary hub and on any hub that transfers the messages to another hub.

You can set up discovery queues in either Admin Console or Infrastructure Manager.

#### Follow these steps:

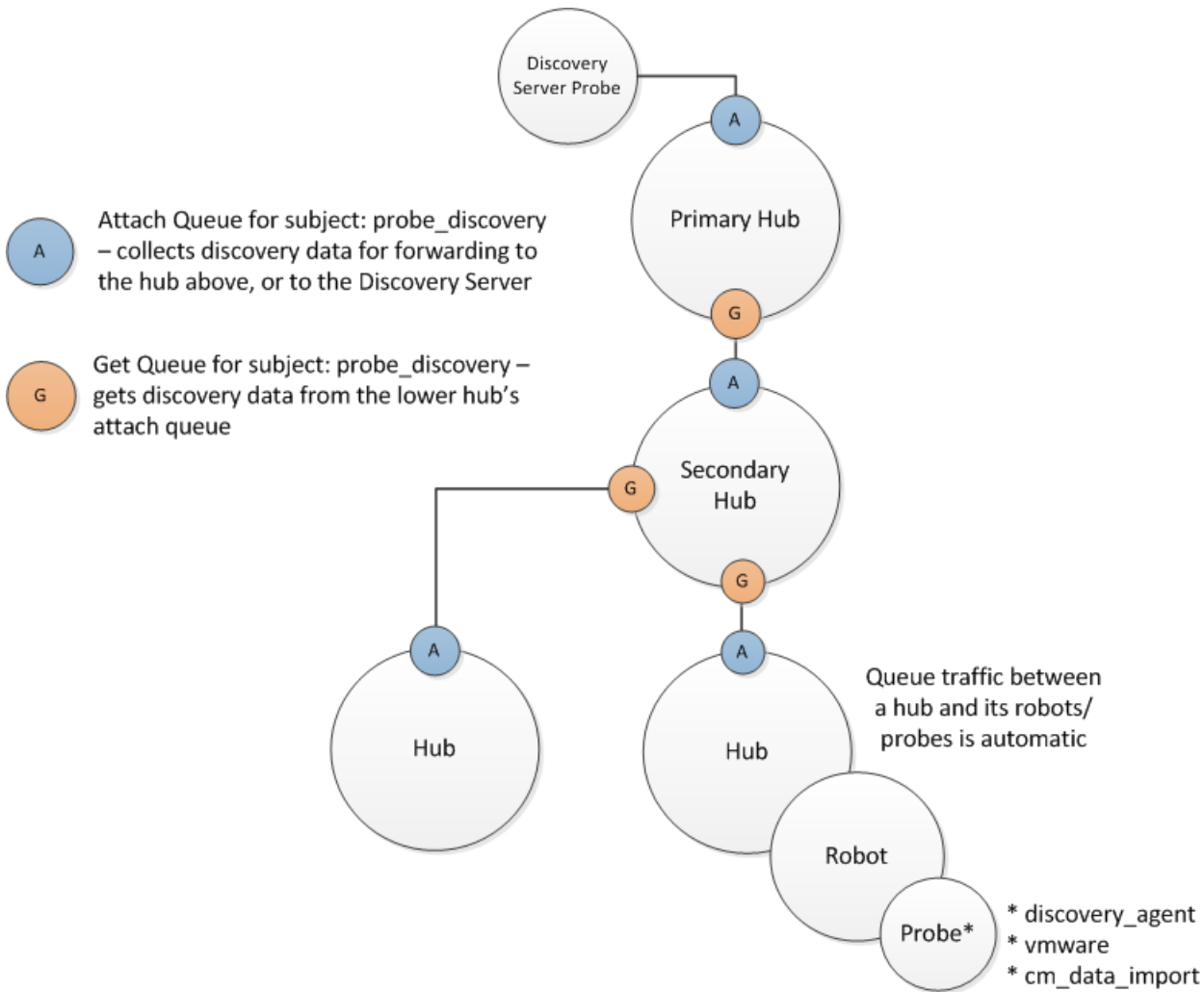
1. Identify the hub on which you want to create a queue and open the hub configuration GUI:
  - *Admin Console*: Expand the hub in the navigation tree and select its robot. Click the arrow next to the hub probe and select **Configure**.
  - *Infrastructure Manager*: Expand the hub node and double-click the hub probe.
2. Navigate to **Queue List** or **Queue**.
3. If you use *attach/get* queues, set up the queues with the corresponding values:
  - *Attach* queue on the downstream hub:
    - **Active**: enabled
    - **Name**: *attachDiscovery* (or other name of your choice)
    - **Type**: *attach*
    - **Subject**: *probe\_discovery*
  - *Get* queue on the upstream hub:
    - **Active**: enabled
    - **Name**: *getDiscovery* (or other name of your choice)
    - **Type**: *get*
    - **Address**: address of the hub that has the *attach* queue
    - **Queue**: name of the corresponding *attach* queue
    - **Bulk size**: number of messages to be transferred together. (Optional: if you expect the queue to carry a significant number of messages, send them in bulk to improve performance.)
4. If you use *post* queues, set up each queue with the corresponding values:
  - *Post* queue on the downstream hub:
    - **Active**: enabled
    - **Name**: *postDiscovery* (or other name of your choice)
    - **Type**: *post*
    - **Subject**: *probe\_discovery*
    - **Address**: address of the upstream hub
    - **Bulk size**: number of messages to be transferred together
5. Repeat the previous steps on all hubs that require a queue.

**NOTE**

In small to medium deployments, a wildcard (\*) subject, which carries any message, can simplify queue configuration. Use of a wildcard subject in large installations is not recommended.

For queue setup details, click the question mark or **Help** button in the configuration GUI.

The following illustration shows discovery queue configuration using *attach/get* pairs. If you use a *post* queue configuration, the flow in the illustration would be similar, but you set up *post* queues instead of *attach* queues on all downstream hubs and you would not need to set up *get* queues.



When you have set up all required queues, run an automated discovery scan to confirm that the queues are operational. Review the list of discovered devices. In addition to local devices, this list would also contain devices that are only addressable from the secondary hubs.

**NOTE**

Setting up other queues for alarms, QoS, and baseline data is a similar procedure of configuring attach and get queues. The subject of the queue changes as required by the type of data to be carried.

## Launch the Discovery Wizard

The first time that you open the Operator Console (OC), the Discovery Wizard is launched from the Setup wizard.

You can launch the Discovery Wizard whenever you want to run discovery or change your discovery settings. You can launch the Discovery Wizard from the **Inventory** node or from the **Setup Wizard**.

### NOTE

The Discovery Wizard will not run after an update of CA Infrastructure Management if there are existing range scopes that define *excluded* IP addresses. Either accept the system prompt to delete excluded range scopes or remove them manually from the database. Then, discovery will run.

### Follow these steps:

1. Hover the cursor over the name of a discovery agent or range in the tree or click on it. The magnifying glass icon



indicates discovery agents. The network icon



indicates ranges.

2. Click the gear icon



to the right of the discovery agent or range name in the tree, or select **Discovery Wizard** from the **Setup Wizard**.

## Navigating in the Discovery Wizard

Be aware of the following when using the Discovery Wizard:

- If you click the **Close** button or the **X** icon in the title bar before completing the Discovery Wizard, you are prompted to save your changes. If you execute discovery by clicking **Finish** on the final screen, changes are saved.
- If valid information is entered in the required fields of an authentication profile or network scope, the information is automatically saved when you click **Next**. Required fields are outlined in red.
- Passwords for authentication profiles are displayed as asterisks. If you want to see a password as you enter it, click the *show password* icon



next to the **Password** field. When you click **Next**, the password is displayed as asterisks.

## Create Authentication Profiles

Authentication profiles allow you to create, edit, view, and delete authentication profiles for discovery. A profile contains credential information necessary to access and gather information about computer systems and devices in your network.

You can create one or more authentication profiles under each of the WMI, Linux/Unix, and SNMP tabs.

### NOTE

Creating authentication profiles is not required for discovery. However, only IP discovery is used if no authentication profiles exist, and information about discovered systems might be limited.


To return further information, the user must create credentials using the authentication profiles defined by the system administrator for the target devices.

### Follow these steps to create an authentication profile:

1. After clicking on the device, Click **New credentials** in the left pane.
2. Enter information in all required fields. Required fields are outlined in red.

**NOTE**

You must use a unique name for each authentication profile name. You can reuse authentication profile names once the previous profile is deleted.

3. Click **Next**. The information that you enter is saved when you click **Next** and move through the Discovery Wizard.
  - – To view the properties of an existing profile, select the appropriate authentication tab and then select a profile in the left pane.
  - To modify an existing authentication profile, select it and edit the fields as necessary, and then click **Save**. To delete an authentication profile, click the trash can icon  next to the name of the profile in the left pane, and click **Save**.

Configuration details specific to each protocol, such as acceptable credential formats, are outlined in the protocol pages

**Linux/Unix**

Linux/Unix authentication profiles use SSH or Telnet to access and discover Linux and Unix systems.

- **Description** - Name for the authentication profile.
- **ID** - This read-only field is the UIM system ID for this authentication profile, which is assigned when the profile is saved. The ID identifies the profile uniquely for reuse in other areas of OC that reference authentication profiles.
- **User** - The user name assigned by the administrator of the target systems.
- **Password** -The user password assigned by the administrator of the target systems. Check the **Show new passwords** check box to verify the text as you enter it.
- **SSH or Telnet** -Select the communication protocol to use, SSH (Secure Shell) or Telnet (no secure authentication or encryption).

CA Unified Infrastructure Management  
UIM

Home

Configure Device Discovery

Setup WMI Credentials | Setup Linux/Unix Credentials | Setup SNMP Credentials | Define Scopes | Schedule Discovery

Search

- Lcred1
- L22
- L33

**Lcred1**

Name  
Lcred1

ID  
19

User  
root

Password  
.....

SSH  Telnet

Remove

Cancel

• **NOTE**

Profiles will accept any username and password entered, but only those assigned by the administrator of the target systems will return information. There is no validation of user names and passwords in the window.

**NOTE**

Discovery Agent uses password authentication to connect to target devices over SSH. Discovery Agent cannot communicate with a device where SSH is configured for other authentication methods, such as keyboard-interactive or challenge-response authentication.

## SNMP

Discovery supports SNMP versions 1, 2c, and 3. SNMP v3 provides security features that are not available in v1 and v2c. As a result, authentication profile configuration fields in the Discovery Wizard that deal with security and privacy (encryption) are only active when you select **3** in the **Version** pull-down menu.

**NOTE**

SNMP authentication profiles can also be imported from an XML file. See [Run File-based Import](#) for details.

We recommend the following best practices:

- Create the minimal set of SNMP authentication profiles to provide SNMP access to all devices and hosts that support SNMP.
- Set up as many of your network devices as possible to use "universal" read-only credentials. For example, you could define a read-only (get-only) credential to be **nms\_get\_only**. Then, set up every device possible to allow read-only SNMP access through this universal credential. Universal credentials minimize the number of SNMP authentication credentials that must be attempted on network nodes, and simplifies discovery configuration.
- If there are devices that accept unique SNMP credentials, create one authentication profile for each of them. You can specify a unique port within the range of 1 to 65535 for the profile. If no port is specified, the default port 161 is used.

For network devices such as routers and switches, SNMP is the sole source for detailed discovery information. For host systems such as Windows, Unix, or Linux servers, you should use WMI or SSH discovery in addition to SNMP. While SNMP provides the most complete network interface information for devices and systems, the host system information available from SNMP (such as processor attributes) is less complete than the information obtained from WMI or SSH. Use WMI or SSH plus SNMP discovery for host systems to provide the most comprehensive set of host and network interface information.

The screenshot shows the 'Configure Device Discovery' wizard in the CA UIM interface. The breadcrumb trail is 'Home > Setup Wizard > Discover Devices'. The wizard has five steps: 'Setup WMI Credentials', 'Setup Linux/Unix Credentials', 'Setup SNMP Credentials', 'Define Scopes', and 'Schedule Discovery'. The 'Setup SNMP Credentials' step is active, showing a list of credentials on the left and a configuration form for 'SNMPCred1' on the right. The list on the left contains one entry, 'SNMPCred1', with a search bar above it. The configuration form for 'SNMPCred1' includes the following fields:

- Name:** SNMPCred1
- ID:** 33
- Version:** 1
- User:** (empty text field)
- Community string:** (masked text field)
- Port:** 161
- Method:** MD5
- Security:** NOAuthNoPriv
- Priv.Protocol:** DES
- Priv.Password:** (empty text field)

There is a 'Remove' button below the configuration form and a 'Cancel' button at the bottom left of the wizard.

For devices that are enabled with the CA SystemEDGE agent, you can create SNMP authentication profiles and monitor them with the snmpcollector probe (v3.0 and later).



**SNMP v1 or v2 Fields**

The SNMP version that the monitored device supports. When version 1 or 2 is selected, only the Community field is active.

| Field       | Required | Description                                                                                                                                                                                                            |
|-------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | Yes      | Name for the authentication profile                                                                                                                                                                                    |
| ID          |          |                                                                                                                                                                                                                        |
| Version     | No       | The SNMP version that the monitored device supports. When version 1 or 2 is selected, only the Community field is active.                                                                                              |
| Community   | Yes      | The SNMP community string. Check <b>Show new passwords</b> to verify the text as you enter it. This string is sent across the network in clear text as part of SNMP v1 or v2c requests and might pose a security risk. |

**SNMP v3 Fields**

The SNMP version that the monitored device supports. Versions 1, 2c, and 3 are supported. When v3 is selected, other fields for security and privacy are enabled. The SNMP v3 username to access the monitored device. Required for all SNMP v3 security levels. See the description for the Security field.

| Field       | Required                                                                                                    | Description                                                                                                                                                                                                                                                                                                                              |
|-------------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | Yes                                                                                                         | The name for the authentication profile                                                                                                                                                                                                                                                                                                  |
| ID          |                                                                                                             |                                                                                                                                                                                                                                                                                                                                          |
| Version     | Yes                                                                                                         |                                                                                                                                                                                                                                                                                                                                          |
| Password    | Enabled and required if <b>AuthNoPriv</b> or <b>AuthPriv</b> is selected (see <i>Security</i> description). | The password that is associated with the SNMP v1/v2c device or SNMP v3 user. Check <b>Show new passwords</b> to verify the text as you enter it. This field is enabled and required if either AuthNoPriv or AuthPriv security is selected. See the description for the Security field.                                                   |
| User        | Yes                                                                                                         |                                                                                                                                                                                                                                                                                                                                          |
| Method      | Yes                                                                                                         | The SNMP v3 method of encryption, when AuthNoPriv or AuthPriv security is selected (see the description for the Security field): <ul style="list-style-type: none"> <li>• <b>MD5</b> - MD5 Message-Digest Algorithm (HMAC-MD5-96)</li> <li>• <b>SHA</b> - Secure Hash Algorithm (HMAC-SHA-96, SHA-256)</li> <li>• <b>None</b></li> </ul> |

|               |                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security      | Yes                                                    | <p>The SNMP v3 security level of the user. Depending on what level of security is selected, other security fields are enabled or disabled:</p> <ul style="list-style-type: none"> <li>• <b>NoAuthNoPriv</b> - messages sent unauthenticated and unencrypted.</li> <li>• <b>AuthNoPriv</b> - messages sent authenticated but unencrypted.</li> <li>• <b>AuthPriv</b> - messages sent authenticated and encrypted.</li> </ul> |
| Priv.Password | Enabled and required when <b>AuthPriv</b> is selected. | <p>The SNMP v3 privacy password to use when <b>AuthPriv</b> security level is selected. The password must contain at least eight characters. Do not confuse the privacy password with the user authentication password.</p>                                                                                                                                                                                                 |
| Priv.Protocol | Enabled and required when <b>AuthPriv</b> is selected. | <p>The SNMP v3 privacy (encryption) protocol to use:</p> <ul style="list-style-type: none"> <li>• <b>DES</b> - Data Encryption Standard</li> <li>• <b>AES</b> - Advanced Encryption Standard</li> </ul>                                                                                                                                                                                                                     |

## WMI

WMI (Windows Management Interface) discovery scans servers and hosts running Windows to gather system information. WMI discovery runs only on discovery agents that are hosted on Windows systems.

- **Description** - Name for the authentication profile.
- **ID** - This read-only field is the system ID for this authentication profile, which is assigned when the profile is saved. The ID identifies the profile uniquely for reuse in other areas of OC that reference authentication profiles.
- **User** - The user name defined by the administrator of the target systems. A user name in the form of **Domain\user name**, **user\_name** and **IP\_address\user\_name** are also allowed.
- **Password** - The password defined by the administrator of the target systems. Check the **Show new passwords** check box to view the text as you enter it.

The screenshot shows the 'Configure Device Discovery' wizard in the CA Unified Infrastructure Management (UIM) interface. The 'Setup WMI Credentials' tab is selected, showing a list of credentials on the left and a configuration form for 'Cred1' on the right. The list includes 'Cred1', 'Test1', and 'SQL'. The configuration form for 'Cred1' shows fields for Name (Cred1), ID (19), User (administrator), and Password (masked). A 'Remove' button is visible below the form. A 'Cancel' button is at the bottom left.

**NOTE**

Profiles will accept any username and password entered, but only those assigned by the administrator of the target systems will return information. There is no validation of user names and passwords in the window.

**Define Scopes**

Use the **Define Scopes** tab of the Discovery Wizard to define addresses, ranges, or masks for devices to be discovered. At least one network range must be entered for discovery to run.

You can assign any combination of SNMP, Linux/Unix, and WMI authentication profiles to a range scope. The discovery process records *any* device within a range that responds to a request on any protocol, including a simple ICMP ping. You can include end nodes (such as servers, network printers, network storage systems, or workstations) in a range even if they do not respond to requests using SNMP or other management protocols.

If an authentication profile is not assigned to a range scope, basic discovery is performed using protocols that do not require authentication. As a result, discovery might not be complete and information about discovered systems is limited.

CA Unified Infrastructure Management  
UIM

Home > Setup Wizard >  
**Discover Devices**

Configure Device Discovery

Setup WMI Credentials | Setup Linux/Unix Credentials | Setup SNMP Credentials | Define Scopes | Schedule Discovery

Search

- R1
- r66
- Mask

New Range Scope

Name  
R1

Scope Definition

Range 10.74.113.225 to 230

Range 10.74.113.0 to 255

Credentials

Search All

Linux/Unix

- Lcred1
- L22
- L33

WMI

- Cred1
- Test1
- SQL

Cancel

## NOTE

**More information:**

## Best Practices for Creating Scopes

For each discovery agent, review the assigned range scopes to minimize predictable timeouts. To optimize performance and avoid duplicate entries, each discovery agent should discover an exclusive part of the network.

Tips to decrease discovery run time:

- You **MUST** use IPs when populating scopes. Use of hostnames is not supported in defining scopes.
- The discovery agent tries each credential on each IP address and waits for success or a timeout with each attempt. To speed up discovery, use a single credential in a scope that has a high probability of immediate success.
- When you apply an authentication profile, verify that most (if not all) devices in that scope accept the authentication profile.
- If you include devices that do not respond to requests on any management protocol, place them in a discovery range scope with no authentication profiles.
- If you use SNMP for devices that accepts only a unique SNMP community string, create a Single type range scope and specify the device IP addresses. Assign the corresponding authentication profile to the range scope.
- When using SNMP, to avoid unnecessary authentication traps/alerts, assign only one SNMP authentication credential per discovery range.

## Create a Range Scope

### Contents

Ranges are defined under the Scopes tab of the Discovery Wizard.

### Create Range Scopes

#### Follow these steps:

1. Click New scope in the left pane of the **Scopes** tab.
2. Enter a name for the range scope.
3. In the Range Scope definition section, specify the area(s) of your network where you want to perform discovery.
  - Mask - Defines a subnet using Classless Inter-Domain Routing (CIDR) notation with a base IPv4 address and a routing prefix. For example, 195.51.100.0/24. The value /24 refers to a Class C subnet of 256 addresses. Other values for reference: /30 (4 addresses) and /16 (65,536 addresses, or a Class B subnet).

#### **NOTE**

When you enter a subnet mask, the number of IP addresses the mask represents is displayed (the number of effective hosts minus two). Only /16 subnets or smaller are supported.

- Range - Range of IPv4 addresses.
  - Single IPv4 or IPv6 address. You can use abbreviated IPv6 address forms, and IPv6 addresses that refer to IPv4 addresses. However, anycast, multicast, link-local, and loopback addresses are not supported.
4. Click **New IP range or single IP address** to add another IP range, address, or mask if desired.
  5. In the Credentials section, you can assign authentication profiles to the selected range. By default, all of the authentication profiles are selected. If you have a large number of authentication profiles in the list, you can enter the name of a profile to filter the list.
  6. To view only the profiles that are selected, click the **Hide unused credentials** check box.

### Assign Authentication Profiles

In the Credentials section, you can assign authentication profiles to the selected range. By default, all of the authentication profiles are selected.

When you have finished defining scopes, click **Next**.

## Schedule Discovery

In the Schedule tab, you can schedule discovery to run in the future, and/or you can run discovery immediately. You can schedule either a single discovery run or recurring runs.

A scheduled discovery does not interrupt a discovery that is already running. If at the time a discovery run is scheduled another discovery run is in progress, the scheduled discovery is ignored.

If you select **Run discovery now** and discovery is in progress, the current discovery run is terminated and the new run is executed.

### Follow these steps to start and/or schedule discovery:

1. Leave the **Run discovery now** check box selected unless you do not want to run discovery when you complete the Discovery Wizard.
2. To schedule discovery, select the **Schedule discovery** check box.
3. Enter information in the date and time fields.  
The time field is in 24-hour format. The time is the local time of the user.
4. To schedule recurring discovery runs, select the **Recurring every** check box, and enter the number of hours for the recurrence interval.
5. Click **Finish** to complete the Discovery Wizard.

The screenshot shows the 'Configure Device Discovery' wizard in the CA Unified Infrastructure Management (UIM) interface. The user is logged in as 'administrator' and is on the 'Schedule Discovery' tab. The wizard is for a selected agent: 'lvnqa012407\_hub/lvndev012409'. The 'Discovery Schedule' section explains that users can run discovery immediately and/or in the future. It notes that 'Run Discovery Now' terminates any current discovery and initiates a new one, while 'Scheduled Discovery' overwrites previous configurations. The 'Configure' section has two checked options: 'Run Discovery Now' and 'Schedule Discovery'. The 'Starting' date is set to 8/7/2020 and the 'At' time is 19:58, with a '(24 Hour)' label. The 'Recurring Every' option is also checked, with a value of '24' hours. At the bottom, there are 'Cancel', 'Previous', and 'Finish' buttons.

## Run File-based Import

In many IT environments, device and host configuration information is maintained in a configuration management database (CMDB). If you have this data, you might prefer to import your device information and SNMP authentication profiles through file-based import. With this method, you import an XML file that contains your device and profile data. Scanning the IT environment is not necessary.

This method offers several benefits:

- **Speed.** Automated discovery can take several hours or longer in an enterprise deployment. An XML file can be imported in minutes.
- **More control over your inventory.** File-based import helps to ensure that your inventory includes all the devices you want to monitor, and no others. Automated discovery

could add devices that you are not interested in (such as printers or personal computers) or fail to include devices that are temporarily non-responsive.

- Fewer security alerts.

#### NOTE

The **cm\_data\_import** probe imports device and SNMP authentication data. If automated discovery finds a system automated discovery that is also included in file-based import, the information from file-based import takes precedence for most properties. However, precedence depends on device reconciliation rules and heuristics. Device reconciliation is the process of aggregating data from multiple views of the same device and resolving the data into a single device view.

**Note:** The XML schema was updated for **cm\_data\_import** version 7.6 to support the import of SNMP authentication profiles. While the probe imports XML files using the old schema, we recommend that you migrate to the new schema.

You can launch file-based import by navigating to the file in OC or by placing the file in a directory where **cm\_data\_import** can find it.

#### Method 1: Navigate to the XML File

1. Prepare the XML file. See [XML File Schema](#) for details.
2. In the OC left menu, click on the **Inventory**.
3. Click on the **right actions menu** and click the Import.
4. Navigate to the XML file and click **OK**. **cm\_data\_import** publishes the data to the message bus, and **discovery\_server** imports it.

#### Method 2: Automatic file import

The **cm\_data\_import** probe monitors a directory for valid XML files. When it finds one, it automatically imports the information into the database. Here is how the process works:

1. Copy the prepared XML file to `<UIM_install_directory>\probes\service\cm_data_import\import` on the system that hosts the **cm\_data\_import** probe (typically the primary hub).
2. **cm\_data\_import** scans the import directory at regular intervals (default is 60 seconds).
3. When the probe finds the XML file you copied to the directory, it publishes the data to the **discovery\_server**.

#### The result of both methods:

- The XML file is placed in a time-stamped subfolder in `<UIM_install_directory>\probes\service\cm_data_import\processed`.
- The activity of the process is logged.
- The probe publishes the imported information to the **discovery\_server**.
- Processing by **discovery\_server** can take several minutes or more to finish. Once complete, the NIS database stores any devices and authentication profiles.
- Imported devices are listed in the **Inventory** node in OC.
- Authentication profiles are viewable in the Discovery Wizard in OC.
- When importing has completed, you can deploy and configure probes to monitor the imported devices.

## XML File Schema

An XML file can import SNMP authentication profiles, device information, or both. This section describes how to create an XML file for use with file-based discovery.

#### NOTE

The XML schema was updated for **cm\_data\_import** version 7.6 to support the import of SNMP authentication profiles. While the probe imports XML files using the old schema, we recommend that you migrate to the new schema. Refer to:

- `<UIM_install_directory>/probes/service/cm_data_import/schema` - new XML schema definition file and example XML files
- `<UIM_install_directory>/probes/service/cm_data_import/schema_old_201211` - previous schema and example files for reference

Note the following parameters.

- The schema allows you to define subsections for for:
  - Devices
  - SnmpV1Profiles
  - SnmpV2Profiles (for SNMP V2c profiles)
  - SnmpV3Profiles
- The definition for V1 and V2 SNMP profiles is the same, but they are placed in the XML file in different sections. The sections identify which are V1 profiles and which are V2 profiles.
- Properties in the schema that contain **minOccurs="1"** are required.
- For properties that refer to open enumerations, go to `<UIM_install_directory>\probes\service\cm_data_import\schema` and open either **usm-openenums.xml** or **cm-data-import-openenums.xml** to view the defined values. Although it is not strictly required, we strongly recommended that you use values defined by the open enumerations.
- In addition to the subsections listed above, the following top-level properties are available in the CmData section:

| Property                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DefaultOrigin</b><br><i>Optional</i>      | Top-level property that specifies the origin to be assigned to any device that does not have a specified origin.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>PasswordsEncrypted</b><br><i>Optional</i> | Top-level property that specifies whether the passwords in SNMP profiles are encrypted. If the value is unspecified or set to false and the XML file includes unencrypted passwords, in the XML file that is saved to the processed directory, the passwords are encrypted and PasswordsEncrypted is set to true. Because UIM uses a custom encryption method, you can let cm_data_import encrypt the passwords for you. You can copy the XML file from the processed directory in order to use the encrypted passwords in the future. |

### Device Examples and Properties

A minimal device XML file must include these properties for each host or device:

- At least one property that enables the device to be correlated: *PrimaryIPV4Address*, *PrimaryIPV6Address*, *PrimaryDnsName*, *PrimaryMacAddress* or *VirtualID*.
- *Origin* or *DefaultOrigin*. This value identifies the hub from which entity QoS messages originate. Setting the origin correctly is important; see the following table for details.

The following example shows how to create a *Devices* section that imports one device with IP address **1.2.3.4** and origin **MyOrigin**.

```

- <Devices>
- <Device>
 <PrimaryIPV4Address>1.2.3.4</PrimaryIPV4Address>
 <Origin>MyOrigin</Origin>
</Device>
</Devices>

```



More optional properties can be included, as shown in the following example. You can find example files in `<UIM_install_directory>\probes\service\cm_data_import\schema` on the system that hosts `cm_data_import` (typically the primary hub).

```
- <Devices>
- <Device>
 <ElementUUID>550e8400-e29b-41d4-a716-446655440000</ElementUUID>
 <Origin>myOrigin</Origin>
 <Label>myComputer</Label>
 <Description>myComputerIsFast</Description>
 <PrimaryDnsName>myComputer.myCompany.com</PrimaryDnsName>
 <OtherDnsNames>name2,name3</OtherDnsNames>
 <PrimaryIPv4Address>1.2.3.4</PrimaryIPv4Address>
 <PrimaryIPv6Address>fe80::223:ebff:fe06:9d40</PrimaryIPv6Address>
 <OtherIPAddresses>2.2.2.2,3.3.3.3</OtherIPAddresses>
 <PrimaryMacAddress>F0-4D-A2-25-5B-7A</PrimaryMacAddress>
 <OtherMacAddresses>22-22-22-22-22-22,33-33-33-33-33-33</OtherMacAddresses>
 <PrimaryOSType>WindowsServer-2008</PrimaryOSType>
 <PrimaryOSVersion>6.1.7601</PrimaryOSVersion>
 <ProcessorType>x86-64</ProcessorType>
 <Vendor>Dell Inc.</Vendor>
 <Model>PowerEdge T620</Model>
 <PhysSerialNumber>123-456-789-ABCD</PhysSerialNumber>
 <PrimaryDeviceRole>ComputerSystem</PrimaryDeviceRole>
 <PrimarySoftwareRole>DatabaseServer</PrimarySoftwareRole>
 <DBServerType>MSSQLServer</DBServerType>
 <WmiAuthId>3</WmiAuthId>
 <ShellAuthId>5</ShellAuthId>
 <SnmpAuthId>7</SnmpAuthId>
 <AppServerType>Unknown</AppServerType>
 <VirtualizationEnvironment>Unknown</VirtualizationEnvironment>
 <VirtualID>550e8400-e29b-41d4-a716-446655440000</VirtualID>
 <MonitorFrom>1.2.33.44</MonitorFrom>
</Device>
</Devices>
```

The following table describes the XML properties. Note the following points:

- For properties that refer to open enumerations, navigate to `<UIM_install_directory>\probes\service\cm_data_import\schema` and open either `usm-openenums.xml` or `cm-data-import-openenums.xml` to view the defined values.

Although it is not strictly required, we strongly recommended that you use values that are defined by the open enumerations.

- To deploy a robot to an imported system using OC and the Automated Deployment Engine (ADE), properties beyond IP address and origin are required. These properties are noted in the following table.
- Optional values allow you to add detail to your inventory.

| Property                                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ElementUUID</b><br><i>Recommended; automatically created if not specified</i> | The universally unique identifier for the device. The UUID must be in standard string representation (for example: 550e8400-e29b-41d4-a716-446655440000). If the UUID is not specified, one is automatically generated for the element. If an existing element is found with a matching UUID, the existing element is updated. Otherwise, a new element is inserted and associated with the UUID. To avoid inserting duplicate records, the same UUID per element should be maintained and used on updates. The XML file saved in the processed directory includes any automatically generated UUIDs for later reuse. |
| <b>SnmpProfileUUID</b><br><i>Optional</i>                                        | The universally unique identifier of the authentication profile to use for SNMP access. The specified profile can either be defined in this XML file or have been previously imported.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Origin</b><br><i>Required if DefaultOrigin is not specified</i>               | Identifies the hub from which QoS messages originate. The default origin is the name of the primary hub, but this origin can be overridden at the hub or robot (controller) to separate data in a multi-tenancy environment. To ensure that QoS probe data is correlated to the discovered device, the origin specified here should match the origin that you intend to use.<br>You can avoid specifying this value for each device by specifying the top-level <i>DefaultOrigin</i> property.                                                                                                                        |
| <b>Label</b><br><i>Optional</i>                                                  | A short description or caption.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b><br><i>Optional</i>                                            | Text description of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>PrimaryDnsName</b><br><i>Optional</i>                                         | The entity Domain System Name, which can be used for correlation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>OtherDnsName</b><br><i>Optional</i>                                           | If an entity has multiple DNS names, this property captures those names. ( <i>PrimaryDnsName</i> is used for correlation.) Multiple names must be comma-separated.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>PrimaryIPv4Address</b><br><i>Either IPv4 or IPv6 is required</i>              | An IPv4 address for the entity that can be used for correlation and identity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>PrimaryIPv6Address</b><br><i>Either IPv4 or IPv6 is required</i>              | An IPv6 address for the entity that can be used for correlation and identity. The address is expressed using the formal, complete IPv6 notation (eight groups of up to four hex numbers, using only uppercase letters where applicable and separated by colons).                                                                                                                                                                                                                                                                                                                                                      |
| <b>OtherIPAddresses</b><br><i>Optional</i>                                       | If an entity has multiple IP addresses, this property captures those addresses for correlation and identity. Multiple addresses must be comma-separated. IPv4 or IPv6 values can be specified. Addresses should be formatted following the regex patterns defined by <code>usm-core:IPV4AddressFormat</code> or <code>usm-core:IPV6AddressFormat</code> .                                                                                                                                                                                                                                                             |
| <b>PrimaryMacAddress</b><br><i>Optional</i>                                      | A MAC address that can be used for correlation and identity. The address is expressed as six groups of two hex numbers, using uppercase letters when necessary and separated by dashes.                                                                                                                                                                                                                                                                                                                                                                                                                               |

|                                                                                         |                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OtherMacAddress</b><br><i>Optional</i>                                               | If an entity has multiple MAC addresses, this property captures those addresses. The <i>PrimaryMacAddress</i> property is used for correlation. Multiple addresses must be comma-separated and formatted following the regex pattern defined by <code>usm-core:MacAddressFormat</code> .                            |
| <b>PrimaryOSType</b><br><i>Required by ADE for robot deployment</i>                     | OS type, defined by the open enumeration <i>OSTypeEnum</i> . For Linux systems, ADE requires the Linux distribution name (for example, <b>Linux-RedHat</b> ).                                                                                                                                                       |
| <b>PrimaryOSVersion</b><br><i>Optional</i>                                              | OS version details.                                                                                                                                                                                                                                                                                                 |
| <b>ProcessorType</b><br><i>Required by ADE for robot deployment</i>                     | Processor environment/type (such as "x86") as defined by the open enumeration <i>ProcessorEnvironmentEnum</i> .                                                                                                                                                                                                     |
| <b>Vendor</b><br><i>Optional</i>                                                        | The hardware manufacturer or vendor name, as defined by the open enumeration <i>VendorEnum</i> .                                                                                                                                                                                                                    |
| <b>Model</b><br><i>Optional</i>                                                         | The hardware model name or number.                                                                                                                                                                                                                                                                                  |
| <b>PhysSerialNumber</b><br><i>Optional</i>                                              | ID string assigned by the hardware manufacturer and attached to the component. Enter the number directly from the manufacturer's tag on the component (which might be an RFID tag), or read the value from the <i>entPhysicalSerialNum</i> field of SNMP's Entity-MIB. Virtual entities do NOT have serial numbers. |
| <b>PrimaryDeviceRole</b><br><i>Optional</i>                                             | The device role as defined by the open enumeration <i>DeviceRoleEnum</i> .                                                                                                                                                                                                                                          |
| <b>PrimarySoftwareRole</b><br><i>Optional</i>                                           | The software role as defined by the open enumeration <i>SoftwareRoleEnum</i> .                                                                                                                                                                                                                                      |
| <b>DBServerType</b><br><i>Optional</i>                                                  | The type of database server instance, defined by the open enumeration <i>DBServerTypeEnum</i> .                                                                                                                                                                                                                     |
| <b>WmiAuthId</b><br><i>ADE requires WmiAuthId or ShellAuthID for robot deployment</i>   | Authentication profile ID to use for WMI access. The Discovery Wizard generates and displays this number when you create a WMI authentication profile.                                                                                                                                                              |
| <b>ShellAuthId</b><br><i>ADE requires WmiAuthId or ShellAuthID for robot deployment</i> | Authentication profile ID to use for SSH or telnet access. Authentication profile ID to use for WMI access. The Discovery Wizard generates and displays this number when you create a shell authentication profile.                                                                                                 |
| <b>SnmpAuthId</b><br><i>Optional</i>                                                    | Authentication profile ID to use for WMI access. The Discovery Wizard generates and displays this number when you create an SNMP authentication profile.                                                                                                                                                            |
| <b>AppServerType</b><br><i>Optional</i>                                                 | The type of application server, as defined by the open enumeration <i>AppServerTypeEnum</i> .                                                                                                                                                                                                                       |
| <b>VirtualizationEnvironment</b><br><i>Optional</i>                                     | Value that specifies the virtualization environment (hypervisor manager) of a hypervisor or virtual system. Values are defined in the open enumeration <i>VirtualizationTypeEnum</i> .                                                                                                                              |
| <b>VirtualID</b><br><i>Optional</i>                                                     | Identifier for a VirtualSystem assigned by the virtualization solution (such as VMware or Microsoft Hyper-V).                                                                                                                                                                                                       |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MonitorFrom</b><br><i>Optional</i> | If the device is intended to be remotely monitored, this value specifies the system from which to monitor this device. The value can be an IP address, simple host name, fully qualified domain name, or CA Unified Infrastructure Management address (/UIMDomain/HubName/RobotName). A UIM robot should be installed on the specified system. If the robot is not installed, this device will not be imported. The origin name used by the robot should match the origin specified for this device to ensure that QoS data from probes is correlated with this device. |
| <b>UserAlias</b><br><i>Optional</i>   | The user-defined alias name for a device. Assign an alias name if a device name is long or not intuitive to make it easier to identify.                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## SNMP V1 and V2c Profile Examples and Properties

The following example shows how to create *SnmpV1Profiles* and *SnmpV2Profiles* sections.

```
<SnmpV1Profiles>
 <SnmpV1Profile>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440001</SnmpProfileUUID>
 <Description>SnmpV1Profile</Description>
 <GetCommunityString>public</GetCommunityString>
 </SnmpV1Profile>
</SnmpV1Profiles>
<SnmpV2Profiles>
 <SnmpV2Profile>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440002</SnmpProfileUUID>
 <Description>SnmpV2Profile</Description>
 <GetCommunityString>public</GetCommunityString>
 </SnmpV2Profile>
</SnmpV2Profiles>
```

SNMP V1 and V2 authentication profile import uses the following properties.

| Property                                     | Description                                                                                                                                                                            |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SnmpProfileUUID</b><br><i>Recommended</i> | The universally unique identifier of the authentication profile to use for SNMP access. The specified profile can either be defined in this XML file or have been previously imported. |
| <b>Description</b><br><i>Optional</i>        | Description for the profile.                                                                                                                                                           |
| <b>Port</b><br><i>Optional</i>               | The SNMP port to use. If not specified, port 161 (default) is used.                                                                                                                    |
| <b>GetCommunityString</b><br><i>Required</i> | Community string to be used for <i>Get</i> , <i>GetNext</i> and <i>GetBulk</i> SNMP requests.                                                                                          |

## SNMP V3 Profile Examples and Properties

The following example shows how to create the *SnmpV3Profiles* section.

```
<SnmpV3Profiles>
 <SnmpV3Profile>
 <SnmpProfileUUID>6f0bf0b7-89cf-416c-a4c3-c70ab84d3483</SnmpProfileUUID>
 <Description>SnmpV3Profile NoAuthNoPriv</Description>
 <Port>161</Port>
```

```

 <UserName>NoAuthNoPrivUser</UserName>
 <AuthenticationProtocol>None</AuthenticationProtocol>
 <PrivacyProtocol>None</PrivacyProtocol>
</SnmpV3Profile>
<SnmpV3Profile>
 <SnmpProfileUUID>543af64d-50d0-46b5-a81e-4bef93005259</SnmpProfileUUID>
 <Description>SnmpV3Profile AuthPriv</Description>
 <Port>161</Port>
 <UserName>AuthPrivUser</UserName>
 <AuthenticationProtocol>MD5</AuthenticationProtocol>
 <AuthenticationKey>authKey</AuthenticationKey>
 <PrivacyProtocol>AES</PrivacyProtocol>
 <PrivacyKey>privKey</PrivacyKey>
</SnmpV3Profile>
</SnmpV3Profiles>

```

SNMP V3 authentication profile import uses the following properties.

| Property                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SnmpProfileUUID</b><br><i>Recommended</i>     | The universally unique identifier of the authentication profile to use for SNMP access. The specified profile can either be defined in this XML file or have been previously imported.<br><br>If the UUID is not specified, one is automatically generated for the element. If an existing element is found with a matching UUID, the existing element is updated. Otherwise, a new element is inserted and associated with the UUID. To avoid inserting duplicate records, the same UUID per element should be maintained and used on updates. The XML file saved in the processed directory includes any automatically generated UUIDs for later reuse. |
| <b>Description</b><br><i>Optional</i>            | Description for the profile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Port</b><br><i>Optional</i>                   | The SNMP port to use. If not specified, port 161 (default) is used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>UserName</b><br><i>Required</i>               | SNMP user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>AuthenticationProtocol</b><br><i>Required</i> | Type of authentication used for messages (if any). The values are defined by <i>SnmpV3AuthenticationProtocolEnum</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>AuthenticationKey</b><br><i>Required</i>      | Specific key used by the <i>AuthenticationProtocol</i> for authenticating messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>PrivacyProtocol</b><br><i>Required</i>        | Type of encryption used for messages (if any). The values are defined by <i>SnmpV3PrivacyProtocolEnum</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>PrivacyKey</b><br><i>Required</i>             | Specific key used by the <i>PrivacyProtocol</i> for encrypting and decrypting messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### Example File with Devices and Profiles

Example files are located in `<UIM_install_directory>/probes/service/cm_data_import/schema`.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
 <CmData xmlns="http://nimsoft.com/2014/05/cm-data-import2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

```

```
<Devices>
 <Device>
 <PrimaryIPv4Address>10.10.10.1</PrimaryIPv4Address>
 <Origin>origin</Origin>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440001</SnmpProfileUUID>
 </Device>
 <Device>
 <PrimaryIPv4Address>10.10.10.2</PrimaryIPv4Address>
 <Origin>origin</Origin>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440002</SnmpProfileUUID>
 </Device>
 <Device>
 <PrimaryIPv4Address>10.10.10.3</PrimaryIPv4Address>
 <Origin>origin</Origin>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440003</SnmpProfileUUID>
 </Device>
 <Device>
 <PrimaryIPv4Address>10.10.10.4</PrimaryIPv4Address>
 <Origin>origin</Origin>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440004</SnmpProfileUUID>
 </Device>
 <Device>
 <PrimaryIPv4Address>10.10.10.5</PrimaryIPv4Address>
 <Origin>origin</Origin>
 </Device>
</Devices>
<SnmpV1Profiles>
 <SnmpV1Profile>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440001</SnmpProfileUUID>
 <Description>SnmpV1Profile</Description>
 <GetCommunityString>public</GetCommunityString>
 </SnmpV1Profile>
</SnmpV1Profiles>
<SnmpV2Profiles>
 <SnmpV2Profile>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440002</SnmpProfileUUID>
 <Description>SnmpV2Profile</Description>
 <GetCommunityString>public</GetCommunityString>
 </SnmpV2Profile>
</SnmpV2Profiles>
<SnmpV3Profiles>
 <SnmpV3Profile>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440003</SnmpProfileUUID>
 <Description>SnmpV3Profile NoAuthNoPriv</Description>
 <UserName>NoAuthNoPrivUser</UserName>
 <AuthenticationProtocol>None</AuthenticationProtocol>
 <PrivacyProtocol>None</PrivacyProtocol>
 </SnmpV3Profile>
<SnmpV3Profile>
 <SnmpProfileUUID>550e8400-e29b-41d4-a716-446655440004</SnmpProfileUUID>
 <Description>SnmpV3Profile AuthPriv</Description>
 <UserName>AuthPrivUser</UserName>
 <AuthenticationProtocol>MD5</AuthenticationProtocol>
```

```

 <AuthenticationKey>authKey</AuthenticationKey>
 <PrivacyProtocol>AES</PrivacyProtocol>
 <PrivacyKey>privKey</PrivacyKey>
 </SnmpV3Profile>
</SnmpV3Profiles>
</CmData>

```

## View Discovered Systems

The **Discovery** section allows you to view computers and devices that have been discovered on your network.

The Discovery section contains discovery agents, with network scopes under each discovery agent. The tree also has an Automatic and an External node.

Icons next to the tree nodes help identify the type of node and provide additional information:



- Top-level Discovery node or discovery agent.



- Network scope.



- Automatic. Some probes automatically discover systems, and those systems are displayed under this node.



- External. Systems listed under this node were imported using file-based discovery.



- A discovery is scheduled. Hover over the icon to see the next scheduled time in the tool tip.



- Discovery in progress. The proportion of blue indicates the progress of discovery.



- No discovery scheduled.

Click a node in the tree to view associated systems and their properties in the table to the right. To view properties for all discovered systems, click the **Discovery** node.

A pie chart above the table displays information about discovered systems for the selected node. Choose a different criterion (**Device Type**, **Operating System**, etc.) from the pull-down menu to change the data displayed in the pie chart.

Click a slice in the pie chart or an item in the chart legend to filter for those systems. Only the systems represented in the slice are displayed in the table and reflected in the response links to the right. Click the slice or legend item again to clear the filter.

The response links to the right of the pie chart list systems according to how recently they responded to a request from the discovery agent. Click one of these links, such as **Recent (last day)**, to filter for those systems. Only those systems are displayed in the pie chart and in the table. Click the link again to clear the filter.

### NOTE

Systems that do not respond are eventually purged from the database. By default, 30 days after the last response from a system, the system is deleted from the database.

A Quick Filter field below the response links allows you to filter for text in the **Name**, **IP Address**, **Domain**, **OS Name**, and **Origin** columns of the table.

Click a column header to sort the table by the column.

A key icon



in the table indicates that a discovery agent authenticated with the system using one of the defined authentication profiles. Hover over the key icon to view the type and name of the authentication profile used.

You can export data for a discovery agent or network range scope. The data includes more columns than are displayed in the Inventory table. Data is exported to a .csv file, which is saved in a location that you select. To export data, click a discovery agent or network range scope in the tree, then select **Export Group** from the **Actions** menu.

#### NOTE

When you choose **Export Group**, all systems for the selected discovery agent, or selected network range scope, are exported, regardless of whether you filtered the display in the Inventory view.

## Advanced Configuration

Automated discovery scan settings, such as network ranges and authentication credential profiles, are configured within the Discovery Wizard that runs in the OC. More advanced configuration is completed using the Raw Configure option or Probe Utility in Admin Console or Infrastructure Manager.

- Use the Raw Configure option to configure Discovery Server to run on a robot other than the primary hub and to set memory sizing.
- Use the Probe Utility option to remove master devices.

For information about automated discovery, see the articles on the [Discovery Wizard](#).

### Run discovery\_server on a Child Robot of the Primary Hub

By default, the discovery server runs on the primary hub, the same robot where the data\_engine probe is running. The discovery\_server probe can be run instead on any child robot connected to the primary hub to free up resources (CPU and memory) on the primary hub or to provide dedicated resources to the discovery server to help improve performance. For more information on the discovery process, see the article [Configuring Discovery](#).

#### Install the Discovery Probe

To run the discovery\_server probe on a child robot of the primary hub, install the probe on the child robot.

#### Follow these steps:

1. Deactivate the discovery server on the primary hub: only one instance of the discovery server can be deployed on a system.
2. Install the discovery\_server probe on a child robot.
3. Deactivate the discovery\_server probe on the child robot.
4. If you customized the discovery server configuration on the primary hub, copy the discovery\_server.cfg file from the primary hub to the child robot.
5. Configure the discovery\_server probe to communicate with the data\_engine and udm\_manager probes on the primary hub.  
See the following instructions for configuring the probe with Admin Console or Infrastructure Manager.
6. Configure the wasp probe on the OC robot to communicate with the discovery\_server probe on the child robot.  
See the following general instructions for configuring the wasp probe.
7. If installed, configure the SNMP probe to communicate with the discovery\_server on the child robot.



See the following general instructions for configuring the SNMP probe.

8. Activate the `discovery_server` probe on the child robot.
9. Consider deleting the discovery server on the primary hub to avoid possible confusion in system configuration.

### **Configure data\_engine and udm\_manager Keys in Admin Console**

#### **Follow these steps:**

1. In Admin Console, click on the icon next to the `discovery_server` probe.
2. Select Raw Configure.
3. Set the location of the `data_engine` probe.
  - a. Select the Setup folder in the content window, and click on the Add Key button.
  - b. Enter **data\_engine** in the Add Key dialog and click **Add**.
  - c. In the Raw Configure Key/Value pane, enter the full `data_engine` probe address (*/domain/primary\_hub/primary\_robot/data\_engine*). You can look up the `data_engine` address in Infrastructure Manager under the primary hub's SLM category.
4. Set the location of the `udm_manager` probe.
  - a. Select the Setup folder in the content window and click the Add Section button.
  - b. Enter **udm** in the Add Section dialog and click **Add**.
  - c. Select the `udm` folder in the content window, and click on the Add Key button.
  - d. Enter **udm\_manager** in the Add Key dialog and click **Add**.
  - e. In the Raw Configure Key/Value pane, enter the full `udm_manager` probe address (*/domain/primary\_hub/primary\_robot/udm\_manager*). You can look up the `udm_manager` address in Infrastructure Manager under the primary hub's Service category.
5. Click **Update** to save your changes.
6. Close the dialog box.

### **Configure data\_engine and udm\_manager Keys in Infrastructure Manager**

#### **Follow these steps:**

1. In Infrastructure Manager, shift + right click on the `discovery_server` probe.
2. Select Raw Configure.
3. Set the location of the `data_engine` probe.
  - a. Select the Setup folder in the content window, and click on the New Key button.
  - b. In the New Key dialog enter:
    - Key Name** = `data_engine`
    - Value** = the full `data_engine` probe address (*/domain/primary\_hub/primary\_robot/data\_engine*). You can look up the `data_engine` address in Infrastructure Manager under the primary hub's SLM category.
4. Set the location of the `udm_manager` probe.
  - a. Select the Setup folder and click the Add Section button.
  - b. Enter **udm** in the Add Section dialog and click **Add**.
  - c. Select the setup folder in the content window, and click on the New Key button.
  - d. In the New Key dialog enter:
    - Key Name** = `udm_manager`
    - Value** = the full `udm_manager` probe address (*/domain/primary\_hub/primary\_robot/udm\_manager*). You can look up the `udm_manager` address in Infrastructure Manager under the primary hub's Service category.
5. Click **OK** to close the dialog.
6. Click **Apply** to save your changes.
7. Close the dialog box.

### **Configure the wasp Probe**

Configure the wasp probe on the OC server to connect to the discovery\_server probe in the new configuration.

#### **Follow these steps:**

1. In Admin Console or Infrastructure Manager, navigate to the OC robot, select the wasp probe, and select a configure option.
2. Navigate to the ump\_common section and revise the path for the discovery\_server probe on the child robot.
3. Apply the change, close the probe configuration screen, and restart the wasp probe.

### **Configure the SNMP Probe**

Configure the SNMP probe to connect to the discovery\_server probe in the new configuration.

#### **NOTE**

You can only change the discovery\_server probe address through Admin Console.

#### **Follow these steps:**

1. In Admin Console, navigate to the robot running SNMP, select the probe, and select a configure option.
2. Open the Discovery Filters section and revise the address for the discovery\_server probe on the child robot.
3. Apply the change, close the probe configuration screen, and restart the SNMP probe.

## **Set Maximum Java Heap Size**

The default maximum Java heap size for the discovery\_server and discovery\_agent probes is set using the Raw Configure option.

#### **NOTE**

The recommendations below are general guidelines only. Memory capacity is highly variable dependent upon your Unified Infrastructure Management environment and configuration, and the recommendations below may not be sufficient for your environment.

### **Discovery Server**

The default maximum Java heap size is 1 GB and is intended to support up to 5000 robots. For deployments with more than 5000 robots, we recommend you increase the maximum Java heap size by 1 GB per 5000 robots.

1. Open the discovery\_server probe in Raw Configure:
  - *Admin Console*: click the icon next to the probe and select **Raw Configure**.
  - *Infrastructure Manager*: shift+right-click the probe and select **Raw Configure**.
2. Navigate to **startup > opt**.
3. Enter the desired value for **java\_mem\_max** using increments of 1024 MB:
  - 1 GB = -Xmx1024m
  - 2 GB = -Xmx2048m

### **Discovery Agent**

The default maximum Java heap size is 256 MB. For discovery ranges equivalent to a class B subnet, or in excess of 30,000 addressable devices, we recommend you increase the maximum heap allocation to 512 MB or 1024 MB.

1. Open the discovery\_agent probe in Raw Configure:

- *Admin Console*: click the icon next to the probe and select **Raw Configure**.
  - *Infrastructure Manager*: shift+right-click the probe and select **Raw Configure**.
2. Navigate to **startup > opt**.
  3. Enter the desired value for **java\_mem\_max**:
    - 512 MB = -Xmx512m
    - 1 GB = -Xmx1024m

## Remove Master Devices through Discovery Server

Discovery Server includes two callbacks that allow you to cleanly remove devices from both the UIM and UDM databases. You can remove all master devices or you can remove individual devices by referencing the device `cs_key`.

### WARNING

The callbacks listed in this article are only supported on `discovery_server` v8.11 and later. For `discovery_server` v8.1, there are no methods to manually delete devices. You will need to upgrade to `discovery_server` v8.11 or later to access this functionality. For `discovery_server` 8.0 and earlier, execute a `DELETE FROM CM_COMPUTER_SYSTEM` SQL call.

### Considerations

When you execute the `remove_master_device` callbacks consider the following:

- After you execute the callbacks, if Discovery is performed again, a deleted device will reappear in the inventory. In this case, the device will be assigned a new `cs_key` and treated as a new device.

### NOTE


The command for deleting master devices by CS key includes a parameter for preventing rediscovery. Setting this parameter to `true` excludes the device from the database. The command for deleting all master devices does not contain this option.

- Executing these callbacks will result in different behavior between the UIM database and the UDM database. In the UIM database, the deleted devices are truly deleted. However, in the UDM database, the deleted devices are actually hidden, rather than deleted, to retain device history.

### Remove All Master Devices

Use the Probe Utility to remove all devices from the UIM and UDM databases.

#### Follow these steps:

1. Invoke the Probe Utility for the Discovery Server.
  - a. In Admin Console, click the pull-down menu for the `discovery_server` probe and select **View Probe Utility in New Window** from the list.
  - b. In Infrastructure Manager, select the `discovery_server` probe and press **Ctrl + p**.
2. Select **remove\_all\_master\_devices** from the command list or commandset pull-down menu at the left.
3. Click the green **Execute** button () to send the command request.

### NOTE

The **remove\_all\_master\_devices** callback removes UIM database robot entries for the UIM Server used by OC. The `discovery_server` probe will automatically repopulate deleted robots. If the robots do not reappear in your inventory, refresh OC.

## Remove Master Devices by CS\_Key

You can remove individual master devices by computer system key (cs\_key). To view a list of cs\_key values, see the webservices REST call documentation for [computer system calls](#).


Use the Probe Utility to remove devices by cs\_key from the UIM and UDM databases.

### Follow these steps:

1. Invoke the Probe Utility for the Discovery Server.
  - a. In Admin Console, click the pull-down menu for the discovery\_server probe and select **View Probe Utility in New Window** from the list.
  - b. In Infrastructure Manager, select the discovery\_server probe and press **Ctrl + p**.
2. Select **remove\_master\_devices\_by\_cs\_keys** from the command list or commandset pull-down menu at the left.
3. Insert *true* for the prevent\_rediscovery value to disable rediscovery of the device.

### NOTE


The default value for this parameter is *false*. Accepting the default value will enable rediscovery of a deleted device and assignment of a new cs\_key value.

4. Enter the value for the device cs\_key.
5. Click the green **Execute** button () to send the command request.

## Rediscover Deleted Devices

You can rediscover all deleted devices by executing a command from the probe utility.

### Follow these steps:

1. Invoke the Probe Utility for the Discovery Server.
  - a. In Admin Console, click the pull-down menu for the discovery\_server probe and select **View Probe Utility in New Window** from the list.
  - b. In Infrastructure Manager, select the discovery\_server probe and press **Ctrl + p**.
2. Select **clear\_all\_prevented\_devices** from the command list or commandset pull-down menu at the left.
3. Click the green **Execute** button () to send the command request.

The previously excluded devices will be added back when they are rediscovered. If the probes are still configured to discover or monitor the devices, they will eventually reappear. You can speed this process by forcing the probes to rediscover the devices. Probes have varying ways to force rediscovery. For the discovery agent, you can perform a Discover Now in the Discovery Wizard. For other probes, restarting the probe will typically get them to republish their inventory.

## Set the Probe Transaction Timeout Value

In some cases, Datomic database transactions can time out in the discovery\_server probe. This can occur if there is a heavy load on the system and the probe is processing particularly large graphs and can result in incomplete data appearing in UIM. If the timeout has been exceeded, an error in the log file will read: "Transaction timeout. You may need to increase the transaction timeout setting. Retrying:"

The default for the transaction timeout is 10000 (10 seconds). To avoid the timeout, you can set the timeout to a greater value in the probe configuration file or through the Raw Configure option in a user interface.

### NOTE

The transaction timeout interval can be set for any probe that acts as a Datomic Peer (discovery\_server or wasp). For OC, the Peer is wasp.

**To reset the timeout in the configuration file, follow these steps:**

- Go to the server on which UIM is installed.
- Navigate to the configuration file for the probe and open it in a text editor.
- Scroll to the bottom of the file and look for the following code:

```
<startup>
```

```
<opt>
```

```
java_mem_init = -Xms64m
```

```
java_mem_max = -Xmx1024m
```

```
java_opts = -server -XX:ErrorFile=./hs_err_pid.log
```

```
</opt>
```

```
</startup>
```

- Add the following to the **java\_opts** line: `-Ddatomic.txTimeoutMsec=xxxxx` where "xxxxxx" is the new timeout value. The new `java_opts` line should look similar to this:  
`java_opts = -server -XX:ErrorFile=./hs_err_pid.log -Ddatomic.txTimeoutMsec=15000`
- Save and close the file.

**To reset the timeout in Admin Console, follow these steps:**

- Open Admin Console and navigate to the device running **discovery\_server**.
- Click on the pulldown menu for `discovery_server` and select the **Raw Configure** option.
- Navigate to the **startup/opt** folder.
- Add the following string to the value for the **java\_opts** key: `-Ddatomic.txTimeoutMsec=xxxxx` where "xxxxxx" is the new timeout value. The new `java_opts` value should look similar to this:  
`-server -XX:ErrorFile=./hs_err_pid.log -Ddatomic.txTimeoutMsec=15000`
- Close the **Raw Configure** window.
- Restart the probe.

**Remove Devices in OC**

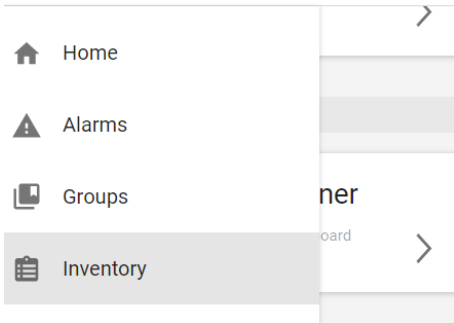
You can remove devices using the OC Inventory view. The process gives you the ability to delete the device from inventory and prevent rediscovery, close alarms associated with the device, and delete stored QoS data for the device.

**NOTE**

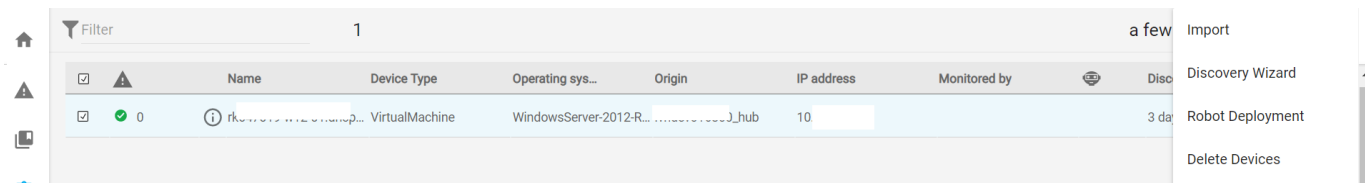
- This functionality is available only to the bus users.
- You can still delete devices through the discovery server probe utility. However, the following method is the preferred method to delete devices.

**Follow these steps:**

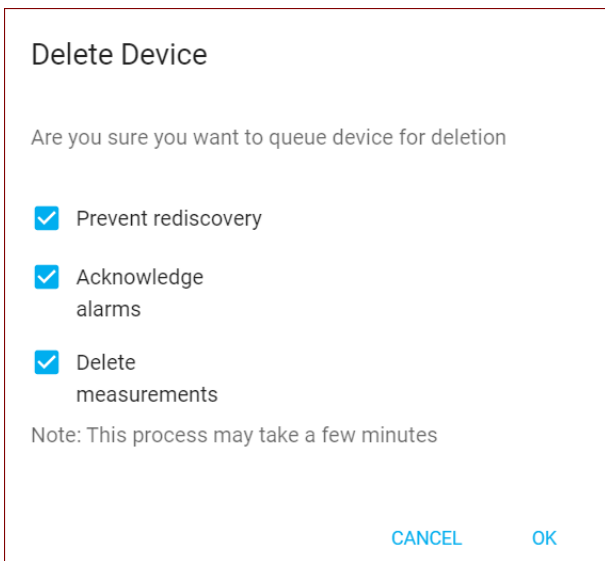
1. Access the OC.
2. Expand the Inventory view.



3. Scroll through the list and select devices by clicking corresponding boxes in the first column. You can also filter the device list using the **Filter** box, which is available above the table. Filtering automatically deselects any device that is not part of the filtered list.
4. Click the **Actions** menu (three dots) at the upper right-hand corner of the table and select the **Delete Devices** option. This option is active only if a device is selected.



A dialog box appears with deletion options related to devices, alarms, and data:



- Prevent rediscovery - Excludes the device instances from being added back into the OC.

**NOTE**

If you do not select the **Prevent rediscovery** option, the devices will be deleted from the OC, but devices still will be monitored by probes and will be rediscovered and re-entered with new cs\_ids. If you do not use the option, you must turn off probe monitoring for the devices to prevent rediscovery. Device deletion does not uninstall robots.

- Acknowledge alarms - Closes all open alarms.

**NOTE**

Closed alarms are moved to the historic alarms table, and historic alarms are aged out of the table according to the configured retention policies. Subsequent alarms for devices will still be displayed in the

global alarms view and must be closed manually. Historic alarms can also be viewed in the global alarms view until they are aged out. To prevent alarms for devices from being generated by probes, configure the probe monitoring the device to exclude the devices.


- Delete measurements - Deletes references to the device QoS data. To prevent the QoS references from being added back, you must disable probe monitoring for the device. After probe monitoring has been disabled, the measurement data will eventually be aged out.
5. Clear unwanted options in the dialog box.
  6. Click **OK**.

### **Allow Rediscovery of Deleted Devices**

You can allow rediscovery of all or selected deleted devices previously removed through the **Prevent Rediscovery** option in removing devices.

To allow rediscovery of all devices, use the command in the Discovery Server probe utility.

#### **Follow these steps:**

1. Invoke the probe utility for the Discovery Server.
  - a. In Admin Console, click the pull-down menu for the `discovery_server` probe and select **View Probe Utility in New Window** from the list.
  - b. In Infrastructure Manager, select the `discovery_server` probe and press **Ctrl + p**.
2. Select **clear\_all\_blacklisted\_devices** from the command list or commandset pull-down menu at the left. This callback unblocks all devices. Similarly, select **unblacklist\_devices** if you want to unblock specific devices. This callback requires `bl_id` as input, which you can get by querying the `cm_blacklist_computer_system` table based on the device name or IP.
3. Click the green **Execute** button () to send the command request.

After completing the steps to allow rediscovery of all or selected deleted devices, the previously excluded devices are added back to the OC when they are rediscovered. If the probes are still configured to discover or monitor the devices, they will eventually reappear in the OC Inventory and any dynamic groups where they previously existed. You can speed this process by forcing the probes to rediscover the devices. Probes have varying ways to force rediscovery: for the discovery agent, you can select **Run discovery now** in the **Schedule** tab of the Discovery Wizard. For other probes, restarting the probe typically will initiate republishing them to inventory.

## **Deploy Robots**

After you have installed the following components:

- The CA UIM database
- The UIM Server
- Any secondary hubs
- Operator Console (OC)

You are ready to deploy robots to the systems you want to monitor. Robots manage the probes that collect monitoring data and perform other functions.

#### **NOTE**

For more information about how to upgrade existing robots to a secure state, see [Secure Hub and Robot](#).

Robots can be installed individually or in bulk. The articles in this section explain the various methods for deploying robots and provide supporting information.

**TIP**

Deploy probes on a robot. Deploy high scale probes on a hub.

You can have many instances of the same probe in a UIM domain, but only one instance of a specific probe per robot.

**To Install a single robot**, you can download the install package from the UIM Server web page to the client system, then execute the install package. You also can install a single robot by manually running one of the native installers.

**To deploy robots in bulk**, you can use one of these methods:

- XML and the `automated_deployment_engine` probe
- XML and OC
- A third-party tool

Note the following items before you begin robot deployment:

- To install robots on remote sites, you can set up tunnels for secure communication.
- Use unique robot names within a UIM domain.

**NOTE**

**More information:**

## Install a Windows Robot

When you install a robot on Windows, you can choose either a **Normal** or **Cloud** installation:

- **Normal** installs a robot on a specific system
- **Cloud** installs a robot onto a master image of a virtual machine (VM) for provisioning purposes. Using this method, you can monitor new VMs as they are deployed. Cloud installation leaves the installed robot in a latent state. The robot starts after a configurable number of host restarts.

**Follow these steps:**

**WARNING**

Robots for Windows systems must be deployed from Hubs running Windows.

1. On the client computer, browse to your UIM Server web page (`http://<UIM_Server_IP_address>:<wasip_port>/uimhome`).
2. In the Infrastructure Deployment (Installers) table, click **Windows Robot**, then select **Run**.
3. Follow the prompts to complete the installation. Note the following items:
  - For **Normal** installation, specify the domain that you want the robot to be part of. Check a domain (if more than one is available), or click **Connect to the network interface through IP address** to attach the robot to a specific hub.
  - For **Cloud** installation, a hub on a cloud instance is assumed. If a hub external to the cloud is used, the robot must be configured with `robotip_alias = <external IP of cloud instance>` after the cloud instance is created.
  - If the computer has multiple network interface cards (NICs), the **Local IP address** dialog appears. Select the network interface the robot uses to send and receive information.
  - In the **Options** dialog:
    - Leave the **First probe port** field blank to assign the first probe to port 48000 (the default) or the first available port after 48000. Alternatively, specify any available port. The port number increments by 1 for each subsequent assignment.
    - Select **Passive mode** if you want the robot to hold its messages until the hub requests them.

**NOTE**

Marketplace probes must be deployed on passive robots.



When the installer exits, installation is complete and the robot is active, which means:

- The robot probes (controller, spooler, and hdb) are installed and running.
- The robot can communicate with its hub.
- You can begin deploying monitoring probes to the robot.

## Install a Unix Robot

The `nimldr` (Nimsoft Loader) utility installs robots and secondary hubs on Linux or Solaris systems.

Installing an individual robot on Linux or Solaris follows the same process as installing a secondary hub on those platforms. The answers that you provide to `nimldr` determine what type of component is deployed.

By default, `nimldr` performs a robot installation. The package files are specific to each supported platform, and include the installation files you need for either infrastructure hub and robot installations, or robot-only installations.

Perform the steps in [Deploy Hubs and Robots on Linux or Solaris Systems](#) on each client system that requires a robot.

## Install an IBM i Robot

The IBM i (previously known as the *IBM AS/400* and *eServer iSeries*) robot is supported on IBM System versions V5r3m0 and up.

### Contents

#### Installing the Robot

This process requires:

- **NIMBUS.SAVF**, which contains the Nimbus library
- **NIMSOF.T.SAVF**, which creates the NimBUS/ directory and files
- A minimum of 35-MB free disk space on the IBM i system

#### Follow these steps.

1. Transfer the SAVF files from the primary hub to the IBM i system:
  - a. Go to the `/install/setup/as400` directory in the UIM Server installation folder (typically `C:\Program Files (x86)\Nimsoft` or `/opt/nimsoft`).  
FTP **NIMBUS.SAVF** and **NIMSOF.T.SAVF** to the **QGPL** library on the IBM i system
  - b. Log in to the IBM i system as a user with `*ALLOBJ` authority (such as `QSECOFR`).
  - c. Verify that the SAVF files were transferred successfully. To see the objects in each SAVF file, execute:
 

```
DSPSAVF FILE(QGPL/NIMBUS)
DSPSAVF FILE(QGPL/NIMSOF.T)
```
2. Create the UIM user profile:
 

```
CRTUSRPRF USRPRF(NIMBUS) PASSWORD(*NONE) USRCLS(*SYSOPR) TEXT('UIM User for UIM
Management') SPCAUT(*JOBCTL *SPLCTL *IOSYSCFG *ALLOBJ) INLMNU(*SIGNOFF) LMTCPB(*YES)
```
3. Restore the SAVF files:
  - a. Restore the NIMBUS library from **NIMBUS.SAVF**:
 

```
RSTLIB SAVLIB(NIMBUS) DEV(*SAVF) SAVF(QGPL/NIMBUS)
```

- b. Create the NimBUS/ directory and restore the file objects from NIMSOFT.SAVF:

```
CRTDIR DIR('/Nimbus_Software')

 CRTDIR DIR('/Nimbus_Software/NimBUS/')

 RST DEV('/QSYS.lib/QGPL.lib/NIMSOFT.file') OBJ('/Nimbus_Software/NimBUS/
*'))
```

4. Edit **robot.cfg** (the robot configuration file):

- a. Open the file:

```
EDTF STMF('/Nimbus_Software/NimBUS/robot/robot.cfg')
```

- b. Edit the following values:

```
<controller>
```

```
domain = my_domain
hub = UIM_host_Ahub
hubrobotname = UIM_host_A
hubip = 111.111.111.111
robotname = IBMi_system
robotip = 222.222.222.222
```

```
</controller>
```

- **domain**: domain of the system
- **hub**: name of the parent hub
- **ubrobotname**: name of the parent hub's robot
- **hubip**: IP address of the parent hub
- **robotname**: desired name for the new robot, or leave blank to the system hostname
- **robotip**: IP address of the IBM i system

5. Start the robot by executing the *Start Subsystem* (STRSBS) command:

```
STRSBS SBS(D/NIMBUS/NIMBUS)
```

Installation is complete.

### Stopping and Restarting the Robot

To stop the robot, execute:

```
ENDSBS SBS(NIMBUS)
```

To restart the robot, execute:

```
STRSBS SBS(D/NIMBUS/NIMBUS)
```

If you shut down the robot each night for backup, manual restarts are required. You can automatically stop and start the robot with the *Add Job Schedule Entry* (ADDJOBSCDE) command. The following example automatically stops the robot at 1 am and starts it again at 7 am every day:

```
ADDJOBSCDE JOB(NIMBUS_END) CMD(ENDSBS SBS(NIMBUS) DELAY(120)) FRQ(*WEEKLY)
SCDDATE(*NONE) SCDDAY(*ALL) SCDTIME(010000) USER(NIMBUS) TEXT('End Nimbus subsystem')
ADDJOBSCDE JOB(NIMBUS_STR) CMD(STRSBS SBS(NIMBUS/NIMBUS)) FRQ(*WEEKLY) SCDDATE(*NONE)
SCDDAY(*ALL) SCDTIME(070000) USER(NIMBUS) TEXT('Start Nimbus subsystem')
```

To change the schedule, use the *Work with Job Schedule Entries* (WRKJOBSCDE) command to edit or delete any entries that you previously created:

## **Uninstalling the Robot**

### **Follow these steps:**

1. Stop the robot:

```
ENDSBS SBS(NIMBUS)
```

2. Wait 30 seconds before continuing to ensure that the subsystem has ended.

3. Delete the NIMBUS library:

```
DLTLIB LIB(NIMBUS)
```

4. Delete the /Nimbus\_Software/NimBUS file tree:

```
RD DIR('/Nimbus_Software') SUBTREE(*ALL)
```

The IBM i robot is uninstalled.

### **NOTE**

You can also delete the NIMBUS user profile with the *Delete User Profile* (DLTUSRPRF) command. If you plan to reinstall the robot, deleting the profile is not required.

## **Bulk Robot Deployment with an XML File**

This article explains how to prepare an XML file to deploy robots in bulk. Once prepared, the XML file can be processed by placing it into the automatic\_deployment\_engine probe folder or by using OC.

### **Contents**

#### **Verify Prerequisites**

Verify the following prerequisites before performing bulk deployment:

- Your Primary Hub is the source system.
- Your UIM Server archive has the required robot installer archive packages:
  - **robot\_exe**
  - **robot\_rpm**
  - **robot\_deb**
  - **robot\_sol**
  - **robot\_aix**
- Your target systems are supported. For supported software versions, see the [Compatibility Matrix](#)

Also ensure that the following requirements are met for your specific operation system:

## Windows

- All appropriate firewall ports and Windows shares must be configured to allow remote WMI and DCOM connections. These ports are open and available on a default Microsoft Server installation.
- Robots for Windows systems must be deployed from Hubs running Windows. The source system and target systems must also be in the same Windows domain, unless the target systems are in the default Windows domain **workgroup**.
- You must have local administrative privileges on the target systems. In addition, the user who is listed in the **host-profiles.xml** for your target Windows systems must have remote access and remote execution privileges. We recommend that this user is an administrator.

## Linux

- The source and target systems must have **/bin/bash**, **ssh** (secure shell), and **glibc**. Most supported Linux distributions include bash and ssh by default; all versions include glibc by default.
- You must have access to *root* or a non-administrative account that supports **sudo** to perform per-command, root-level operations.

## Solaris

If you are using **sudo**, configure your Solaris system to support passwordless requests to CA UIM. To allow passwordless requests, enter the following commands in the **etc/sudoer** file:

### WARNING

Ensure that you are adding the following commands to the **NOPASSWD:** section for your sudo user. Also, ensure that you are using the **visudo** command to edit the **etc/sudoer** file, not a text editor.

- (root) /usr/bin/sh -c /usr/sbin/pkgadd -d /tmp/nimsoft-robot-amd64 -a /tmp/ask < /tmp/input
- (root) /usr/bin/bash /opt/nimsoft/install/RobotConfigurer.sh
- (root) /etc/init.d/nimbus start

## Prepare the XML File for Robot Deployment

Before you begin preparing your XML file, note the following items:

- Advanced users who want to perform extra customization can specify any supported robot parameter.
- **(Linux and Solaris)** The XML field that defines the relative path to the private key on the Hub system at **<rsakeyfile>/relative\_path/to/private\_key\_file</rsakeyfile>**.
- **(Linux and Solaris)** The **sudo\_password** parameter is only required for non-root users with administrative privileges.
- **(Windows)** If the target host is part of a domain, Windows usernames can also specify the domain (**domain \username**).
- To deploy a passive robot, add the following line to the <host> section:  

```
<robot_mode>passive</robot_mode>
```
- If not specified, defaults are used for some required parameters:
  - **name** defaults to the target host name.
  - **IP\_version** defaults to IPv4
  - **Origin** defaults to the parent Hub name

### NOTE

The origin value is attached to all messages created by monitoring probes. MSPs, for example, might want to set origin to a client name.

- **Robot mode** defaults to active

**NOTE**

Users who plan to deploy marketplace probes can specify passive mode, as those probes are required by default to run on passive robots.

**Example XML File**

```

<hosts>
 <host>
 <profile>Windows</profile>
 <arch>32</arch>
 <hostname>customer1</hostname>
 <username>domain\Administrator</username>
 <password>admin_password</password>
 <domain>AutoEnv</domain>
 <hubip>10.10.10.10</hubip>
 <hub>w2k8-x64-Primaryhub</hub>
 <hubrobotname>w2k8-x64-Primary</hubrobotname>
 <hubport>48002</hubport>
 <robotname>w2k8-x86</robotname>
 <tempdir>c:\tmp\supertmp</tempdir>
 </host>

 <host>
 <profile>CentOS</profile>
 <arch>64</arch>
 <hostname>server1</hostname>
 <username>root</username>
 <password>root_password</password>
 <domain>AutoEnv</domain>
 <hubip>101.101.101.101</hubip>
 <hub>w2k8-x64-Primaryhub</hub>
 <hubrobotname>w2k8-x64-Primary</hubrobotname>
 <hubport>48002</hubport>
 <robotname>CentOS6-x64</robotname>
 <tempdir>/opt/tmp</tempdir>
 </host>

 <host>
 <profile>CentOS</profile>
 <arch>64</arch>
 <hostname>server1</hostname>
 <username>username</username>
 <password>user_password</password>
 <sudo_password>sudo_password</sudo_password>

```

```

 <domain>AutoEnv</domain>
 <hubip>101.101.101.101</hubip>
 <hub>w2k8-x64-Primaryhub</hub>
 <hubrobotname>w2k8-x64-Primary</hubrobotname>
 <hubport>48002</hubport>
 <robotname>CentOS6-x64</robotname>
 <tempdir>/opt/tmp</tempdir>
 </host>
</hosts>

```

## Required Attributes

The following table lists all robot attributes that are required when you deploy a robot.

| Attribute           | Description                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>profile</b>      | Operating system on target system: <ul style="list-style-type: none"> <li>• aix</li> <li>• centos</li> <li>• debian</li> <li>• hp-ux</li> <li>• linux (legacy support for previous RPM packages)</li> <li>• opensuse</li> <li>• rhel (Red Hat Enterprise Linux)</li> <li>• solaris</li> <li>• suse (SUSE Linux Enterprise Server)</li> <li>• ubuntu</li> <li>• windows</li> </ul> |
| <b>arch</b>         | Architecture of target system: <ul style="list-style-type: none"> <li>• 32 (32-bit)</li> <li>• 64 (64-bit)</li> <li>• ia64 (HP-UX Itanium)</li> <li>• pa-risc (HP-UX PA-RISC)</li> <li>• ppc64 (AIX 64-bit)</li> <li>• s390x (zLinux)</li> <li>• sparcv9 (Solaris)</li> </ul>                                                                                                     |
| <b>hostname</b>     | Target system hostname or IP address.                                                                                                                                                                                                                                                                                                                                             |
| <b>username</b>     | User name for an account on the target that has administrative permissions or supports sudo for root-level permission.                                                                                                                                                                                                                                                            |
| <b>password</b>     | Account password.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>domain</b>       | Domain to which the robot belongs. Case-sensitive.                                                                                                                                                                                                                                                                                                                                |
| <b>hubip</b>        | IP address of the Hub that manages this robot (referred to as the parent hub).                                                                                                                                                                                                                                                                                                    |
| <b>hub</b>          | Name of the parent Hub.                                                                                                                                                                                                                                                                                                                                                           |
| <b>hubrobotname</b> | Robot name of the parent Hub. Case-sensitive.                                                                                                                                                                                                                                                                                                                                     |
| <b>hubport</b>      | Port that the parent Hub listens on. The default is 48002.                                                                                                                                                                                                                                                                                                                        |

## Optional Attributes

You can specify values for these attributes as needed. This table also shows default values when they exist.

| Optional Attribute   | Description                                                                                                                                                                                                                                                                                                                                                                                               | Default                                                                                                          |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>installdir</b>    | Path to the directory where the robot is installed on the target system.                                                                                                                                                                                                                                                                                                                                  | C:\Program Files\Nimsoft or<br>C:\Program Files (x86)\Nimsoft ( <i>Windows</i> )<br>/opt/nimsoft ( <i>Unix</i> ) |
| <b>robot_mode</b>    | Mode of communication with the Hub: <ul style="list-style-type: none"> <li>Active (default) – Robot sends messages to its parent Hub when it receives them from the probes.</li> <li>Passive – Robot sends data to the Hub at the Hub's request. Limits are placed on the amount of data the robot can send.</li> <li>Offline – Robot does not initiate or expect communications from its Hub.</li> </ul> | Active                                                                                                           |
| <b>robotname</b>     | Unique name to be assigned to the deployed robot.                                                                                                                                                                                                                                                                                                                                                         | Target system hostname                                                                                           |
| <b>rsakeyfile</b>    | Relative path to RSA private key certificate on the system hosting ADE in this format. Key files with pass phrases are not supported.                                                                                                                                                                                                                                                                     | None                                                                                                             |
| <b>sudo_password</b> | Password string for sudo. This password lets you use sudo over ssh during installation. The ssh password is still required. This parameter is not applicable to root users.                                                                                                                                                                                                                               | None                                                                                                             |
| <b>tempdir</b>       | Desired path for a temp directory on the target system. For example, <b>C:\tmp\supertmp</b> ( <i>Windows</i> ) or <b>/opt/tmp</b> ( <i>Unix</i> ).                                                                                                                                                                                                                                                        |                                                                                                                  |
| <b>ip_version</b>    | IP address schema version: <b>IPv4</b> or <b>IPv6</b> .                                                                                                                                                                                                                                                                                                                                                   | IPv4                                                                                                             |
| <b>robotip</b>       | IP address of the robot. The robot communicates on this interface only. This value is propagated to its probes. If no value is specified (default) the robot automatically finds its IP address. If the system has multiple interfaces, it is unpredictable which interface the robot will use.                                                                                                           |                                                                                                                  |
| <b>robotip_alias</b> | Robot IP address in a NAT environment.                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                  |
| <b>tz_offset</b>     | Time zone offset override, in seconds, positive or negative.                                                                                                                                                                                                                                                                                                                                              | 0                                                                                                                |
| <b>autoremove</b>    | Specifies whether the robot should unregister itself from the Hub after it terminates. Value: <b>yes</b> or <b>no</b> .                                                                                                                                                                                                                                                                                   | no                                                                                                               |
| <b>hub_dns_name</b>  | Fully qualified DNS name of the parent Hub. If specified, this value overrides the hubip, which is then used only as a cached value if the DNS lookup fails.                                                                                                                                                                                                                                              |                                                                                                                  |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>hub_update_interval</b>     | Interval, in seconds, at which the controller should send alive or probelist information to the Hub.                                                                                                                                                                                                                                                                                                                                                             | 900                                                                                |
| <b>hubdomain</b>               | Domain of the parent Hub.                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                    |
| <b>secondary_domain</b>        | Domain of the Secondary Hub that manages the robot if its assigned parent Hub is unavailable.                                                                                                                                                                                                                                                                                                                                                                    |                                                                                    |
| <b>secondary_hub</b>           | Hub that manages the robot if its assigned parent hub is unavailable.                                                                                                                                                                                                                                                                                                                                                                                            | None. Robot attaches to the first hub it locates if its own parent is unavailable. |
| <b>secondary_hub_dns_name</b>  | Fully qualified DNS name of the Secondary Hub. If specified, this value overrides the <code>secondary_hubip</code> , which is then used only as a cached value if the DNS lookup fails.                                                                                                                                                                                                                                                                          |                                                                                    |
| <b>secondary_hubip</b>         | IP address of the Secondary Hub. Overridden if the DNS name is specified.                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                    |
| <b>secondary_hubport</b>       | Hub port of the secondary Hub.                                                                                                                                                                                                                                                                                                                                                                                                                                   | 48002                                                                              |
| <b>secondary_hubrobotname</b>  | Name of the secondary Hub's robot.                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                    |
| <b>secondary_robotip_alias</b> | The NAT addresses the robot uses when connected to the secondary Hub. Valid values are: <ul style="list-style-type: none"> <li>• <b>same</b>, which uses the parent hub NAT address (default)</li> <li>• <b>IP address</b></li> </ul>                                                                                                                                                                                                                            | same                                                                               |
| <b>send_alive</b>              | Whether or not to send alive messages to the Hub. Values: <ul style="list-style-type: none"> <li>• <b>1</b> – Send at each hubupdate interval</li> <li>• <b>0</b> – Do not send alive messages (useful if the robot runs in an offline mode and you want to establish contact between the robot and Hub only when needed)</li> <li>• <b>-1</b> – Send the complete probe list; use with very old Hubs that do not understand the alive message format</li> </ul> | 1                                                                                  |
| <b>do_not_broadcast</b>        | Prevent the robot from broadcasting to locate any Hub. By default, a robot that is not attached to a Hub will broadcast to locate a temporary Hub. Value: <b>yes</b> or <b>no</b>                                                                                                                                                                                                                                                                                | no                                                                                 |
| <b>temporary_hub_broadcast</b> | Prevent the robot from broadcasting to locate a temporary Hub if its parent Hub and secondary Hub are not available. This causes the robot spools its messages until its parent or Secondary Hub is available. By default, a robot that is not attached to a Hub will broadcast to locate a temporary Hub. Value: <b>yes</b> or <b>no</b> .                                                                                                                      | no                                                                                 |



|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                |                 |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>unmanaged_security</b>       | Specifies which Hubs the robot can broadcast to in order to establish contact.<br>Values: <ul style="list-style-type: none"> <li>• <b>not_locked</b>, <b>none</b>, or <b>open</b> – any Hub</li> <li>• <b>domain_locked</b> or <b>domain</b> – only to Hubs in the robot's domain</li> <li>• <b>hub_locked</b> or <b>hub</b> – no broadcast is allowed; controller can only contact its parent Hub.</li> </ul> | domain_locked   |
| <b>controller_port</b>          | Port assigned to the controller probe.                                                                                                                                                                                                                                                                                                                                                                         | 48000           |
| <b>first_probe_port</b>         | First port assigned to a probe by the controller. Ports are assigned to subsequent probes in sequence. Use this option if you want the probes to have port numbers in a specific range for router or firewall purposes.                                                                                                                                                                                        | 48000           |
| <b>port_alive_check</b>         | Interval, in seconds, for port alive checking.                                                                                                                                                                                                                                                                                                                                                                 | 330             |
| <b>port_alive_include_local</b> | Specifies whether to include ports that are registered from local probes when performing the port check. Value: <b>yes</b> or <b>no</b> .                                                                                                                                                                                                                                                                      | yes             |
| <b>spooler_port</b>             | Port that is assigned to the spooler probe.                                                                                                                                                                                                                                                                                                                                                                    | 48001           |
| <b>logfile</b>                  | Name for the log file.                                                                                                                                                                                                                                                                                                                                                                                         | controller.log  |
| <b>loglevel</b>                 | Logging level for messages from the robot.<br>Values: <b>0</b> through <b>8</b> .                                                                                                                                                                                                                                                                                                                              | 0               |
| <b>logsize</b>                  | Maximum size, in kilobytes, for the controller.log file.                                                                                                                                                                                                                                                                                                                                                       | 100             |
| <b>proxy_log</b>                | Logging level for proxy functions in the controller.log file. Typically set from 1 to 5.<br>Values: 0 through 8.                                                                                                                                                                                                                                                                                               | 4               |
| <b>origin</b>                   | Origin for messages that identifies the source of the message. Typically used to partition data in a multi-tenant environment.<br>Value: any string. Typically a Hub or robot name.                                                                                                                                                                                                                            | Parent Hub name |
| <b>os_user1</b>                 | Tag added by the controller when sending internal messages directly to the Hub and by the spooler when any message is spooled.                                                                                                                                                                                                                                                                                 |                 |
| <b>os_user2</b>                 | Tag added by the controller when sending internal messages directly to the Hub and by the spooler when any message is spooled.                                                                                                                                                                                                                                                                                 |                 |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                               |      |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| <b>capture_output</b>           | Creates pipes for each started probe to capture any output they send to stdout or stderr. This output is appended to the probe's log file. Value: <b>yes</b> or <b>no</b> .<br>Enabling this functionality introduces extra overhead in the probe. On Windows systems, the probes must inherit resources from the controller. In some situations this might prevent the controller from terminating properly. | no   |
| <b>default_fail_window</b>      | Number of seconds a probe must run before its restart counter is reset. This setting applies to all probes managed by the robot. This value can be overridden for a particular probe by specifying a <i>fail_window</i> in that probe's configuration.                                                                                                                                                        | 15   |
| <b>default_priority_level</b>   | Numeric value that specifies the priority level for all probes that do not have this value set at the probe level. Probes with lower priority levels are started first, with a delay between each priority level.<br>Note that the <i>start_after</i> probe property gives you more control over the start order of probes.                                                                                   | None |
| <b>max_restarts</b>             | Number of starts allowed before a probe is set to the error state. The restart counter is reset for a probe if it runs longer than its <i>fail_window</i> .                                                                                                                                                                                                                                                   |      |
| <b>proxy_mode</b>               | Allows the controller to act as a proxy for probes. When on, all callback functions to the probes are performed through the controller port. Value: <b>0</b> (off) or <b>1</b> (on)                                                                                                                                                                                                                           | 0    |
| <b>suspend_on_loopback_only</b> | Suspend all probes if loopback is the only network. Windows only. Values: <ul style="list-style-type: none"> <li>• <b>yes</b> – robot enters a "sleep" mode where all probes are suspended until a network connection is available</li> <li>• <b>no</b> – alarm messages are spooled, then flushed when a network connection is again available</li> </ul>                                                    | yes  |
| <b>set_qos_source</b>           | Specifies whether probes use the robot name as the QoS source instead of the host name. Not supported for all probes. Value: <b>yes</b> or <b>no</b> .                                                                                                                                                                                                                                                        | no   |
| <b>system_uptime_qos</b>        | Specifies whether to send asynchronous QoS when the robot is up or down. Value: <b>yes</b> or <b>no</b> .                                                                                                                                                                                                                                                                                                     | no   |

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>alarm_level_comfail_restart</b> | <p>The alarm severity that is sent after the fourth unsuccessful attempt to communicate with a probe that has a registered port. Controller restarts the probe after alarm is sent. Values:</p> <ul style="list-style-type: none"> <li>• <b>no alarm</b></li> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul>                                                                                                          | no alarm |
| <b>alarm_level_dispatch_error</b>  | <p>Severity level for an internal alarm indicating a socket system failure. Alarm is sent only if the log level is greater than 0. Values:</p> <ul style="list-style-type: none"> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul>                                                                                                                                                                                      | major    |
| <b>alarm_level_max_restarts</b>    | <p>Severity level for the alarm that is sent when a probe is restarted and quickly terminates 10 times. Values:</p> <ul style="list-style-type: none"> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul>                                                                                                                                                                                                                 | major    |
| <b>alarm_level_postinstall</b>     | <p>Severity level for the alarm that is sent when there is an error during probe distribution. This error occurs when the controller is unable to start a post-install script after distributing a package distribution, or if the post-install script does not return an "okay" (0) status. Values:</p> <ul style="list-style-type: none"> <li>• <b>no alarm</b></li> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul> | no alarm |

|                                       |                                                                                                                                                                                                                                                                                                                                                                             |          |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>alarm_level_request_error</b>      | Severity level for the alarm that is sent when the controller is unable to issue a request to distsrv. Values: <ul style="list-style-type: none"> <li>• <b>no alarm</b></li> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul>                             | major    |
| <b>alarm_level_start_error</b>        | Severity level for an alarm that is sent when unable to start a probe. Values: <ul style="list-style-type: none"> <li>• <b>no alarm</b></li> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul>                                                             | major    |
| <b>alarm_level_suspended</b>          | Severity level for an alarm that is sent when a probe start is aborted because the robot state is suspended. Values: <ul style="list-style-type: none"> <li>• <b>no alarm</b></li> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul>                       | no alarm |
| <b>alarm_level_timed_error_return</b> | Severity level for an alarm that is sent when a probe start is aborted because the robot state is suspended. Values: <ul style="list-style-type: none"> <li>• <b>no alarm</b></li> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul>                       | warning  |
| <b>alarm_level_timed_not_finished</b> | Severity level for an alarm that is sent when a timed probe is not completed at the next scheduled start time. The timed probe is restarted when this occurs. Values: <ul style="list-style-type: none"> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul> | warning  |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                      |       |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| <b>alarm_level_unregister</b> | Severity level for an alarm that is sent when a probe unregisters its port but does not terminate. Values: <ul style="list-style-type: none"> <li>• <b>clear</b></li> <li>• <b>informational</b></li> <li>• <b>warning</b></li> <li>• <b>minor</b></li> <li>• <b>major</b></li> <li>• <b>critical</b></li> </ul>                                                                                                     | major |
| <b>alarm_timeout</b>          | Interval, in minutes, at which alarms for probes in the error state are repeated.                                                                                                                                                                                                                                                                                                                                    |       |
| <b>wait_after_unregister</b>  | Wait time, in seconds, after a probe unregisters a port. If the process is still running, the unregister alarm is issued and the probe is set to the error state.                                                                                                                                                                                                                                                    |       |
| <b>audit</b>                  | When and where to send audit messages. Values: <ul style="list-style-type: none"> <li>• <b>post</b> – Send audit message on controller events</li> <li>• <b>yes</b> – Log controller events to local file</li> <li>• <b>post_detail</b> – Send audit event on controller events and configuration file changes</li> <li>• <b>file_detail</b> – Log controller events and file change events to local file</li> </ul> |       |
| <b>audit_checkpoint_count</b> | Number of versions of configuration files to retain.                                                                                                                                                                                                                                                                                                                                                                 |       |
| <b>audit_max_config_size</b>  | Maximum size, in bytes, of the configuration file for content comparison.                                                                                                                                                                                                                                                                                                                                            |       |
| <b>config_locking</b>         | Signals the configuration tools that they should acquire a lock at startup and should relinquish it on termination. Value: <b>yes</b> or <b>no</b> .                                                                                                                                                                                                                                                                 | no    |
| <b>config_lock_timeout</b>    | Timeout, in seconds, for the configuration file lock.                                                                                                                                                                                                                                                                                                                                                                | 360   |
| <b>startup_timeout</b>        | If the robot is a Hub robot, specifies how long (in seconds) the controller waits for the Hub probe to start before starting other probes. If the timeout is reached, the robot does a failover.                                                                                                                                                                                                                     |       |

### Deploy the XML File

To deploy robots using OC, refer to the topic [Deploy Robots in OC](#).

To deploy robots using automated\_deployment engine, copy the host-profiles.xml file into the automated\_deployment\_engine probe directory. By default this directory is:

- **Windows** — C:\Program Files (x86)\Nimsoft\probes\service\automated\_deployment\_engine
- **Linux, Solaris, AIX, and HP-UX** — /opt/nimsoft/probes/service/automated\_deployment\_engine

Once host-profiles.xml is updated, deployment begins automatically. After processing host-profiles.xml, automated\_deployment\_engine renames it **host-profiles-YYYY-MM-DD\_HH-mm-ss** to reflect the date and time of

deployment. Renaming the file also ensures that if the `automated_deployment_engine` probe restarts, deployment does not automatically restart.

### **Deployment Notes**

- The `automated_deployment_engine` probe cannot deploy robots from an unchanged `host-profiles.xml` file. To restart a distribution, remove the date and time from the file name and change the file size by a nominal amount (for example, edit the file and add an extra line). Deployment begins within 30 seconds of the change.
- After a robot is deployed, the scan waits for the robot to start before reporting its status in the history tab. The default wait time is set to 100 seconds. During this 100-second period, the `automated_deployment_engine` polls the robot every 25 seconds. If the robot does not respond within 100 seconds, the Hub declares the robot to be inactive.

#### **TIP**

The delay time is controlled by the `verifyDelay` key in the `automated_deployment_engine` configuration file (`automated_deployment_engine.cfg`). Changing this value also changes the polling interval, which is always 1/4 of the delay time.

- You can view the `automated_deployment_engine` log file (`automated_deployment_engine.log`) for more information regarding robot deployment activity.

#### **TIP**

You can use the `tail` command on Unix-like systems to view the end of the text file.

- The `automated_deployment_engine` probe installs robots in groups. The number of CPU cores on the Hub where the scan is running determines the group size.
- If you are using **ADE REST 1.30** calls and your passwords are encrypted, include the following line in the authentication portion of the REST XML:
 

```
"nimcrypt" , "true"
```
- If you deploy more than one instance of the `automated_deployment_engine` probe or specify a secondary Hub under **hubname**, tasks are executed in this order:
  - a. The primary instance of the `automated_deployment_engine` probe runs its deployment.
  - b. The primary `automated_deployment_engine` probe deploys any secondary instances.
  - c. The secondary probe instances execute their robot deployment tasks.

## **Deploy Robots in OC**

CA UIM administrators can use OC to deploy robots automatically to a group of systems or to an individual system. The Administration in the Settings View of the Operator Console lets you select systems to deploy robots to, or you can import an XML file of systems.

### **Deployment Considerations**

The OC deployment feature targets the default (C: drive) installation location. To specify a different location, use XML deployment so that an alternate `install_dir` can be specified.

You cannot use Operator Console (OC) to automatically deploy robots to zLinux systems that were placed in your inventory through automated discovery. To deploy robots to zLinux systems, use one of the following methods:

- Run the native installer manually or with a third-party tool. See [Deploy Robots in Bulk with a Third-Party Tool and Native Installers](#).
- Deploy Robots in bulk with an XML file. See [Bulk Robot Deployment with an XML File](#).

Robots can only be deployed to systems that have known credentials. Credential information is specified in the Discovery Wizard, and you can use Linux/Unix or WMI authentication profiles. However, robots cannot be automatically deployed to systems discovered with SNMP authentication profiles. With the file-based import option, credentials are specified in an

XML file, and not in the Discovery Wizard. For more information about using an XML file for bulk robot deployment, see the topic [Bulk Robot Deployment with an XML File](#).

In cases, for instance, where primary and secondary hubs are connected through a firewall, it may be easier to deploy robots automatically from a secondary hub. This avoids having to open port 22, the default port, on the primary hub for deployment.

#### Follow these steps:

1. Deploy the `automated_deployment_engine` to the secondary hub, where port 22 is not blocked.
2. Login to Infrastructure Manager directly from the secondary hub (not the primary hub, as is usual).
3. Drag and drop the robot packages to be deployed into the archive on the secondary hub.
4. Deploy the robots from the secondary hub using XML files as discussed in [Bulk Robot Deployment with an XML File](#).

You can also configure a custom SSH port and select the version of the robot package to deploy. Add a new section with the updated information to the `automated_deployment_engine` configuration.

#### Follow these steps:

1. In Infrastructure Management or Admin Console, navigate to the robot running the `automated_deployment_engine` and select the probe.
2. In Infrastructure Management, select the Configure or Raw Configure option to add a new section. In Admin Console, select the Raw Configure option to add a new section.
3. At the Root level, create a section with the name *deployment*.
4. Open the deployment section and create the following key/value pairs:
  - `sshport` - <port number>
  - `robot_pkg_version` - <version number>
5. Close the configuration window.

### Deploy Robots

You must have the **OC Automatic Robot Installation** ACL permission to deploy robots automatically. Account contact users cannot deploy robots automatically. Also, the `automated_deployment_engine` probe version 1.10 or later must be running in your environment.

Administrators can also use either the GUI or the command-line interface for the `automated_deployment_engine` probe to deploy robots automatically.

For a list of platforms that support automatic robot deployment, see the [Compatibility Matrix](#).

To deploy robots automatically you must be a regular UIM user, and you must have the **OC Automatic Robot Installation** permission set in the ACL. Also, the `automated_deployment_engine` probe version 1.10 or later must be running in your environment.

OC uses the `automated_deployment_engine` probe to perform an ssh file transfer to a target. Typical deployment is performed through the primary hub.

#### Follow these steps:

1. Navigate Inventory view in the left navigation of the OC.
2. In the Inventory view, select systems to deploy robots to. You can select the check box in the column header to select all the systems in the list.
3. Choose **Robot Deployment** from the **Actions** menu.
4. Click **Deploy**.

## Deploy Robots in Bulk with a Third-Party Tool and Native Installers

### WARNING

CA UIM does not support the use of native installers to perform robot upgrades. To upgrade your robots, you must use the **robot\_update** package that is available in either the Admin Console or Infrastructure Manager Archive.

For first-time robot installations, the native robot installers are still supported.

If you already have a software deployment tool (such as *Yum* or *Altiris*), you can use it to deploy robots. Almost any third-party distribution mechanism can be used as long as it can:

1. Copy a native robot installer to a remote system. 32-bit and 64-bit installers for Windows, Linux, Ubuntu, Debian, Solaris, and AIX are available on your primary hub. See the [Support Compatibility Matrix](#) for details on supported versions.
2. Copy an answer file that you have prepared. The native robot installers execute silently using the robot configuration values in the answer file. This file must follow the correct syntax and format.
3. Execute the steps for the appropriate installer.

### NOTE

You can install a single robot with an answer file.

1. Copy the answer file and the appropriate installer to the target system.
2. Manually execute the installation steps on the target system.

### Preparing an Answer File

Your answer file must be a text file in the following syntax and format. Supply actual values for each parameter. Do not include spaces between the parameter and value. For example, **domain=Mydomain** .

Name the answer file **nms-robot-vars.cfg**.

*domain=UIM\_domain\_to\_which\_the\_robot\_will\_belong*

*hub=name\_of\_parent\_hub*

*hubip=parent\_hub\_IP\_address*

*hubrobotname=parent\_hub\_local\_robot*

*hubport=parent\_hub\_port\_number*

*(optional fields)*

Note the following information:



- The **domain**, **hub**, **hubip**, **hubrobotname**, and **hubport** are required.
- Optional parameters with no answer are valid. However, it is better to omit a parameter from the answer file than to include it with an empty value.
- The default port for a hub is 48002.
- We recommend preparing a simple answer file with only required fields during initial robot deployment. You can add optional fields later. Make bulk changes to the robot configuration using drag-and-drop in Infrastructure Manager.
- Any robot attribute can be configured in the answer file with the format **parameter=value** . For a complete list of robot parameters, see [Bulk Robot Deployment with an XML File](#).

| Parameter                          | Definition                                           | Example        |
|------------------------------------|------------------------------------------------------|----------------|
| <b>domain</b>                      | UIM domain                                           | HOST_ABC_DOM   |
| <b>hub</b>                         | Name of the parent hub of the robot                  | HOST_ABC_HUB   |
| <b>hubip</b>                       | Hostname or IP address of the robot parent hub       | 10.0.0.10      |
| <b>hubrobotname</b>                | Name of the parent hub robot                         | HOST_ABC_ROBOT |
| <b>hubport</b>                     | Hub listening port                                   | 48002          |
| <b>robotip</b> (optional)          | IP address of the target system                      | 10.0.0.11      |
| <b>robotname</b> (optional)        | Desired name for the robot. Default, <i>hostname</i> | HOST_MNO       |
| <b>first_probe_port</b> (optional) | Port that is used by the first probe                 | 48000          |
| <b>origin</b> (optional)           | Desired origin value                                 | HUBNAME        |

## Deploying to Windows

Your third-party deployment tool must perform the following actions.

1. Copy the appropriate Windows installer to any folder on the target system:
  - **nimsoft-robot-x64.exe** (*64-bit*)
  - **nimsoft-robot.exe** (*32-bit*)
2. Copy the **nms-robot-vars.cfg** answer file to the same folder.
3. Install the robot by executing:
 

```
<EXE_package>.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART
```

The default install folder is **C:\Program Files (x86)\Nimsoft** for 32-bit systems, and **C:\Program Files\Nimsoft** for 64-bit systems. To specify the folder, append the following parameter to the command. Quotation marks are required.

```
/DIR="c:\path\to\install"
```

To specify the log file, append:

```
/LOG="name_of_install_log.txt"
```

After installation, the robot starts automatically.

## Deploying to Linux

Use your third-party deployment tool to perform the following actions.

**Note:** If you are not using root access, use either **sudo <command>** or **su -c "<command>"**. You can also use **su** to get a root shell and execute the command.

1. Copy the appropriate Linux installer to **/opt** on the target system:

- **nimsoft-robot-x64.rpm** 64-bit SUSE, SLES, or RHEL
  - **nimsoft-robot.rpm** 32-bit SUSE, SLES, or RHEL
  - **nimsoft-robot+debian\_amd64.deb** 64-bit Debian
  - **nimsoft-robot+debian\_i386.deb** 32-bit Debian
  - **nimsoft-robot+ubuntu\_amd64.deb** 64-bit Ubuntu (supports Ubuntu 14 and 16)
  - **nimsoft-robot+ubuntu\_i386.deb** 32-bit Ubuntu
2. Copy the **nms-robot-vars.cfg** answer file to **/opt**.
  3. Install the robot.
    - On Red Hat, SUSE, or CentOS, execute the following command, where *<arch>* is **i386** or **amd64**:  
`rpm -ivh nimsoft-robot.<arch>.rpm`  
 The default install directory is **/opt/nimsoft**. To specify the installation directory, execute the following command, where *<directory>* is the full path:  
`rpm -ivh nimsoft-robot.<arch>.rpm --prefix=<directory>`  
 The rpm flags function as follows:
      - **-i** install the software package.
      - **-v** display a simple status line to show what is being installed (*verbose* mode).
      - **-h** display fifty hash marks (#) to show the status as the install proceeds; when all fifty have displayed, installation is complete.
    - On Debian or Ubuntu, execute the following command using **sudo**, **su -c**, or as the root user. Specify *<OS>* as **debian** or **ubuntu**, and specify *<arch>* as **i386** or **amd64**.  
`dpkg -i nimsoft-robot+<OS>_<arch>.deb`
  4. Execute the **RobotConfigurer.sh** script to configure the robot when the installer exits.  
`cd /opt/nimsoft/install`  
`bash RobotConfigurer.sh`
  5. **Perform these steps only if your controller version is 7.91 or earlier:**
    - a. This step is not required for Ubuntu 14. For Ubuntu 16, execute **/opt/nimsoft/install/service-ctrl.sh enable** to enable the robot service.
    - b. The installation is complete. To start the robot, use one of the following commands:
      - For Red Hat, SUSE, CentOS, or Debian:  
`/etc/init.d/nimbus start`
      - For Ubuntu:  
`/opt/nimsoft/bin/niminit start`
  6. **Perform this step only if your controller version is 7.93 or later.** The installation is complete. To start the robot, use the following command for all platforms:  
`/opt/nimsoft/bin/niminit start`

## **Deploying to HP-UX**

Use your third-party deployment tool to perform the following actions.

1. Copy the appropriate installer to the **/opt** directory on the target system.
  - For HP-UX on PA RISC: **nimsoft-robot-hppa-11.31.depot.gz**
  - For HP-UX on Itanium: **nimsoft-robot-ia64-11.31.depot.gz**
1. Copy the **nms-robot-vars.cfg** answer file to **/opt**.
2. Extract the **.gz** file. Execute the following command, where *<arch>* is **hppa** or **ia64**:  
`/usr/contrib/bin/gunzip /opt/nimsoft-robot-<arch>-11.31.depot.gz`
3. Execute the following command to install the robot.  
`/usr/sbin/swinstall -s /opt/nimsoft-robot-<arch>-11.31.depot \*`

- Execute the **RobotConfigurer.sh** script to configure the robot when the installer exits.

```
cd /opt/nimsoft/install
/bin/sh RobotConfigurer.sh
```

- The installation is complete. To start the robot, use the following command.

```
/opt/nimsoft/bin/niminit start
```

To stop the robot or view the status, **ssh** to the system, and execute the **niminit** command.

```
/opt/nimsoft/bin/niminit stop
/opt/nimsoft/bin/niminit status
```

## Deploying to Solaris

**Note:** Beginning with robot version 7.95, if you create a new Solaris zone, a robot installed in the global zone is not automatically deployed to the new zone. To install a robot in a new, non-global zone, install the robot into the non-global zone using the same steps that you use to install the robot in the global zone.

Use your third-party deployment tool to perform the following actions.

**Note:** If you are not using root access, use either **sudo <command>** or **su -c "<command>"**. You can also use **su** to get a root shell and execute the command.

- Copy the appropriate Solaris installer to the **/opt** directory on the target system.
  - For Solaris 32-bit: **nimsoft-robot-i386.gz**
  - For Solaris 64-bit: **nimsoft-robot-amd64.gz**
  - For Solaris SPARC: **nimsoft-robot-sparcv9.gz**
- Copy the **nms-robot-vars.cfg** answer file to **/opt**.
- Execute the following commands to extract and install the robot. Replace **<arch>** with **i386**, **amd64**, or **sparcv9**.
 

```
gunzip -c nimsoft-robot-<arch>.gz
pkgadd -d /opt/nimsoft-robot-<arch>
```
- When the installer completes, execute the **RobotConfigurer.sh** script to configure the robot.
 

```
cd /opt/nimsoft/install
bash RobotConfigurer.sh
```

Installation is complete. To view status of the robot, ssh to the server, and execute:

```
ps -ef | grep nimbus
```

## Deploying to AIX

The AIX robot is supported on 64-bit systems only. To determine whether the target kernel is 32-bit or 64-bit, execute:

```
getconf KERNEL_BITMODE
```

Use your third-party deployment tool to perform the following actions.

- Copy the AIX installer to the target system:
 

```
nimsoft-robot.aix6.1.ppc64.rpm
```
- Copy the **nms-robot-vars.cfg** answer file to **/opt**.
- Execute the following command as the root user to install the robot to the default directory, **/opt/nimsoft**:
 

```
rpm -ivh nimsoft-robot.aix6.1.ppc64.rpm
```

To install the robot to a specific directory, execute the following command as root, where **<directory>** is the full path:

```
rpm -ivh nimsoft-robot.aix6.1.ppc64.rpm --prefix=<directory>
```

The rpm flags function as follows:

  - i** install the software package

- v display a simple status line to show what is being installed (*verbose* mode)
  - h display fifty hash marks (#) to show the status as the install proceeds; when all fifty have displayed, installation is complete
4. To run the robot as a non-root user account, take the following steps:
    - Add the non-root user to **/etc/nimbus.conf**:
 

```
echo "NIMBUS_USR=<NonRootUser>" >> /etc/nimbus.conf
```

 Change the ownership of the **/etc/nimbus.conf** file, and the UIM installation to the non-root user:
 

```
chown <NonRootUser> /etc/nimbus.conf
chown -R <NonRootUser> /UIMHOME
```
  5. Run the **RobotConfigurer.sh** script as root to configure the robot:
 

```
cd /opt/nimsoft/install
sh RobotConfigurer.sh
```
  6. Enable the Nimbus service as root:
 

```
/opt/nimsoft/install/service-ctrl.sh enable
```
  7. Start the robot as root. If the robot is configured to run as a non-root account, the processes are running as the non-root user.
 

```
/usr/bin/startsrc -s nimbus
```

Installation is complete. To stop the robot or view the status, execute:

```
/usr/bin/stopsrc -s
```

```
nimbus/usr/bin/lssrc -s nimbus
```

## Install Multiple Robots on a Single Host

Some situations are best addressed by installing multiple robots on a single host. For load balancing, you can install an additional robot on a single host to run a specific probe: for example, the `discovery_server` probe. For performance reasons, you can install the Operator Console (OC) on a child robot of the primary hub when monitoring small networks. For load reasons, you can use multiple robots on a server to run more than one instance of a single probe: for example, if your SNMP devices are only reachable from a specific server and you need to run more than one `snmpcollector` probe, you can install multiple robots on the same server for the same probe.

You can use the following information to install multiple robots on one server.

### Install Multiple Robots on a Windows Host

1. Install the first robot on the Windows host using the *Normal* install method described in [Install a Windows Robot](#).
2. Stop the Windows service `NimbusWatcherService` in Windows Services, or from a command prompt with `net stop NimbusWatcherService`
3. Open a command prompt window and change directories to the robot installation bin directory. Default, `C:\Program Files (x86)\Nimsoft\bin`. Use the `nimbus` command to remove the `NimbusWatcherService` from Windows services. For example,
 

```
cd c:\Program Files (x86)\Nimsoft\bin
nimbus.exe -servicename "NimbusWatcherService" -remove
```
4. Locate the `niscache` directory under the robot installation directory, and delete all the files in the `niscache` directory.
5. Locate the `robot` directory under the robot installation directory. Copy the file `controller.cfg` to the `robot\changes` directory.
6. Edit the file `robot\changes\controller.cfg` you copied to the `changes` directory in Step 5, and delete all the lines beginning with `magic_key`. Save the file back to the `changes` directory.

7. Copy the robot installation directory and all subdirectories to a new location. For example, `C:\Program Files (x86)\Nimsoft2`
8. In the new location, open the file `robot\robot.cfg` with a text editor.
9. Assign the robot a unique name and a unique port number for this host.  
By default, robots are configured to use `controller_port 48000`. The robot `spooler_port` and `first_probe_port` are relative to the robot `controller_port`.  
One robot on the server can use the default ports, but extra robots require unique ports.  
For example,
 

```
robotname = nimsoft2
controller_port = 50000
spooler_port = 50001
first_probe_port = 50005
```
10. Create a `NimbusWatcherService` for the new robot. This service starts when Windows is started. Each watcher service requires a unique name.
  - a. Go to the `bin` directory of the new robot.
  - b. Execute the `nimbus` command from the `bin` directory of the new robot to install a unique watcher service for this robot.
 

```
nimbus.exe -servicename "NimbusWatcherService2" -install
```
11. To create more robots on the host, repeat Steps 7- 10. Provide a unique robot name, a unique watcher service name, and unique port numbers for each robot. For example, increment the next robot to use `controller_port 51000`, and increment the `spooler_port` and `first_probe_port` relative to 51000.
12. When Windows is restarted, the new robot watcher services start. You can also start and stop the services manually in Windows Services.

### **Install Multiple Robots on a Linux Host**

1. Install the first robot on the Linux system using the procedure described in [Install a Unix Robot](#).
2. Stop the robot from a command prompt with the command `/opt/nimsoft/bin/niminit stop`.
3. Locate the `niscache` directory under the robot installation directory, and delete all the files in the `niscache` directory.
4. Locate the `robot` directory under the robot installation directory. Copy the file `controller.cfg` to the `robot\changes` directory.
5. Edit the file `robot\changes\controller.cfg` you copied to the `changes` directory in Step 4, and delete all the lines beginning with `magic_key`. Save the file back to the `changes` directory.
6. Copy the robot installation directory and all subdirectories to a new location. For example, `/opt/nimsoft2`

```
cp -dpr /opt/nimsoft /opt/nimsoft2
```
7. In the new location, open the file `robot/robot.cfg` with a text editor.
8. Assign the robot a unique name and a unique port number number for this host.  
By default, robots are configured to use `controller_port 48000`. The robot `spooler_port` and `first_probe_port` are relative to the robot `controller_port`.  
One robot on the server can use the default ports, but extra robots require unique ports.  
For example,
 

```
robotname = nimsoft2
controller_port = 50000
spooler_port = 50001
first_probe_port = 50005
```
9. Change to the `/etc/init.d` directory
 

```
cd /etc/init.d
```

10. Copy the `nimbus` file to `nimbus2`  

```
cp nimbus nimbus2
```
11. Open the file `nimbus2` with a text editor  
 Replace all occurrences of `/opt/nimsoft` with `/opt/nimsoft2`  
 Change the line `touch /var/lock/subsys/nimbus` to say `touch /var/lock/subsys/nimbus2`  
 Save the file.
12. To create more robots on the host, repeat Steps 6 - 11. Provide a unique robot name, a unique service name, and unique port numbers for each robot. For example, increment the next robot to use `controller_port 51000`, and increment the `spooler_port` and `first_probe_port` relative to 51000.
13. When Linux is restarted, the new robot processes start. You can also start and stop the services manually. For example, `/opt/nimsoft/bin/niminit start | stop`

## Optional Post-Installation Tasks

Once you have completed setting up your CA UIM environment, you can customize your CA UIM environment to meet the needs of your business.

### Configure Admin Console to Use a Proxy Server

If necessary, you can configure Admin Console to use a proxy server.

#### NOTE

If you require secure access for Admin Console, you must configure its associated wasp probe to use HTTPS. For more information, see the topic [Configure HTTPS in Admin Console or OC](#).

#### Follow these steps:

1. Deploy the webgtw probe if it is not already deployed.
2. Open the wasp probe running Admin Console in Raw Configure.
3. Navigate to `webapps/adminconsole/custom/uncrypted`.
4. Edit the `webgtw_address` as follows:  

```
{domain}/{hub}/{robot}/webgtw
```
5. Restart the wasp probe.

### Configure Email Address Login to OC

This article describes how to configure OC for email address login.

#### NOTE

OC does not currently support the mixed use of screen name and email address authentication.

#### Follow these steps:

1. Deactivate the wasp probe.
2. Open the following file for editing: `<UIM_Installation>\probes\service\wasp\conf\config.properties`.
3. Change the value of the parameter `company.security.auth.type=screenName` to `company.security.auth.type=emailAddress`.
4. Remove all instances of the `screenName` parameter from the `portalpreferences` table in the NimsoftSLM database:
  - a. Run the following query:
 

```
select * from portalpreferences where preferences like '%screenName%'
```

If no rows in the `preferences` column contain the `screenName` parameter, go to step 5.

- b. Issue the following command to delete all rows that contain `screenName` from the table:

```
delete from portalpreferences where preferences like '%screenName%'
```

5. Reactivate the wasp probe.

## Configure HTTPS in Admin Console or OC (Self-Signed Certificate)

This article describes how to configure a Secure Sockets Layer (SSL) connection to access Operator Console or Admin Console using HTTPS. It provides instructions for setting up a self-signed certificate.

### Contents

We recommend that you consult your network security engineers and compliance specialists regarding your specific security requirements. In general, industry-standard security requirements mandate the use of SSL encryption for client/server communications on an untrusted network. This includes the following situations:

- If users access Operator Console or Admin Console using a public network, such as the Internet
- If sessions traverse an unsecured part of your network, such as wireless networks in meeting rooms or in public-access areas
- If sessions traverse mobile networks

#### NOTE

For high-security environments, we recommend using at least 2048-bit encryption. However, using longer RSA keys significantly affects the speed of encryption and decryption.

### Prerequisites

Verify the following prerequisites before continuing:

- You are an administrative user with access to Infrastructure Manager.
- Your environment is configured to run `keytool` commands if you plan to use a certificate other than a 1024-bit self-signed certificate. This means that the `$PATH` system variable includes a path to `java.exe` and `keytool`.
- Due to the security polices on some operating systems, you might have to run the `keytool` commands as an administrator.

#### WARNING

If running the `keytool` commands gives unexpected results on Windows systems, use the **Run as Administrator** option.

### HTTPS Redirect and Admin Console

Admin Console does not support the use of an HTTPS redirect. You must access Admin Console directly using the **HTTPS://** URL. You can also disable the HTTP port for Admin Console.

You can also change your wasp configuration using Admin Console. However, you are automatically logged out of Admin Console when wasp restarts.

#### Follow these steps:

1. Use Remote Desktop to connect to the UIM or OC server.
2. Open Infrastructure Manager.
3. Navigate to the robot running the wasp probe.
4. Press the Ctrl key as you right-click the wasp probe, and then select **Raw Configure**.
5. With the **setup** section highlighted, select the **http\_port** key, and click **Delete Key**.

## **Implement Self-Signed SSL Certificate**

This section provides instructions for configuring Operator Console to use a self-signed SSL certificate. This section includes separate procedures for 1024-bit and 2048-bit self-signed SSL certificates:

- [Upgrade Pre-Existing Self-Signed Certificates to Java 1.8](#)
- [Implement a 1024-Bit Self-Signed SSL Certificate](#)
- [Implement a 2048-Bit Self-Signed SSL Certificate](#)

## **Upgrade Pre-Existing Self-Signed Certificates to Java 1.8**

The Java version was updated to Java 1.8 starting with CA UIM version 8.5.1. You must upgrade any self-signed certificates generated by CA UIM from previous CA UIM versions. If you do not upgrade the pre-existing certificates, HTTPS connections to Admin Console or OC will not work due to the change in security encryption levels in Java 1.8.

### **Follow these steps:**

1. Repeat the following steps for each instance of wasp that you configured for HTTPS.
2. On the robot with wasp, navigate to the wasp.keystore file in `<nimsoft_home>\probes\service\wasp\conf\wasp.keystore`.
3. Delete the wasp.keystore file.
4. Restart wasp on the robot. The wasp.keystore file is regenerated according to the SHA256 algorithm standard.
5. Verify that you can reestablish browser connectivity to the system. Accept any prompts to accept the new self-signed certificate in your browser.

## **Implement a 1024-Bit Self-Signed SSL Certificate**

This section provides instructions for configuring Operator Console to use a 1024-bit self-signed SSL certificate:

1. [Modify wasp to Use HTTPS](#)
2. [\(Optional\) Change the HTTPS Ciphers](#)
3. [Test the HTTPS Connection](#)
4. [\(OC Only\) Set Automatic HTTP to HTTPS Redirect](#)

## **Modify wasp to Use HTTPS**

### **NOTE**

If you are configuring HTTPS for OC, modify the wasp probe on the OC server. If you are configuring HTTPS for Admin Console, modify the wasp probe on the UIM server.

Regardless of the certificate you want to implement, the first required step is to modify the wasp.cfg file to enable HTTPS. When this change takes effect, the following actions occur:

- The wasp.keystore file, an encrypted file that stores certificates, is generated in the directory `<OC or UIM server installation>/UIM/probes/service/wasp/conf`
- A 1024-bit self-signed certificate is automatically generated in wasp.keystore

### **Follow these steps:**

1. Use Remote Desktop to connect to the UIM or OC server.
2. Open Infrastructure Manager.
3. Navigate to the robot running the wasp probe.
4. Press the Ctrl key as you right-click the wasp probe, and then select **Raw Configure**.
5. With the **setup** section highlighted, locate the **https\_port** key, and click **Edit Key** to specify a port. If necessary, click **New Key** and enter **https\_port**.



**NOTE**

The maximum port value that you can set is 65535.

6. Edit the **https\_max\_threads** key to configure the number of concurrent https requests. The default value is 500.
7. Restart the wasp probe.  
After the wasp probe restarts, wasp is configured to use an HTTPS connection, and the wasp.keystore file is generated. This file is located in **<nimsoft\_home>\probes\service\wasp\conf\wasp.keystore**.

**(Optional) Change the HTTPS Ciphers**

If necessary, you can customize the list of ciphers that are used by the wasp probe.

**Follow these steps:**

1. Navigate to the system where wasp is installed.
2. Navigate to the **wasp.cfg** file located in the following location:  
**<OC or UIM server\_installation>\Nimsoft\probes\service\wasp\wasp.cfg**
3. Open the **wasp.cfg** file in a text editor.
4. Locate the **https\_ciphers** key. By default, the https\_ciphers key lists several values.
5. Change the **https\_ciphers** key to use the desired ciphers. Refer to the [SSL documentation](#) for a list of available cypher suites.
6. Restart the wasp probe.

**Test the HTTPS Connection****NOTE**

Self-signed certificates can cause some browser errors or notifications, such as "Your connection is not private" or "The identity of this website has not been verified." These are normal messages and can be prevented by importing the certificate to the browser (though not all browsers allow this). To avoid these messages altogether, you must use a certificate from a certificate authority.

**Follow these steps:**

1. Open a supported Web browser.
2. Enter **https://<Operator Console or AdminConsole or hostname>:<port>** followed by the URL for OC or Admin Console.

The login page appears if wasp configuration was successfully modified to use HTTPS.

**NOTE**

You can click the lock icon to the left of the URL in the browser address window to view information about the connection.

**(Operator Console Only) Set Automatic HTTP to HTTPS Redirect**

You can set the automatic HTTP to HTTPS redirect by following this procedure.

**Follow these steps:**

1. Search for the **WEB-INF/web.xml** files in the **<OC or UIM server\_installation>/Nimsoft/probes/service/wasp/webapps/** folder, and open the files for editing.
2. Locate the following content:
 

```
<security-constraint>
 <web-resource-collection>
 <web-resource-name>un restricted methods</web-resource-name>
```

```

 <url-pattern>*/</url-pattern>
 </web-resource-collection>
 <user-data-constraint>
 <transport-guarantee>NONE</transport-guarantee>
 </user-data-constraint>
</security-constraint>

```

3. Replace `<transport-guarantee>NONE</transport-guarantee>` with `<transport-guarantee>CONFIDENTIAL</transport-guarantee>` .
4. Save the web.xml files.
5. Open the following file for editing:
 

```
<OC or UIM server_Installation>\Nimsoft\probes\service\wasp\wasp.cfg
```
6. Add the following lines before `</setup>` :
 

```
<http_connector> redirectPort=<desired port></http_connector>
```

 where `<desired port>` matches the `https_port` key defined in the Modify wasp to Use HTTPS subsection .

#### NOTE

Ensure that you include the redirect code within the `<setup>` section.

7. Save the wasp.cfg file.
8. Restart the wasp probe.

#### NOTE

Dual mode (that is, both HTTP and HTTPS) is not allowed. Administrators can configure HTTP-only, HTTPS-only, or HTTP to HTTPS redirect.

### **Implement a 2048-Bit Self-Signed SSL Certificate**

This section provides instructions for configuring Operator Console to use a 2048-bit self-signed SSL certificate:

1. [Download OpenSSL for Windows](#)
2. [Modify wasp to Use HTTPS](#)
3. [\(Optional\) Change the HTTPS Ciphers](#)
4. [Reinitialize wasp.keystore](#)
5. [Generate a Public and Private Key Pair](#)
6. [Export the Private Key](#)
7. [Generate and Import the Certificate](#)
8. [Test the HTTPS Connection](#)
9. [Record Certificate Information](#)
10. [\(OC Only\) Set Automatic HTTP to HTTPS Redirect](#)

### **Download OpenSSL for Windows**

To begin the process, you must have a copy of OpenSSL on the system.

Follow these steps:

1. Use Remote Desktop to connect to the system server.

#### NOTE

If you are configuring SSL for OC, modify the wasp probe on the OC server. If you are configuring SSL for Admin Console, modify the wasp probe on the UIM server.

2. Download the executable <http://downloads.sourceforge.net/gnuwin32/openssl-0.9.8h-1-setup.exe>.
3. Run the executable to install the package.

## **Modify wasp to Use HTTPS**

### **NOTE**

If you are configuring HTTPS for Operator Console, modify the wasp probe on the OC server. If you are configuring HTTPS for Admin Console, modify the wasp probe on the UIM server.

Regardless of the certificate you want to implement, the first required step is to modify the wasp.cfg file to enable HTTPS. When this change takes effect, the following occurs:

- The wasp.keystore file, an encrypted file that stores certificates, is generated in the directory **<OC or UIM server installation>/UIM/probes/service/wasp/conf**
- A 1024-bit self-signed certificate is automatically generated in wasp.keystore

You must replace the automatically generated 1024-bit self-signed certificate with the certificate that you want to use.

### **Follow these steps:**

1. Use Remote Desktop to connect to the UIM server.
2. Open Infrastructure Manager.
3. Navigate to the server running the wasp probe.
4. Press the Ctrl key as you right-click the wasp probe, and then select **Raw Configure**.
5. With the **setup** section highlighted, locate the **https\_port** key, and click **Edit Key** to specify a port. If necessary, click **New Key** and enter **https\_port**.

### **NOTE**

The maximum port value that you can set is 65535.

6. Edit the **https\_max\_threads** key to configure the number of concurrent https requests. The default value is 500. After the wasp probe restarts, wasp is configured to use an HTTPS connection, and the wasp.keystore file is generated. This file is located in <nimsoft\_home>\probes\service\wasp\conf\wasp.keystore.

## **(Optional) Change the HTTPS Ciphers**

If necessary, you can customize the list of ciphers that are used by the wasp probe.

### **Follow these steps:**

1. Navigate to the system where wasp is installed.
2. Navigate to the **wasp.cfg** file located in the following location:  
**<OC or UIM server\_Installation>\Nimsoft\probes\service\wasp\wasp.cfg**
3. Open the **wasp.cfg** file in a text editor.
4. Locate the **https\_ciphers** key. By default, the https\_ciphers key lists several values.
5. Change the https\_ciphers key to use the desired ciphers. Refer to the [SSL documentation](#) for a list of available cypher suites.
6. Restart the wasp probe.

## **Reinitialize wasp.keystore**

The wasp probe is an embedded web server running as a probe. Modifying the wasp probe to use HTTPS creates the wasp.keystore file. To use SSL, you must regenerate this file. To regenerate the file, you must:

1. Locate and delete the existing file from the fileset.
2. Run a probe utility command to reinitialize the file.

### **WARNING**

Only perform the following steps if you are NOT using a 1024-bit self-signed certificate, and *at least one of the following statements is true*:

- You do not know the password of wasp.keystore.
- This is the *first time that you are* configuring OC to use HTTPS.

You must configure the associated wasp probes for Admin Console and OC servers to fully configure HTTPS.

#### NOTE

If you are running the UIM and OC servers on the same system, there is only wasp probe that must be configured to enable HTTPS on both Admin Console and Operator Console.

In addition, you must enter a valid password for wasp.keystore. However, wasp.keystore has a *hard-coded, unknown* password. Therefore, the first time you configure wasp for HTTPS, it is recommended that you execute the `ssl_reinitialize_keystore` callback and set a new password.

The `ssl_reinitialize_keystore` callback re-creates wasp.keystore and its password hash. When you run this callback, enter a new password as an argument, and then *securely store the new password for future use*. If you lose or forget this password, the only way to reset it is to reinitialize wasp.keystore again.

#### WARNING

Use caution with the `ssl_reinitialize_keystore` callback. This callback changes the encryption hash of wasp.keystore, and will *invalidate any certificates you are currently using*. For this reason, it is strongly recommended that you back up individual key and certificate files, so that if you have to reinitialize the keystore, you can reload the keys and certificates into the new keystore.


In addition, do not use the keytool utility to change the password of wasp.keystore, as wasp will not recognize the new password. Currently, the only way to change the password of wasp.keystore is to use the `ssl_reinitialize_keystore` callback.

#### Follow these steps:

1. Use Remote Desktop to connect to the appropriate server.
2. Open Infrastructure Manager.
3. Navigate to the robot running the wasp probe.
4. Open the actions menu for the probe and select 'Deactivate'.
5. In the fileset, navigate to `/Nimsoft/probes/service/wasp/conf` and delete the file `wasp.keystore`.
6. In Infrastructure Manager, open the actions menu and select 'Restart'.
7. In Infrastructure Manager, click on the wasp probe to highlight it.
8. Press **Ctrl+<P>** to open the probe utility.
9. In the drop-down list under **Probe commandset**, select **ssl\_reinitialize\_keystore**.
10. Enter a new password as an argument.

#### NOTE

Use a password that is at least six characters long. The wasp probe utility will not prevent you from using a shorter password, but you will be unable to make changes to the wasp.keystore file as described later.

11. Click the green Execute button () to run the callback. The **Command** status bar displays the text **OK**.
12. Securely record the password that you set for future use.

#### Generate a Public and Private Key Pair

To generate a new certificate, you must delete the existing 1024-bit certificate, create a public and private key pair, and create a new certificate. Enter keytool commands at a command prompt in the same directory as the wasp.keystore file, typically `<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf`. The keytool utility is located in the directory where the JRE resides, typically `<OC or UIM server_installation>/jre/<jre_version>/bin/keytool`.

**Follow these steps:**

1. Open an administrator command prompt on the server running wasp and navigate to the wasp configuration directory.
2. Set the JAVA\_HOME environment variables as follows:  
`<OC or UIM server_installation>/jre/<jre_version>/bin/`
3. Verify that you have a valid password for the wasp.keystore file:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf>keytool -list -keystore wasp.keystore`  
 You will receive a confirmation message, 'Your keystore contains 1 entry.'
4. Delete the current 1024-bit certificate:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> keytool -delete -alias wasp -keystore wasp.keystore`
5. Verify that the key was deleted:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf>keytool -list -keystore wasp.keystore`  
 You will receive a confirmation message, 'Your keystore contains 0 entries.'
6. Generate the public and private key pair with the key size you require. The valid period is set in calendar days: for example, 365 represents one calendar year.  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> keytool -genkeypair -alias wasp -keyalg RSA -keysize 2048 -keystore wasp.keystore -validity <days_cert_is_valid>`
7. When prompted for your first and last name, enter the FQDN.
  - a. When prompted, provide entries for the following fields:
    - Organizational unit
    - Organization
    - City or Locality
    - State or Province
    - Two-letter country code
 You are prompted to confirm that the information you entered is correct.  
 Generate a certificate signing request for the certificate:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> keytool -certreq -alias wasp -validity 365 -keystore wasp.keystore -file wasp.csr`

**Export the Private Key**

Next, export the private key from the keystore so that you can use it to generate a self-signed certificate. You will need to enter the keystore password which you noted in a previous step in the appropriate fields.

**Follow these steps:**

1. Create a file called wasp.keystore.p12 in the wasp/conf folder:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> keytool -importkeystore -srckeystore wasp.keystore -srcstorepass (keystore password) -srckeypass (keystore password) -destkeystore wasp.keystore.p12 -deststoretype PKCS12 -srcalias wasp -deststorepass (keystore password) -destkeypass (keystore password)`
2. Set the environment path variable to "C:\Program Files (x86)\GnuWin32\bin".
3. Set the environment variable OPENSSL\_CONF to "C:\Program Files (x86)\GnuWin32\share\openssl.cnf".
4. Open a new command window to get the new values.
5. Export the private key from this .p12 file to create a wasp.key file in the wasp/conf folder:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> openssl pkcs12 -in wasp.keystore.p12 -passin pass:(keystore password) -nocerts -out wasp.key -passout pass:(keystore password)`

## **Generate and Import the Certificate**

Generate the certificate with the key created in the previous steps.

### **Follow these steps:**

1. Create a wasp.cer file in the wasp/conf folder, which is the certificate:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> openssl req -x509 -sha256 -days 365 -key wasp.key -in wasp.csr -out wasp.cer`
2. Change the location for the command and import the certificate:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> keytool -import -trustcacerts -alias wasp -file wasp.cer -keystore wasp.keystore`

## **Test the HTTPS Connection**

### **NOTE**

Self-signed certificates can cause some browser errors or notifications, such as "Your connection is not private" or "The identity of this website has not been verified." These are normal messages and can be prevented by importing the certificate to the browser (though not all browsers allow this). To avoid these messages altogether, you must use a certificate from a certificate authority.

### **Follow these steps:**

1. Open a supported Web browser.
2. Enter https:// followed by the URL for OC or Admin Console.

The login page appears if wasp configuration was successfully modified to use HTTPS.

### **NOTE**

You can click the lock icon to the left of the URL in the browser address window to view information about the connection.

## **Record Certificate Information**

### **Follow these steps:**

1. Securely record the new password that you set for the wasp.keystore file.
2. Ensure that you record the validity period you set for the certificate.
3. Back up the certificate files to a secure location.

## **(OC Only) Set Automatic HTTP to HTTPS Redirect**

### **Follow these steps:**

1. Open the following file for editing:  
**<OC\_installation>/Nimsoft/probes/service/wasp/conf/config.properties.**
2. Add the following line at the bottom of the file:  
`web.server.protocol=https`
3. Save the config.properties file.
4. Open the following file for editing:  
`<OC or UIM server_installation>/Nimsoft/probes/service/wasp/webapps/ROOT/WEB-INF/web.xml.`
5. Add the following lines before `</web-app>`:  

```
<security-constraint>
 <web-resource-collection>
 <web-resource-name>Entire Application</web-resource-name>
 <url-pattern>/*</url-pattern>
```

```

</web-resource-collection>
<user-data-constraint>
 <transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>

```

6. Save the web.xml file.
7. Open the following file for editing:  
**<OC or UIM server\_Installation>\Nimsoft\probes\service\wasp\wasp.cfg**
8. Add the following lines before </setup>:

```

<http_connector>
 redirectPort=<desired port>
</http_connector>

```

where <desired port> matches the https\_port key defined in the subsection *Modify wasp Configuration to Use HTTPS*.

#### NOTE

Be sure to include the redirect code within the <setup> section.

9. Save the wasp.cfg file.
10. Restart the wasp probe.

### Set/Enable Secure Flag for Cookie

You can set/enable a secure flag for cookies in Admin Console and OC:

- [Set/Enable Secure Flag for Cookie in Admin Console](#)
- [Set/Enable Secure Flag for Cookie in Operator Console](#)

### Set/Enable Secure Flag for Cookie in Admin Console

For setting/enabling the secure flag for the cookie in Admin Console.

#### Follow these steps:

1. Open the following file for editing:  
<UIM server\_installation>/Nimsoft/probes/service/wasp/webapps/adminconsoleapp/WEB-INF/web.xml.

2. Uncomment the < secure> Tag
 

```

<session-config>
 <session-timeout>1</session-timeout>
 <cookie-config>
 <http-only>true</http-only>
 <!--<secure>true</secure>-->
 </cookie-config>
</session-config>

```

### Set/Enable Secure Flag for Cookie in Operator Console

For setting/enabling the secure flag for the cookie in Operator Console.

#### Follow these steps:

1. Open the following file for editing:  
<OC>/Nimsoft/probes/service/wasp/webapps/ROOT/WEB-INF/web.xml.
2. Uncomment the < secure> Tag
 

```

<session-config>

```

```
<session-timeout>1</session-timeout>
 <cookie-config>
 <http-only>true</http-only>
 <!--<secure>true</secure>-->
 </cookie-config>
</session-config>
```

### **Update Expect-CT Header Values**

You can update Expect-CT-Header values in Admin Console and OC:

- [Update Expect-CT Header Values in Admin Console](#)
- [Update Expect-CT Header Values in Operator Console](#)

### **Update Expect-CT Header Values in Admin Console**

By default Expect-CT is set to “enforce, max-age=300”, to change the values or adding report-uri.

#### **Follow these steps:**

1. Navigate to the **wasp.cfg** file located in the following location:  
**<UIM server\_Installation>\Nimsoft\probes\service\wasp\wasp.cfg**
2. Open the **wasp.cfg** file in a text editor.
3. In the webapps\adminconsole section, add/edit configuration attributes in Expect-CT-Header property as below  
Expect-CT-Header = enforce, max-age=300
4. Restart the wasp.

### **Update Expect-CT Header Values in Operator Console**

By default Expect-CT is set to “enforce, max-age=300”, to change the values or adding report-uri in the Operator Console.

#### **Follow these steps:**

1. Navigate to the **wasp.cfg** file located in the following location:  
**<OC server\_Installation>\Nimsoft\probes\service\wasp\wasp.cfg**
2. Open the **wasp.cfg** file in a text editor.
3. In the webapps\operatorconsole\_portlet\custom\unencrypted section, add/edit configuration attributes in Expect-CT-Header property as below  
Expect-CT-Header = enforce, max-age=300
4. Restart the wasp.

### **(Optional) Access CABI Server**

Additional configuration is required if you are using the CABI for UIM dashboards. For more information, see the (Optional) Access CABI Server with HTTPS section in [CA Business Intelligence with CA UIM](#).

#### **NOTE**

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.



## Configure HTTPS in Admin Console or OC (Authority-Signed Certificate)

This article describes how to configure a Secure Sockets Layer (SSL) connection to access Operator Console or Admin Console using HTTPS. It provides instructions for setting up an authority-signed certificate.

### Contents

We recommend that you consult your network security engineers and compliance specialists regarding your specific security requirements. In general, industry-standard security requirements mandate the use of SSL encryption for client/server communications on an untrusted network. This includes the following situations:

- If users access Operator Console or Admin Console using a public network, such as the Internet
- If sessions traverse an unsecured part of your network, such as wireless networks in meeting rooms or in public-access areas
- If sessions traverse mobile networks

#### NOTE

For high-security environments, we recommend using at least 2048-bit encryption. However, using longer RSA keys significantly affects the speed of encryption and decryption.

### Prerequisites

Verify the following prerequisites before continuing:

- You are an administrative user with access to Infrastructure Manager.
- Your environment is configured to run keytool commands if you plan to use a certificate other than a 1024-bit self-signed certificate. This means that the \$PATH system variable includes a path to java.exe and keytool.
- Due to the security policies on some operating systems, you might have to run the keytool commands as an administrator.

#### WARNING

If running the keytool commands gives unexpected results on Windows systems, use the **Run as Administrator** option.

### HTTPS Redirect and Admin Console

Admin Console does not support the use of an HTTPS redirect. You must access Admin Console directly using the **HTTPS://** URL. You can also disable the HTTP port for Admin Console.

You can also change your wasp configuration using Admin Console. However, you are automatically logged out of Admin Console when wasp restarts.

#### Follow these steps:

1. Use Remote Desktop to connect to the UIM or OC server.
2. Open Infrastructure Manager.
3. Navigate to the robot running the wasp probe.
4. Press the Ctrl key as you right-click the wasp probe, and then select **Raw Configure**.
5. With the **setup** section highlighted, select the **http\_port** key, and click **Delete Key**.

### Implement an Authority-Signed SSL Certificate

This section includes information about how to implement an authority-signed SSL certificate:

1. [Entity, Intermediate, and Root Certificates](#)
2. [Modify wasp to Use HTTPS](#)

3. (Optional) Change the HTTPS Ciphers
4. Reinitialize wasp.keystore
5. Generate a Public and Private Key Pair
6. Record Certificate Information
7. Generate and Submit a CSR
8. Import the Certificates
9. Test the HTTPS Connection
10. (Operator Console Only) Set Automatic HTTP to HTTPS Redirect

### **Entity, Intermediate, and Root Certificates**

A number of certificate authorities issue intermediate, or *chained* certificates. If your certificate authority issues chained certificates, you will typically receive the following certificate files:

- An *entity* certificate
- One or more *intermediate* certificates
- A root certificate might be included

You must upload the entity certificate and any intermediate certificates your certificate authority provides. You might not need to upload a root certificate. This is because the UIM installation automatically installs a Java Runtime Environment (JRE) that includes the root certificates of many certificate authorities. However, your certificate authority may provide a new root certificate and advise that you upload it.

You can view the root certificates installed automatically with the JRE during the UIM installation.

#### **Follow these steps:**

1. Open an administrator command prompt on the server running OC.
2. Change directories as follows:  
`cd <OC or UIM server_installation>/jre/<jre_version>/lib/security`
3. Issue the following command:  
`<OC or UIM server_installation>/jre/<jre_version>/bin/keytool keytool -list -keystore cacerts`  
 The system prompts you to enter the keystore password. After you enter a valid password, the system displays the default root certificates in the cacerts file.

### **Modify wasp to Use HTTPS**

#### **NOTE**

If you are configuring HTTPS for Operator Console, modify the wasp probe on the OC server. If you are configuring HTTPS for Admin Console, modify the wasp probe on the UIM server.

Regardless of the certificate you want to implement, the first required step is to modify the wasp.cfg file to enable HTTPS. When this change takes effect, the following occurs:

- The wasp.keystore file, an encrypted file that stores certificates, is generated in the directory **<OC or UIM server installation>/UIM/probes/service/wasp/conf**
- A 1024-bit self-signed certificate is automatically generated in wasp.keystore

You must replace the automatically generated 1024-bit self-signed certificate with the certificate that you want to use.

#### **Follow these steps:**

1. Use Remote Desktop to connect to the UIM server.
2. Open Infrastructure Manager.
3. Navigate to the server running the wasp probe.
4. Press the Ctrl key as you right-click the wasp probe, and then select **Raw Configure**.

- With the **setup** section highlighted, locate the **https\_port** key, and click **Edit Key** to specify a port. If necessary, click **New Key** and enter **https\_port**.

#### NOTE

The maximum port value you can set is 65535.

- Edit the **https\_max\_threads** key to configure the number of concurrent https requests. The default value is 500. After the wasp probe restarts, wasp is configured to use an HTTPS connection, and the wasp.keystore file is generated. This file is located in <nimsoft\_home>\probes\service\wasp\conf\wasp.keystore.

### **(Optional) Change the HTTPS Ciphers**

If necessary, you can customize the list of ciphers that are used by the wasp probe.

#### **Follow these steps:**

- Navigate to the system where wasp is installed.
- Navigate to the **wasp.cfg** file located in the following location:  
**<OC or UIM server\_Installation>\Nimsoft\probes\service\wasp\wasp.cfg**
- Open the **wasp.cfg** file in a text editor.
- Locate the **https\_ciphers** key. By default, the https\_ciphers key lists several values.
- Change the https\_ciphers key to use the desired ciphers. Refer to the [SSL documentation](#) for a list of available cypher suites.
- Restart the wasp probe.

### **Reinitialize wasp.keystore**

#### **WARNING**

Only perform the following steps if you are not using a 1024-bit self-signed certificate, and *at least one of the following statements is true*:

- You do not know the password of wasp.keystore.
- This is the *first time that you are* configuring Operator Console to use HTTPS.

If neither of the above statements is true, review the section Wasp and the ssl\_reinitialize\_keystore Callback before continuing.

You must configure the associated wasp probes for Admin Console and Operator Console to fully configure HTTPS. The wasp probe is an embedded web server running as a probe.

#### **NOTE**

If you are running the UIM and OC servers on the same system, there is only wasp probe that must be configured to enable HTTPS on both Admin Console and Operator Console.

In addition, you must enter a valid password for wasp.keystore. However, wasp.keystore has a *hard-coded, unknown* password. Therefore, the first time you configure wasp for HTTPS, it is recommended that you execute the *ssl\_reinitialize\_keystore* callback and set a new password.

The *ssl\_reinitialize\_keystore* callback re-creates wasp.keystore and its password hash. When you run this callback, enter a new password as an argument, and then *securely store the new password for future use*. If you lose or forget this password, the only way to reset it is to reinitialize wasp.keystore again.

#### **WARNING**

Use caution with the *ssl\_reinitialize\_keystore* callback. This callback changes the encryption hash of wasp.keystore, and will *invalidate any certificates you are currently using*. For this reason, it is

strongly recommended that you back up individual key and certificate files, so that if you have to reinitialize the keystore, you can reload the keys and certificates into the new keystore.

In addition, do not use the keytool utility to change the password of wasp.keystore, as wasp will not recognize the new password. Currently, the only way to change the password of wasp.keystore is to use the `ssl_reinitialize_keystore` callback.

#### Follow these steps:

1. Open Infrastructure Manager.
2. Navigate to the server running the wasp probe.
3. Click on the wasp probe to highlight it.
4. Press `Ctrl+<P>` to open the probe utility.
5. In the drop-down list under **Probe commandset**, select **ssl\_reinitialize\_keystore**.
6. Enter a new password as an argument.

#### NOTE

Use a password that is at least six characters long. The wasp probe utility will not prevent you from using a shorter password, but you will be unable to make changes to the wasp.keystore file as described later.

7. Click the green play button to run the callback.  
The **Command** status bar displays the text **OK**.
8. Securely record the password you set for future use.

#### Generate a Public and Private Key Pair

#### Follow these steps:

1. Open an administrator command prompt on the server running wasp

#### NOTE

Run the following keytool commands in the same directory as the wasp.keystore file, typically `<OC or UIM server_installation>/probes/service/wasp/conf`. The keytool utility is located in the directory where the JRE resides, typically `<OC or UIM server_installation>/jre/<jre_version>/bin/keytool`.

2. Set the JAVA\_HOME environment variables as follows:  
`<OC or UIM server_installation>/jre/<jre_version>/bin/`
3. Verify that you have a valid password for the wasp.keystore file:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> keytool -list -keystore wasp.keystore`  
You will receive a confirmation message, 'Your keystore contains 1 entry.'
4. Delete the automatically generated private key:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> keytool -delete -alias wasp -keystore wasp.keystore`
5. Verify that the key was deleted:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> keytool -list -keystore wasp.keystore`  
You will receive a confirmation message, 'Your keystore contains 0 entries.'
6. Generate the public and private key pair with the key size you require:  
`<OC or UIM server_installation>Nimsoft/probes/service/wasp/conf> keytool -genkeypair -alias wasp -keyalg RSA -keysize <key_size> -keystore wasp.keystore -validity <days_cert_is_valid>`
7. When prompted for your first and last name, enter the FQDN.
8. When prompted, provide entries for the following fields:

- Organizational unit
- Organization
- City or Locality
- State or Province
- Two-letter country code

You are prompted to confirm that the information you entered is correct.

### **Record Certificate Information**

#### **Follow these steps:**

1. Securely record the new password that you set for the wasp.keystore file.
2. Ensure that you record the validity period you set for the certificate.
3. Back up the certificate files to a secure location.

### **Generate and Submit a CSR**

#### **NOTE**

For a wildcard certificate, enter **<your\_domain>.csr** as the last argument in this command.

#### **Follow these steps:**

1. Generate a Certificate Signing Request (CSR):  
`<OC or UIM server_installation>/jre/<jre_version>/bin/keytool -certreq -alias wasp -validity <days_cert_is_valid> -keystore <OC or UIM server_installation>Nimsoft/probes/service/wasp/conf/wasp.keystore -file <your_domain>.csr`

#### **NOTE**

The CSR is built with the public keys that are generated by using the RSA key algorithm. Therefore, the certificates from the certificate authority must be built with the key encipherment ("Allows key exchange only with key encryption") encryption option.

2. **(Optional)** Create a backup copy of the wasp.keystore. This is not a required step, but it is strongly recommended. In the event you encounter a problem later in this procedure, a backup copy of the wasp.keystore file will save you from having to repeat previous steps.
3. Submit the CSR to the certificate authority:
  - a. Paste the CSR into the web form of the certificate authority.
  - b. Remove any characters before **----BEGIN CERTIFICATE REQUEST** and after **END CERTIFICATE REQUEST----**.

### **Import the Certificates**

#### **NOTE**

All keystore entries must use a unique alias. You must use the alias wasp for the signed, or entity certificate. If your certificate authority provides multiple intermediate certificates, each intermediate certificate must also use a unique alias.

#### **Follow these steps:**

1. Open an administrator command prompt on the server running OC.

#### **NOTE**

Run the following keytool commands in the same directory as the wasp.keystore file, typically `<OC or UIM server_installation>/probes/service/wasp/conf`. The keytool utility is located in the directory where the JRE resides, typically `<OC or UIM server_installation>/jre/<jre_version>/bin/keytool`

2. If your certificate authority provided a root certificate, import the root certificate:

- ```
<OC or UIM server_installation>/jre/<jre_version>/bin/keytool -import -trustcacerts -alias <root_certificate> -
file <root_certificate>.cer -keystore <OC or UIM server_installation>Nimsoft/probes/service/wasp/conf/wasp.keystore
```
3. Import the intermediate certificate:

```
<OC or UIM server_installation>/jre/<jre_version>/bin/keytool -import -trustcacerts -
alias <first_intermediate_certificate> -file <first_intermediate_certificate>.cer -
keystore <OC or UIM server_installation>Nimsoft/probes/service/wasp/conf/wasp.keystore
```
 4. Repeat the previous step as needed for additional intermediate certificates.
 5. Import the signed certificate. This is the entity certificate if you received a chained certificate:

```
<OC or UIM server_installation>/jre/<jre_version>/bin/keytool -import -trustcacerts -alias wasp -
file <your_domain>.crt -keystore <OC or UIM server_installation>Nimsoft/probes/service/wasp/conf/wasp.keystore
```
 6. Click **yes** at the prompt **Existing entry alias wasp exists, overwrite?**
 7. Issue the following command to verify that the wasp.keystore file was updated:

```
<OC or UIM server_installation>/jre/<jre_version>/bin/keytool -list -keystore <OC or UIM server_installation>Nimsoft/
probes/service/wasp/conf/wasp.keystore
```
 8. Restart the wasp probe.

Test the HTTPS Connection

NOTE

Self-signed certificates can cause some browser errors or notifications, such as "Your connection is not private" or "The identity of this website has not been verified." These are normal messages and can be prevented by importing the certificate to the browser (though not all browsers allow this). To avoid these messages altogether, you must use a certificate from a certificate authority.

Follow these steps:

1. Open a supported Web browser.
2. Enter https:// followed by the URL for Operator Console or Admin Console.

The login page appears if wasp configuration was successfully modified to use HTTPS.

Note: You can click the lock icon to the left of the URL in the browser address window to view information about the connection.

(Operator Console Only) Set Automatic HTTP to HTTPS Redirect

You can set the automatic HTTP to HTTPS redirect by following this procedure.

Follow these steps:

1. Search for the WEB-INF/web.xml files in the <OC or UIM server_installation>/Nimsoft/probes/service/wasp/webapps/ folder, and open the files for editing.
2. Locate the following content:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>un_restricted_methods</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>NONE</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```
3. Replace <transport-guarantee>NONE</transport-guarantee> with <transport-guarantee>CONFIDENTIAL</transport-guarantee> .

4. Save the web.xml files.

5. Open the following file for editing:

```
<OC or UIM server_Installation>\Nimsoft\probes\service\wasp\wasp.cfg
```

6. Add the following lines before </setup> :

```
<http_connector>    redirectPort=<desired port></http_connector>
```

where <desired port> matches the https_port key defined in the Modify wasp to Use HTTPS subsection .

NOTE

Ensure that you include the redirect code within the <setup> section.

7. Save the wasp.cfg file.

8. Restart the wasp probe.

NOTE

Dual mode (that is, both HTTP and HTTPS) is not allowed. Administrators can configure HTTP-only, HTTPS-only, or HTTP to HTTPS redirect.

Set/Enable Secure Flag for Cookie

You can set/enable a secure flag for cookies in Admin Console and OC:

- [Set/Enable Secure Flag for Cookie in Admin Console](#)
- [Set/Enable Secure Flag for Cookie in Operator Console](#)

Set/Enable Secure Flag for Cookie in Admin Console

For setting/enabling the secure flag for the cookie in Admin Console.

Follow these steps:

1. Open the following file for editing:

```
<UIM server_installation>/Nimsoft/probes/service/wasp/webapps/adminconsoleapp/WEB-INF/web.xml.
```

2. Uncomment the < secure> Tag

```
<session-config>
  <session-timeout>1</session-timeout>
  <cookie-config>
    <http-only>true</http-only>
    <!--<secure>true</secure>-->
  </cookie-config>
</session-config>
```

Set/Enable Secure Flag for Cookie in Operator Console

For setting/enabling the secure flag for the cookie in Operator Console.

Follow these steps:

1. Open the following file for editing:

```
<OC>/Nimsoft/probes/service/wasp/webapps/ROOT/WEB-INF/web.xml.
```

2. Uncomment the < secure> Tag

```
<session-config>
  <session-timeout>1</session-timeout>
  <cookie-config>
    <http-only>true</http-only>
```

```

        <!--<secure>>true</secure>-->
    </cookie-config>
</session-config>

```

Update Expect-CT Header Values

You can update Expect-CT-Header values in Admin Console and OC:

- [Update Expect-CT Header Values in Admin Console](#)
- [Update Expect-CT Header Values in Operator Console](#)

Update Expect-CT Header Values in Admin Console

By default Expect-CT is set to “enforce, max-age=300”, to change the values or adding report-uri.

Follow these steps:

1. Navigate to the **wasp.cfg** file located in the following location:
<UIM server_Installation>\Nimsoft\probes\service\wasp\wasp.cfg
2. Open the **wasp.cfg** file in a text editor.
3. In the webapps\adminconsole section, add/edit configuration attributes in Expect-CT-Header property as below
 Expect-CT-Header = enforce, max-age=300
4. Restart the wasp.

Update Expect-CT Header Values in Operator Console

By default Expect-CT is set to “enforce, max-age=300”, to change the values or adding report-uri in the Operator Console.

Follow these steps:

1. Navigate to the **wasp.cfg** file located in the following location:
<OC server_Installation>\Nimsoft\probes\service\wasp\wasp.cfg
2. Open the **wasp.cfg** file in a text editor.
3. In the webapps\operatorconsole_portlet\custom\uncrypted section, add/edit configuration attributes in Expect-CT-Header property as below
 Expect-CT-Header = enforce, max-age=300
4. Restart the wasp.

(Optional) Access CABI Server

Additional configuration is required if you are using the CABI for UIM dashboards. For more information, see the (Optional) Access CABI Server with HTTPS section in [CA Business Intelligence with CA UIM](#).

NOTE

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

Configure OC to Use SAML Single Sign-On

This scenario describes how a security administrator configures the Operator Console (OC) to use the Security Assertion Markup Language (SAML) 2.0 for single sign-on (SSO) for Account Contact users.

Contents

Verify Prerequisites

Ensure that the following prerequisites have been met before using the instructions in this scenario:

- You are proficient with CA UIM Monitor, your SAML 2.0 identity provider, and LDAP directory administration.
- UIM Server and OC 20.3.0 are installed and configured.
- You are an administrative user with access to Infrastructure Manager.
- Your environment is configured to run Java keytool commands. The %PATH% system variable must include the path to java.exe and keytool.exe.
- A SAML 2.0 Identity Provider (Issuer) such as CA SiteMinder r12.51 or higher is installed and configured.
- An LDAP directory for authentication and for linking to CA UIM Monitor is installed and configured. The following LDAP directory services are supported:
 - Novell © eDirectory(TM) 8.8 SP1 (20114.57) and Novell © KDC (Key Distribution Center) server
 - SUN Java Directory Server v5.2
 - Windows 2008 and Windows 2012 Active Directory

Verify LDAP Mapping

The following table identifies the user and group attributes that must map between your directory and the UIM hub and OC. The attributes designated with an asterisk (*) are the required mappings for OC. It is recommended that you determine these attributes in your directory service before continuing.

Refer to this table as needed as you perform the steps in the following sections.

| Description | UIM Hub Mapping | UIM Mapping | LDAP Example |
|-------------------|----------------------------|---------------------------------|---------------------------|
| Group identifier | filter_group | ldap.import.group.search.filter | objectClass=groupOfNames |
| Group name | attr_grp_name | groupName | cn |
| Group member | attr_grp_member_name | user | member |
| Group description | attr_grp_description | description | description |
| User identifier | --- | ldap.import.user.search.filter | objectClass=inetOrgPerson |
| *Username | attr_usr_id | screenName | cn |
| *User Password | --- | password | userPassword |
| *User firstname | attr_usr_firstname | firstName | givenName |
| *User lastname | attr_usr_lastname | lastName | sn |
| *User email | attr_usr_mail, filter_user | emailAddress | mail |

Configure LDAP on the Hub Probe

Configure the hub probe to forward login requests to your LDAP server, and to access the container with user groups.

Follow these steps:

1. Log into Infrastructure Manager and locate the hub probe.
2. Press the <Ctrl> key as you right-click the hub probe, and select Raw Configure.

3. Expand the LDAP section, and expand the templates section.
4. Select the appropriate directory service, and edit the value of the key *filter_user* to use either *attr_usr_email* or *attr_usr_id* for log in lookups as follows:
(`!(($attr_usr_mail=$loginname))($attr_usr_id=$loginname)`)
5. Set the value of the key *attr_usr_id* to *cn*.
6. Depending on the directory service you are using, you may need to update the values of other keys to match your directory. Attributes that may be of particular importance are as follows:
 - *filter_group*
 - *filter_user*
 - *attr_grp_name*
 - *attr_grp_member_name*
 - *attr_grp_description*
 - *attr_usr_firstname*
 - *attr_usr_lastname*
7. Click Ok to commit your changes.
The hub probe restarts.
8. In Infrastructure Manager, right-click on the hub probe and select Configure.
9. In the lower right of the General tab, select Settings.
10. In the LDAP tab, do the following:
 - a. Select Direct LDAP.
 - b. Select LDAP Authentication.
 - c. In the Server Name field, enter the `<IP_address:port>` or the `<server_FQDN:port>` of the LDAP server.
 - d. Select the appropriate directory service from the Server Type drop-down menu.
 - e. Select *LDAP > Nimsoft* from the Authentication Sequence drop-down menu.
 - f. In the User field, enter the distinguished name (DN) of a directory user with administrative privileges.
 - g. Provide a distinguished name (DN) in the Group Container (DN) and User Container (DN) fields as appropriate.
 - h. Click the Lookup button to verify the connection to the LDAP server.
 - i. Click the Test button to verify the credentials of the directory user with administrative privileges.
 - j. Click Ok and confirm the dialog to restart the hub. Your changes are committed.

Link ACLs to LDAP Groups

Use the following steps to link ACLs to LDAP groups.

Follow these steps:

1. In Infrastructure Manager, select Security >Manage Access Control List.
2. Make a selection from the Access Control List, and click the Set LDAP Group button.
3. Select an LDAP group from the list.
4. Select or de-select permissions in the list if desired.

Modify the OC Configuration to Enable SAML

Use the following steps to edit the `config.properties` file to configure OC for SAML.

Follow these steps:

1. In Infrastructure Manager, deactivate the wasp probe.

WARNING

Do not edit `config.properties` while the wasp probe is running. Doing so will cause the wasp probe to crash.

2. On the OC server, open the following file for editing: `<OC_installation>\probes\service\wasp\conf\config.properties`.

3. Locate the property `company.security.auth.type` and set it to `screenName` or `emailAddress`, depending on the attribute you authenticate with.
4. Open the `samlSsoConfig.properties` in the directory `<OC_installation>\probes\service\wasp\webapps\samlSso\WEB-INF\classes\`. The values in the SAML configuration of the Operator Console (OC) server and to configure your SAML identity provider need to be updated. Below are the key values:
 - a. `saml.configuration.enabled` - to enable SAML configuration
 - b. `saml.sp.metadata.id` - specifies the ID provided by the Service Provider
 - c. `saml.sp.metadata.entityid` - specifies the EntityID provided by the Service Provider
 - d. `saml.sp.metadata.wantAssertionSigned` - to enable Assertion for the Service Provider
 - e. `saml.sp.keystore.path` - specifies the path for the keystore file
 - f. `saml.sp.keystore.password` - specifies the password for the keystore file
 - g. `saml.sp.keystore.aliasName` - specifies the alias name for using keystore file
 - h. `saml.sp.keystore.aliasPassword` - specifies the password for the alias name for the keystore file
 - i. `saml.sp.tempredirect.url` - specifies the temporary redirect url
 - j. `saml.idp.authenticationsuccess.redirecturl` - specifies the redirect url after successful authentication
 - k. `saml.idp.metadatafile.path` - specifies the path for the metadata file by IDP

TIP

You may specify the same or different passwords for `saml.sp.keystore.password` and `saml.sp.keystore.aliasPassword`. We recommend using the same password for both properties unless you have a specific security reason.

7. Save the `config.properties` and `samlSsoConfig.properties` files and reactivate the `wasp` probe.

Create a Keystore for use with SAML**Follow these steps:**

- Open an administrator command prompt on the Operator Console (OC) server. Use the values you specified in `config.properties` to generate the file `keystore.jks`.
- The `keytool` utility is located in the directory where the JRE resides, typically `<OC_installation>\jre<jre_version>\bin\keytool`.
- Generate the keystore and key:

```
Keytool -genkey -keyalg RSA -alias <ocEntityId> -keystore keystore.jks -storepass <keystorePassword> -validity
<days_cert_is_valid> -keysize 2048
```

NOTE

The alias you use for `<ocEntityId>` in the `keytool` command must match the value in the `samlSsoConfig.properties` file for the key `saml.sp.metadata.entityid`.

- Move the `keystore.jks` file to the location specified in the `samlSsoConfig.properties` file for `saml.sp.keystore.path`, which is equivalent to `<OC_installation>\probes\service\wasp\webapps\samlSso\WEB-INF\classes\security\keystore.jks`.

Generate OC Metadata for SAML

OC provides a mechanism to generate the SAML metadata used by an identity provider for single sign-on. The service provider entity information generated by OC can be imported into many SAML 2.0 identity providers, including CA SiteMinder.

Use the following steps to generate OC metadata for SAML.

Follow these steps:

1. Open a browser and go to `http://<OC_Server>/samlSso/saml/metadata`. The SAML metadata for OC is displayed.

WARNING

You can access the metadata page using the OC server FQDN, Operator Console (OC) server IP address, or via a proxy URL if you are using a proxy server. The SAML metadata address you use must match the format you will use in production. Specific metadata is generated based on the address you use to access the SAML metadata page.

2. Save the generated metadata as a file of type xml.

Configure a SAML Identity Provider for OC

OC supports SAML version 2.0 for single sign-on. OC acts in the role of a service provider. If your identity provider does not support importing generated OC SAML metadata, you must provide some or all of the following information directly to your identity provider.

NOTE

See the appendix [Configure CA SiteMinder for OC with SAML Single Sign-On](#) for specific instructions to configure CA SiteMinder as an identity provider.

Information to provide to identity providers

- SAML Version. OC supports SAML version 2.0.
- Issuer. A URL that uniquely identifies your SAML identity provider.
- Entity ID. Another name for the Issuer.
- Identity Provider Certificate. The authentication certificate issued by your identity provider.
- Signing Certificate. The certificate you generate in a keystore to secure communications between Operator Console (OC) and a SAML identity provider.
- Identity provider login URL. The URL where OC sends a SAML request to start the login sequence.
- Identity provider logout URL. The URL a user is directed to when logout is selected.
- LDAP directory. The LDAP directory used by OC. The identity provider must use the same LDAP directory as OC.
- SAML Identity Attribute Name. The SAML assertion element which contains the string identifying an OC user. This value is equivalent to the value of the `company.security.auth.type` property in `config.properties`.
- Required assertions. Supply the assertions mapped in the file `config.properties`. For each assertion, provide the LDAP directory field name which maps to the assertion attributes specified in the property `saml.sp.user.attribute.mappings`.
Example required assertions:
 - – `screenName` LDAP value `cn`.
 - – `emailAddress` LDAP value `mail`.
 - – `firstName` LDAP value `givenName`.
 - – `lastName` LDAP value `sn`.

NOTE

Your identity provider may require additional information. Refer to the documentation specific to your identity provider for details.

Information to collect from identity providers

- Entity ID (Issuer) of the identity provider.
- Authentication certificate from the identity provider.
- SAML user id type assertion.
- SAML user id assertion location.

Many identity providers allow you to generate and export identity provider metadata for the OC server to use. To use a generated metadata file, follow these steps:

- Rename a generated metadata file to match the file name specified in the property `saml.idp.metadatafile.path` in the file `samlSsoConfig.properties`.
- Copy the renamed file to the location specified in `saml.idp.metadatafile.path` on the OC server.
- Restart the wasp probe to ensure that the keystore and identity provider metadata are properly imported.

Verify SAML Single Sign-On

You can log in to OC in two ways:

1. Click the Single sign On link on the OC login page.
This method performs a SAML login.
2. Perform a local (non-SAML) login using the SIGN IN option in the OC login page.

NOTE

First time users need to perform the local login using the SIGN IN option in the main login page.

Back Up the SAML Configuration

Upgrading OC does not preserve the SAML configuration files. Perform the following procedure to ensure that SAML configuration is preserved during an upgrade:

1. Copy the file `<OC_installation>\probes\service\wasp\webapps\ROOT\WEB-INF\classes\portal-ext.properties` to a backup directory which is not a part of the `<OC_installation>` directory tree.
2. Copy the directory `<OC_installation>\probes\service\wasp\webapps\ROOT\data` to a backup directory which is not a part of the `<OC_installation>` directory tree.

After completing the upgrade, copy the backup folder to the original location to restore your SAML configuration. In UIM 20.3.0, `portal-ext.properties` file is deprecated and the data can be added to the file `<OC_installation>\probes\service\wasp\conf\config.properties`.

Configure SiteMinder for OC with SAML Single Sign-on

To implement SAML single sign-on for OC, configure OC to act in the role of Service Provider and configure SiteMinder to act in the role of Identity Provider.

You implement SAML for OC in CA SiteMinder by importing the OC service provider entity, and creating a Federation Partnership between the CA SiteMinder identity provider entity and the OC service provider entity.

Create an OC Service Provider Federation Entity

Follow these steps:

1. Log in to the SiteMinder Administrative UI.
2. Expand Federation, Partnership Federation, Entities.
The list of existing Federation Entities is displayed.
3. Click Import Metadata.
The Import Metadata Wizard opens.
4. Browse to the .xml file you saved previously in [Generate OC Metadata for SAML](#).
5. Select Import As Remote Entity, and Operation as Create New.
The OC entity is imported into SiteMinder as type SAML2 SP.

NOTE

If you receive an error trying to extract entities from the metadata, check to be sure the metadata.xml file you are attempting to import was saved as type xml.

6. Enter an Entity Name. The Entity Name can be the same as the Entity ID.
7. Select certificate key entries to import. Enter the alias name you used when you created the keystore in the section [Create a keystore for Use with SAML](#).
8. Click Finish.
A new entry with the following parameters is created in the Federation Entity List corresponding to the OC metadata you imported:
 - Entity Name is the name you provided.
 - Entity Id is the Id stored in the metadata.
 - Location is Remote.
 - Entity Type is SAML2 SP. *SAML2* identifies the entity as SAML Version 2.0. *SP* identifies the entity as a SAML Service Provider.
 - Partnership Count is 0 because a partnership with a SAML Identity Provider has not yet been created.

Create a Federation Partnership**Follow these steps:**

1. Expand Federation, Partnership Federation, Partnerships.
2. Select SAML2 IDP - > SP in the Create Partnership drop-down list.
The Configure Partnership Wizard opens.
3. Enter a name for the Partnership.
4. Optionally, provide a description.
5. Select a Local IDP from the drop-down list.

NOTE

If you do not have a local SiteMinder Identity Provider, click Create Local Entity to create one. See the [CA SiteMinder documentation](#) for information on how to create a local CA SiteMinder Identity Provider and secure it with a certificate.

6. Select the Service Provider entity you created in the Federation Entity List.
7. Skew Time (Seconds) defaults to 30 seconds. Refer to the [CA SiteMinder documentation](#) for details about Skew Time.
8. In User Directories and Search order, select the LDAP Directory you specified in config.properties. Use the arrow button to move the directory to the Selected Directories list on the right.

NOTE

The Identity Provider must use the same LDAP directory as the OC SAML Service Provider.

9. Click Next.
10. For the selected LDAP directory, select the users to include in the partnership from the User Class drop-down list.
11. Click Next. The Assertion Configuration page opens. The values you supply for Name ID must map to the values you provided in the property `saml.sp.user.attribute.mappings` in the `config.properties` file. Required assertions are:
 - `screenName`
 - `emailAddress`
 - `firstName`
 - `lastName`
12. Select Email Address for Name ID Format.
13. Select User Attribute for Name ID Type.

14. Enter *mail* in the Value field.
15. For each assertion, set the Type to *User Attribute*, and provide the LDAP directory field name in the Value field which maps to the assertion attribute.
For example:
 - screenName Value: cn
 - emailAddress Value: mail
 - firstName Value: givenName
 - lastName Value: sn
16. Click Next to advance to the SSO and Single Log-out (SLO) Authentication configuration page.

Configure the Authentication Section

Follow these steps:

1. Select Authentication Mode Local.
2. Enter the URL for LDAP authentication in the Authentication URL field.
For example:
`http://<Federation_Web_Services_Server>/affwebservices/redirectjsp/redirect.jsp`
3. Use the default values for all other fields in the Authentication section.

Configure the SSO Section

Follow these steps:

1. In the SSO section, select HTTP-POST for Authentication Request Binding, and for SSO Binding.
2. Use the default values for all other fields in the SSO section.

Configure the SLO Section

Follow these steps:

1. Select HTTP-Redirect and SOAP for SLO Binding.
2. Use the default values for all other SLO fields.
3. Provide SLO Service URLs for each SLO Binding selected:
 - For HTTP-Redirect: `http://<OC_Server_FQDN>/saml/SingleLogout`
 - For SOAP: `http://<OC_Server_FQDN>/saml/SingleLogout`
4. Enter `mail=%s` in the LDAP field for User Lookup for Attribute and Name ID Services.
5. Use the default settings for Back Channel configuration.
6. Click Next to proceed to Signature and Encryption.

Configure the Signature Section

Follow these steps:

1. Select `sm_idp_entity` for Signing Private Key Alias.
2. Select `RSAwithSHA1` for Signing Algorithm.
3. Select the Operator Console (OC) Alias you used when generating the OC Keystore for Verification Certificate Alias.
4. Select Sign Neither for Artifact Signature Options.
5. Select Sign Both for Post Signature Options.
6. Select Sign Both for SLO SOAP Signature Options.
7. Check Require Signed Authentication Requests

Configure the Encryption section

Follow these steps:

1. Use the default settings provided for the Encryption section.
2. Click Finish.
You are returned to the Federation Partnership List.

Activate and Export the Partnership Metadata the OC Server Will Use

Follow these steps:

1. In the Federation Partnership List, verify that the partnership status is Active.
2. Select Export Metadata from the partnership Action drop-down list.
A summary of the metadata options you provided is displayed.
3. Select <Idp_EntityId> as the Document Signature Alias.
4. Select RSAwithSHA1 for the Document Signature Algorithm.
5. Select the number of days for the partnership to remain valid.
6. Click Export.
7. Rename the generated output file to match the file name specified in the property saml.idp.metadatafile.path in the samlSsoConfig.properties file.
8. Copy the file to the location specified on the OC server in the property saml.idp.metadatafile.path in the samlSsoConfig.properties file.

Verify that the Partnership between the CA SiteMinder Identity Provider and the OC Service Provider Exists in CA SiteMinder

Follow these steps:

1. Go to the CA SiteMinder Federation Entity List page.
2. Verify that the OC SP Entity exists in the list and has a Partnership count of 1.
3. Verify that the CA SiteMinder Identity Provider Entity exists in the list and that the Partnership Count has increased by one.

Define Account Contact Users Before Attempting SAML Authentication

Any account contact users that use SAML single sign-on must be defined before authentication will work. Account contacts are defined by linking them to an account and defining an associated ACL. For more information, see the article [Add or Modify Users with the Account Admin](#).

Encrypting the Passwords

Passwords can be encrypted using a java utility (EncryptionUtil) and can be used as part of the SAML configuration. To encrypt the passwords, **follow these steps:**

1. Make sure Java is installed on your machine. To verify, open the command prompt and type java -version.
2. Open the folder location <Nimsoft Installation Directory>\probes\service\was\webapps\samlSso using command prompt. [e.g - C:\Program Files (x86)\Nimsoft\probes\service\was\webapps\samlSso]
3. Execute the command java -jar EncryptionUtil.jar <TextToEncrypt> and press Enter . [Example : java -jar EncryptionUtil.jar UMP2030]
4. Encrypted text will appear, copy the encrypted text to use as passwords.

NOTE

SAML authentication will not work for a NimBUS user.

Enable Login with LDAP

The **Lightweight Directory Access Protocol** (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an IP network.

The LDAP solution:

- Makes it possible to log in to the management consoles using LDAP rather than the login method
- Allows the primary hub to check all login requests against the LDAP server before trying the standard login method
- Is supported on Windows and Linux
- Requires certain configuration tasks on the hub and in Infrastructure Manager

Supported LDAP software:

- Active Directory
- eDirectory
- Red Hat Directory Server (RHDS) 10

Supported LDAP versions:

- V2
- V3

Contents

Basic LDAP Configuration

Configure your hub to forward login requests to an LDAP server and to access the container with the user groups.

Follow these steps:

1. On the hub system, start Infrastructure Manager.
2. Select the hub probe for the domain (domain/hub/robot/hub probe).
3. Right-click the hub probe and select **Configure** to open the hub configuration window.
4. On the **General** tab, click **Settings**. Go to the **LDAP** tab and specify the following settings.
 - **Direct LDAP**
Select this if the hub connects directly to the LDAP server.
 - **Nimsoft Proxy Hub**
Select this if the hub does not connect directly to the LDAP server.
 - **Server Name**
Hostname or IP for the LDAP server to which the hub will connect (click Lookup to test the communication).
 - **Server Type**
LDAP server type, either Active Directory, eDirectory, or RHDS 10.
 - **Authentication Sequence**
Specify the order in which Unified Infrastructure Management authenticates users.
 - **Use SSL**
Select to use SSL during LDAP communication (most LDAP servers are configured to use SSL).
 - **User/Password**
Name and password for an account on the LDAP server that the hub will use when accessing the LDAP server.
How you specify it depends on the server type:
 - **Active Directory** -- ordinary user name
 - **eDirectory** -- path to the user in the format *CN=username,O=organization*, where *username* and *organization* are replaced by appropriate values

Note: This account does not need administrative privileges but does need the appropriate lookup privileges.

- **Group Container (DN)**
Location in the LDAP structure where you want to search for users (click **Test** to check if the container is valid).
 - **User Container (DN)**
Location in the Group Container where you want to search for users.
5. Click **Test** to verify that the user/password and container settings are valid.

Advanced LDAP Configuration

If you do not want to use the default configuration values, you can add tree keys to the hub configuration. These keys are read by the hub LDAP engine and affect how the hub communicates with the LDAP protocol.

1. On the hub system, start Infrastructure Manager.
2. Select the hub robot's hub probe (domain/hub/robot/hub probe).
3. Shift-right-click the hub probe to open the **Raw Configure** window.
4. In the left pane, navigate to **ldap > server**.
5. Click **New Key** and enter the following tree keys and values:
 - **Timeout**
Number of seconds to spend on each searching or binding (authentication) LDAP operation.
Accepted values are:
 - 10 (default)
 - Desired number
 - **codepage**
Specifies which codepage to use when translating characters from UTF-8 encoding to ANSI (which all CA Unified Infrastructure Management components use internally). Text in the LDAP library is encoded as UTF-8. Because CA Unified Infrastructure Management products do not have true Unicode support, all characters are translated into ANSI using this codepage.
Accepted values are:
 - 28591* (Windows default)
 - Valid codepage number (Windows)
 - ISO-8859-1* (Linux default)
 - Text string that is passed to the iconv_open function (Linux)
 * *ISO 8859-1 Latin 1; Western European (ISO)*
6. Click **OK**.

The tree key is added.

Hub LDAP Client Authentication

This feature will enable the Hub to send client certificates to the LDAP server which will then be validated at the server end.

For Linux Hub

Follow these steps:

1. If there are no server/client certificates, download openssl application and use the documentation of [openssl](#) to create self-signed certificates.

NOTE

When creating the certificates CN (common name) of the certificates should be FQDN of that target machines where the certificates are to be installed.

2. Convert all the client certificates into PEM format, if the format of certificates are different (eg. crt, der etc.).

3. Copy the client certificates to the hub machine. For instance it is copied to “/root/certs/”
4. Create a .ldaprc file in the ‘/root/’ folder of the hub machine.
5. Edit the .ldaprc file and point the certificate file and key file to the path where the certificates are copied.

a. **Contents of .ldaprc:**

```
TLS_CACERT /root/certs/cacert.pem
TLS_CACERTDIR /root/certs/
TLS_REQCERT allow
TLS_CERT /root/certs/client.pem
TLS_KEY /root/certs/client.key
```

6. Refer to [5.2 Client](#) of the [OpenLDAP Server With Server-Side SSL/TLS and Client Authentication](#) documentation for the detailed explanation of the above parameters of the OpenLdap Client.
7. Create a new Environment variable for robot in the robot.cfg of that hub, name it as **LDAPRC** and point to the .ldaprc path.

```

1 <controller>
2   domain = ci653811_win12r2_domain
3   robotname = ci653811_ldev2
4   robotip = 10.17.167.64
5   ip_version = ipv4 ipv6
6   robotip_alias =
7   first_probe_port =
8   autoremove =
9   robot_mode = normal
10  reuse_async_session = 1
11  access_0 = 0
12  access_1 = 1
13  access_2 = 2
14  access_3 = 3
15  access_4 = 4
16  hub = ci653811_ldev2_hub
17  hubrobotname = ci653811_ldev2
18  hubip = 10.17.167.64
19  hubport = 48002
20  <environment>
21    LD_LIBRARY_PATH = .:$LD_LIBRARY_PATH:..:$LD_LIBRARY_PATH:..:$LD
22    LDAPRC = /root/.ldaprc
23  </environment>
24 </controller>
25

```

C:\Users\ci653811\DOCUMENTS\MobaXterm\slash\Ren UNIX Plain text 25 lines Row #1 Col

- Restart the hub robot.

For Windows Hub

Follow these steps:

- If there are no server/client certificates, download openssl application and use the documentation of [openssl](#) to create self-signed certificates.

NOTE

When creating the certificates CN (common name) of the certificates should be FQDN of that target machines where the certificates are to be installed.

- Convert the client certificates and 'ca chain' certificates to a single p12 or pfx, so that it can be imported to windows certificate store.

3. Install the client p12/pfx file into windows "local machine" using the Certificate Import Wizard. The certificates will be imported to your "local machine" personal store and can be verified by opening "mmc certificate console".
4. Go to "computer account" in the certificates snap-in wizard of mmc and add the certificates. The Hierarchy of the certificates is displayed by double clicking the certificates.
5. If the ca certificates chain is not installed properly then it shows a warning "*The issuer of this certificate could not be found.*" Try importing certificate into "trusted root certification authority" by browsing the p12/pfx file.
6. Download and run the [LdapAdminExe tool](#) and create a new connection with "SSL" checkbox. Verify the connection by clicking on the "Test Connection", proper certificate installation will give the "Connection is successful" message. Successful connection in the tool ensures the successful connection in the hub as well.

Windows operating system internally maintains certificates in its trust store and forwards the matching certificate to the server without intervention of the application (Hub) and then server validates the certificate for the legitimacy of the client.

Codepage Values

The hub LDAP library uses these functions.

- **Windows:** *MultibyteToWideChar* and *WideCharToMultiByte*
These functions translate to and from ANSI/UTF-8. Both take a code page as a parameter. For a list of Windows code page numbers, go to <http://www.microsoft.com> (*not affiliated with CA*) and search for *Code Page Identifiers*.
- **Linux:** *iconv* functions
For further reference, go to <http://www.gnu.org/software/libiconv> (*not affiliated with CA*).

The code page key is not shipped with the hub configuration file.

Connecting Access Control Lists to LDAP Users

You can create Access Control Lists (ACLs) and can associate them with specific LDAP groups. The users in the LDAP group are then assigned the privileges for the associated ACL.

For example, if an LDAP user logs in to a UIM component, the request is directed to the LDAP server for authentication. If the user name is found in a group that is attached to an ACL, the user is assigned privileges as defined in the ACL. If the user belongs to multiple groups, privileges are assigned from the ACL with the most extended privileges.

WARNING

LDAP users must be direct members of the group that you are connecting to an ACL. UIM does not support the use of Nested or *Role Based* groups. Bus users should not share an ACL with LDAP users, or bus users will inherit LDAP accounts..

Follow these steps:

1. In Infrastructure Manager, select **Security > Manage Access Control List**.
2. To create an ACL:
 - a. Click **New** under **Access Control List**.
 - b. Name the new ACL, then select an ACL (if any exist) to copy its settings. Click **OK**.
 - c. Select the desired options in the **Permissions** area.
3. To associate a group with an ACL:
 - a. Select the new or existing ACL.
 - b. Click **Set LDAP Group**. All groups in the container are listed.
 - c. Select a group and click **OK**.
4. Click **OK** in the **Manage Access Control List** dialog.

The new setting is active. To verify the configuration, start Infrastructure Manager and log in as an LDAP user who is not a CA Unified Infrastructure Management user. Verify that you have the appropriate privileges and can access the expected contents.

Encrypt UIM Network Traffic with SSL

NOTE

This functionality is achieved through secure hub and robot in CA UIM 20.3.0.

CA UIM supports an SSL encrypted communication between CA UIM components. By default, communication is *not* encrypted.

- Only network traffic is encrypted. Encryption is not used for authentication.
- A compatibility mode enables communication between components that support SSL and components that do not.

The SSL mode is specified in the hub configuration, and is used primarily for robot-to-hub communication. When hubs are not connected with tunnels, the hub SSL mode controls the hub-to-hub communication.

SSL communication is enabled through the `UIMHOME/robot/robot.pem` certificate file. The controller creates the file containing the key to decode encrypted messages at startup.

NOTE

Java probes do not support SSL mode or Compatibility mode. Use SSL mode 0 for communication with java probes, and on hubs where the wasp probe is installed.

The v7.70 release of the hub and robot improve the robustness of SSL communication. Before, in a nontunneled domain, hubs that are configured for unencrypted communication can decode encrypted messages. In a multiple hub domain, upgrading to v7.70 breaks this type of communication. For details, see the [Hub \(hub\) Release Notes](#) in Probes Documentation Space.

Any tunnels set up between hubs remain after an upgrade, and communication continues. We recommend that you connect hubs with tunnels to ensure the integrity of the communications.

You can set the communication mode in Admin Console or Infrastructure Manager.

1. Navigate to the hub. Expand the hub robot, and open the hub probe in the configuration UI.
2. Go to the SSL settings:
 - In Admin Console, navigate to **Advanced > SSL**.
 - In Infrastructure Manager, navigate to the **General** tab, click **Settings**, and click the **SSL** tab.
3. Select the mode. CA UIM hubs have three communication mode options:
 - **Normal** SSL mode 0 - Communication occurs with no encryption. The OpenSSL transport layer is not used.
 - **Compatibility mode** SSL mode 1 - Communication occurs without encryption, or with OpenSSL encryption. Components first attempt to communicate through SSL. If a request is not acknowledged, the component sends the request unencrypted.
 - **SSL Only** SSL mode 2 - Communication occurs only with OpenSSL encryption.
4. Save the configuration.

NOTE

We recommend compatibility mode which supports:

- Encrypted communication between the components that support SSL
- Unencrypted communication between the components that do not support SSL

SSL settings are specific to each hub. Follow these steps in Admin Console to specify the SSL mode.

1. Navigate to the hub, and expand the local robot. Open the hub configuration UI.

2. On the **General** tab, click **Settings**, and go to the **SSL** tab.
3. Select a **Mode**:
 - **Normal**, communication occurs with no encryption. The OpenSSL transport layer is not used.
 - **Compatibility Mode** (recommended), enables encrypted or unencrypted communications. The components first attempt SSL communication, and switch to unencrypted communication when SSL is not supported.
 - **SSL Only** – SSL encryption only
4. Specify the **Cipher Type**.
5. Click **OK**. The hub propagates the SSL settings to the robots. The robots propagate the settings to the probes.

Follow these steps in Infrastructure Manager to specify the SSL mode.

1. Locate the hub probe.
2. Right-click the hub probe and select **Configure** to open the hub configuration window.
3. On the **General** tab, click **Settings**, and go to the **SSL** tab.
4. Select a **Mode**:
 - **Normal** – communication occurs with no encryption. The OpenSSL transport layer is not used.
 - **Compatibility Mode** (recommended) – Mixed Normal/SSL mode. The components first attempt SSL communication, and switch to unencrypted communication when SSL is not supported.
 - **SSL Only** – SSL encryption only
5. Specify the **Cipher Type**.
6. Click **OK**. The hub propagates the SSL settings to the robots. The robots propagate the settings to the probes.

Set Up Access to Operator Console (OC) Using a DMZ

As a system administrator, you enable secure communication through a proxy web server to set up access to Operator Console (OC) through a DMZ.

A DMZ limits your network vulnerability to unauthorized use or attack. External users have direct access only to the proxy web server in the DMZ and not your internal network.

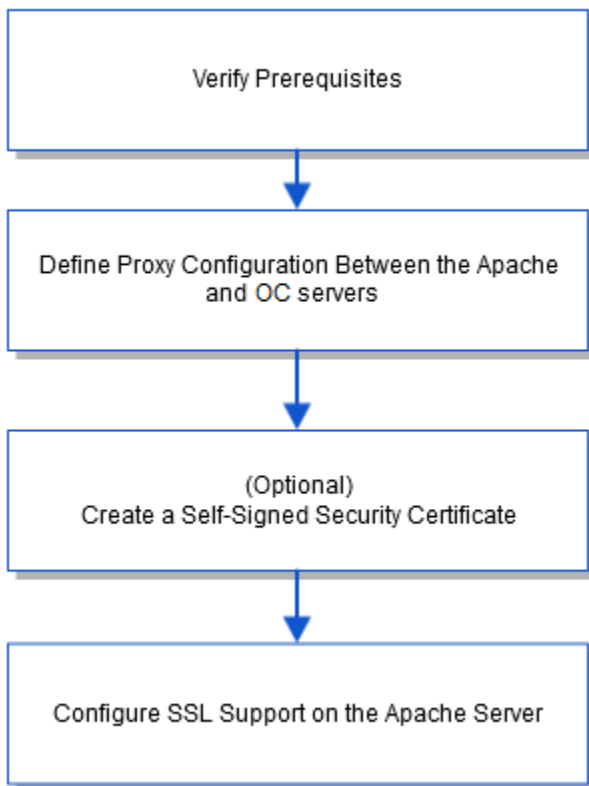
Contents

WARNING

The traffic that passes from the Apache 2 web server to the secure zone is insecure. Enabling https communication between the proxy server and Operator Console (OC) within your *internal* firewall is beyond the scope of this article. For more about how to configure https in this situation, see Apache documentation on the [mod_proxy_http module](#).

Configuration Overview

The following diagram shows the high-level steps for setting up access to Operator Console (OC) through a DMZ:



Verify Prerequisites

- Install CA Unified Infrastructure Management. Install Operator Console (OC) and ensure that it is communicating with the CA Unified Infrastructure Management server.
- Download and install Apache 2.
- Designate a public IP address for the Apache web server (if you want to access Operator Console (OC) from the Internet).

NOTE

By default AJP Connector will not start in UIM 20.3.0. To start the AJP Connector before configuring the DMZ, follow the below steps:

- Deactivate the wasp probe.
- Add below configuration with in setup tag of wasp.cfg
 - Location: File location ~ \Nimsoft\probes\service\wasp\wasp.cfg


```
<ajp_connector>
secretRequired = false
</ajp_connector>
```
- Activate the wasp probe.

Define Proxy Configuration between the Apache and Operator Console (OC) Servers

Configure proxy communication between the Apache proxy web server and Operator Console (OC) server so that external browsers can access Operator Console (OC) through the DMZ.

Follow these steps:

1. Edit the Apache configuration file, `httpd.conf`, as follows:

- a. Uncomment the following lines:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
```

- b. Locate: `#ServerName www.example.com`; uncomment and change it to:

```
ServerName <Apache_server_name>.<domain>.com:80
```

- a. Add the following lines to the end of the `httpd.conf` file:

```
ProxyRequests On
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
ProxyPass / ajp://<oc_server_name_orIP>:8009/
ProxyPass /c/portal ajp://<oc_server_name_orIP>:8009/c/portal
ProxyPass /web/guest ajp://<oc_server_name_orIP>:8009/web/guest
ProxyRequests Off
```

For example:

```
ProxyRequests On
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
ProxyPass / ajp://10.10.10.10:8009/
ProxyPass /c/portal ajp://10.10.10.10:8009/c/portal
ProxyPass /web/guest ajp://10.10.10.10:8009/web/guest
ProxyRequests Off
```

2. On the *inside* firewall, open Port 8009.
3. On the *outside* firewall, open Port 80

NOTE

(Optional) To allow internet access to a hub in the DMZ, you must assign a public IP address.

4. (Optional) If you want to enable *only* https access and disable standard http, you must do the following:
 - a. In the `http.conf`, comment out the following line

```
#Listen 80
```

- b. In the `ServerName` entry, specify port 443 instead of port 80.

WARNING

If you enable https access and do *not* disable http access, both http and https access are possible.

5. Restart the Apache server.
6. To test whether the Apache web server proxies you to the Operator Console (OC) login page, access the URL of the proxy server in your web browser.

Troubleshooting Proxy Configuration between the Apache and Operator Console (OC) Servers**Symptom:**

When you configure SSL using 64bit Apache on a Windows installation, Apache fails to start.

Solution:

Modify the SSLSessionCache path 'Program Files (x86)' portion:

```
SSLSessionCache "shmcb:C:/PROGRA~2/Apache Software Foundation/Apache2.2/logs/ssl_scache(512000) "
```

(Optional) Create a Self-Signed Certificate

You must have a security certificate to configure a secure connection between the proxy web server and web browsers. A certificate from a certificate authority ensures site visitors that any transferred data is more secure. If you do not transfer sensitive data and you are less concerned about security, create a self-signed certificate.

NOTE

Visitors see a warning that a trusted certificate authority did not issue the certificate but they can proceed to the website.

Follow these steps:

1. Open a command prompt on the web server.
2. Change directories:
C:\Program Files\Apache\conf
3. Generate a private key:
.. \bin\openssl genrsa -des3 -out server.key 1024
4. Generate a CSR (Certificate Signing Request):
.. \bin\openssl req -config .. \conf\openssl.cnf
-new -key server.key -out server.csr
5. Remove the passphrase from the key:
copy server.key server.key.org
.. \bin\openssl rsa -in server.key.org -out server.key
6. Generate a self-signed certificate:
.. \bin\openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
7. Edit httpd-ssl.conf to update paths to:
SSLCertificateFile and SSLCertificateKeyFile
You created a self-signed certificate.

Configure SSL Support on the Apache Server

Configure SSL support on the Apache server to establish an encrypted link between the web proxy server and external browsers

Follow these steps:

1. In the Apache configuration file, httpd.conf, uncomment the following lines:
LoadModule ssl_module modules/mod_ssl.so
Include conf/extra/httpd-ssl.conf
2. In the Apache configuration file conf/extra/httpd-ssl.conf, edit the following parameters:
 - **Listen port**
Identifies the port number that is opened on the inside firewall for SSL as required.

NOTE

You can use the netstat command to make sure that no other applications are using the port that you specify. If you use port 443 on an Internet Information Services (IIS) web server, this may be an issue.

- **VirtualHost**
Identifies the port number that is opened on the inside firewall for SSL. (Default value is 443.)
- **ServerName**

- Defines the name for the Apache server, including port number (for example: 10.10.10.10:443).
 - **ServerAdmin**
Defines the email address for the administrator.
 - **SSLCertificateFile**
Identifies the path to the PEM encoded certificate.
 - **SSLCertificateKeyFile**
Identifies the path to the private key if it is not already combined with the certificate.
3. In the Apache configuration file `conf/extra/httpd-ssl.conf`, accept the default or specify the desired path for the following parameters:
 - **DocumentRoot**
 - **SSLSessionCache**
 - **ErrorLog**
 - **TransferLog**
 - **CustomLog**
 4. Restart the Apache web server.
You configured SSL support on the Apache server.

Restrict Computer-Level (IP) Access to the CA UIM Database

You can restrict computer-level (IP) access to the UIM database through the Windows firewall. You do this by blocking certain IP addresses that must not be allowed to communicate with the UIM database. This ability helps you ensure that you install the UIM Server only on authorized computers. It prevents the UIM Server installation on unauthorized computers as the IP addresses of such computers are blocked.

Follow these steps:

1. Access the UIM database computer.
2. Enable the Windows firewall by selecting the private and public network settings on the UIM database computer:
 - a. Navigate to **Control Panel, System and Security, Windows Firewall, Customize Settings**.
 - b. Under **Private network settings**, enable the **Turn on Windows Firewall** option.
 - c. Under Public network settings, enable the **Turn on Windows Firewall** option.
3. Follow the steps outlined in the [How to Block Single IP Address or Range of IP Addresses from Windows Firewall 2008](#) article to restrict the IPs on the UIM database computer.
These steps let you specify the IP addresses that you want to block.

You have successfully restricted access to the UIM database from the specified IP addresses. If you try to install the UIM Server on any such computer, the installer displays an error message and does not allow the installation. An example of the error message, where Microsoft SQL Server is the UIM database, is as follows:

```
Failed to connect to database server with provided field values. Recheck fields for accuracy.
```

```
The TCP/IP connection to the host <IP address>, port 1433 has failed. Error: "Connection timed out: no further information. Verify the connection properties. Make sure that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port. Make sure that TCP connections to the port are not blocked by a firewall.
```

Deploy Your Monitoring Probes

After you have installed your CA UIM environment, you can deploy and configure your monitoring probes. This article describes some of the probes that you can deploy based on environment type.

Contents

WARNING

The purpose of this article is to act as a starting point before you begin deploying monitoring probes. This article does not contain a full list of all of the probes that are available as part of CA UIM. Contact your CA sales associate for a full probe list or specific recommendations for your environment.

Probe Documentation Links

You can view the documentation for individual probes on the [Probes TechDocs Space](#).

Probe Packs

Typically, probes are bundled into offerings called packs. Packs are solution-oriented sets of probes with licensing that varies by the pack type. Some examples of current pack types are:

- Server Pack
- Big Data Pack
- Server and Application Pack

WARNING

Probe packs are subject to change, contact your CA sales associate for an up-to-date list of the available probe packs.

Probes by Functional Area

This section lists probes by their functional area or use case.

Applications

The CA UIM solution contains a set of probes that you can use to determine whether your key applications are up and responsive.

| Probe Name | Description |
|--------------|---|
| apache | Remotely monitors Apache HTTP servers. |
| cisco_ucm | Manages the health and performance of your Call Manager systems and services. The cisco_ucm probe is able to monitor all performance counters and services (checkpoints) available on defined agents running the Cisco Unified CallManager. |
| cisco_unity | Manages the health and performance of your Unity systems and services. |
| iis | Monitors Microsoft IIS servers. |
| ica_response | Tests a Citrix terminal server client connection by executing the login and logout commands. The ica_response probe also enables you to launch an application or run a macro script. |
| jboss | Monitors JBoss Application Servers utilizing the JMX (jsr160) interface. |
| jvm_monitor | Monitors CPU, threads, and memory usage on Java Virtual Machines (JVM) |
| jmx | Monitors WebLogic Servers based on user-defined profiles. |
| easerver | Handles all common monitoring and data collection tasks for Sybase EAServer. |

| | |
|------------------|---|
| ecometer | Captures near real time data from IT and building infrastructure to provide a clear and comprehensive picture of power, cooling, energy use and other environmental variables. |
| ews_response | Tests Exchange Server mail response times by sending test e-mail messages and reading a mailbox. |
| lync_monitor | Monitors the health and performance of Microsoft Lync Server by gathering information about the performance of the server and the audio and video quality of network media. |
| notes_server | Monitors Lotus Notes servers. |
| notes_response | Monitors Notes servers from the client perspective. Alarm messages can be generated on availability, failover situations and response times. |
| ocs_monitor | Monitors the health and performance of Microsoft Office Communications Server by gathering information about the audio and video quality of network media. Additionally, the probe collects usage information (CDR) about Office Communications Server, which helps you to calculate the return on investment of your deployment and also enables you to plan future growth of your deployment. |
| sapbasis_agentil | CA UIM for SAP is developed and maintained by AGENTIL, and utilizes our monitoring infrastructure and reporting to give customers a unified view of SAP and datacenter performance. |
| sharepoint | Monitors Microsoft Sharepoint Server (both Sharepoint Services and Microsoft Office Sharepoint Server). |
| tomcat | Monitors Apache Tomcat servers using a JMX interface (jsr160). Apache Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. |
| weblogic | Handles all the common monitoring and data collection tasks on WebLogic Servers. |
| websphere | Handles all common monitoring and data collection tasks on IBM WebSphere Application Servers. |
| websphere_mq | Monitors Queue Manager, Queue and Channel on IBM MQ Series systems. |

Cisco UCS

The Cisco Unified Computing System is a next-generation data center platform that unites computing, networking, storage access, and virtualization into a cohesive system designed to reduce total cost of ownership (TCO) and increase business agility.

CA UIM supports several probes that you can use to monitor Cisco UCS.

| Probe Name | Description |
|------------|--|
| cisco_ucs | Remotely monitors Cisco UCS chassis series server blade systems. Monitoring availability metrics in terms of server blades present and their status and environmental metrics in terms of temperature, power, current of various parts of the UCS chassis. |
| cisco_nxos | Monitors Cisco NX/MDS devices. |

Cloud/SaaS

Cloud/SaaS probes include complete monitoring environments for those building a public or private cloud, as well as specific monitoring elements to monitor instances in cloud services such as Amazon, Rackspace, and Salesforce. The probes automate all common monitoring and data collection tasks.

| Probe Name | Description |
|-------------------|---|
| aws | Uses CloudWatch and other techniques to monitor Amazon Web Service Status, CloudWatch and EC2 and S3. |
| azure | Automatically discovers and monitors any number of Windows Azure role instances, including dynamic scaling. |
| cloudstack | Automates all common monitoring and data collection tasks for the Citrix Cloud Platform Powered by Apache CloudStack (Citrix Cloud Platform and Apache CloudStack). |
| google_app_engine | Monitors Google-published runtime and subsystem statuses that are available from http://code.google.com/status/appengine . The GAE probe is also capable of directly measuring the performance of the Java runtime and all subsystems through the use of the CA UIM GAE Plugin (NGaeP). |
| google_apps | Monitors the Google-published application statuses that are available from http://www.google.com/appsstatus . The google_apps probe is also capable of measuring and alarming on aspects of a specific domain. Google provides a set of domain reports from which the probe gathers metrics. The probe is also capable of performing various end-user operations, like creating a document, and measuring the latency of the operation. |
| rackspace | Monitors Rackspace IaaS offerings (called Cloud Servers) and Cloud Files (storage) integrated with the Limelight content delivery network (CDN). |
| salesforce | Monitors Salesforce availability and response times. |

Databases

Database probes monitor databases, associated applications, and user transactions to ensure high throughput and peak performance.

| Probe Name | Description |
|-------------------|--|
| cassandra_monitor | Monitors the internal performance and resource usage throughout a node in a Cassandra cluster. |
| db2 | Monitors IBM's DB2 UDB. |
| hadoop_monitor | Monitors the availability and performance of a Hadoop cluster. This includes hosts, nodes (named and secondary), HDFS, Hive, and other services. |
| informix | Monitors IBM Informix databases. |
| jdbc_response | Issues custom SQL statements against database servers utilizing the JDBC client interface for the purpose of measuring response time and data gathering. |
| mongodb_monitor | Monitors the internal performance and resource usage throughout a node in a MongoDB cluster. |
| mysql | Monitors MySQL database application servers. |

| | |
|---------------|---|
| oracle | Runs selected SQL statements to extract vital information about your Oracle servers. The information is presented to the database administrator as alarms and/or as a report. |
| oracle_logmon | Contains predefined watcher definitions for monitoring the Oracle Alert Log. This package is an extension to the logmon probe. |
| sqlserver | Monitors internal performance and space allocation throughout the SQL Server database and feeds essential information based on pre-defined criteria. |
| sql_response | Executes SQL queries (using ADO or ODBC connectivity) and evaluates response time, number of returned rows, and returned value. |
| sybase | Runs selected SQL to extract vital information about your Sybase servers. |
| sybase_rs | Monitors Sybase Replication Servers. |

Data Center Management (Power and Cooling)

Data center management probes monitor power and cooling for your server hardware.

| Probe Name | Description |
|------------|---|
| ecometer | Collects and monitors power and cooling data from devices using various protocols (SNMP, Modbus, BACnet, and EnergyWise). |

Response Time Monitoring

The Response Time Monitoring probes focus on collecting accurate response time information from all of critical locations.

| Probe Name | Description |
|----------------|---|
| dns_response | Queries Domain Name Servers and monitors their response times. It is possible to query the DNS for A records (normal hostnames), MX records (mail servers) and NS records (name servers). |
| sql_response | Monitors SQL databases by using ADO or ODBC connections to execute SQL queries and monitor SQL databases. The probe evaluates the result of the query (for example, response time, number of returned rows, and returned value) to generate alarms and QoS |
| ntp_response | Tests Network Time Protocol responses by requesting status information from the NTP server, or in the case of an SNTP server, requesting the current time. |
| e2e_appmon_dev | Creates customized NimRecorder scripts. Individual transactions can be timed and Quality of Service (QoS) messages can be sent from the script, as well as the total run time as measured by the probe itself. Finished scripts can be run by the e2e_appmon probe. |
| e2e_appmon | Runs pre-compiled NimRecorder scripts. Individual transactions can be timed and Quality of Service (QoS) messages can be sent from the script, as well as the total run time as measured by the probe itself. |

| | |
|---------------|--|
| url_response | Monitors the page download time for a URL. The url_response probe can also perform comparison checks on the page-contents. The url_response probe supports proxies and user authentication. The probe also supports QoS (Quality of Service) messages, directed towards the CA UIM SLA (Service Level Agreement) family. |
| webservicemon | Monitors the status of web services, including the ability to monitor responsiveness, status codes, SSL certificates and response validation. |

Directory and Email Servers

The directory and email server probes allow you to monitor server health and bandwidth.

| Probe Name | Description |
|------------------|--|
| ad_response | Monitors the availability of the Active Directory. |
| ad_server | Monitors selected counters on the Windows Active Directory. These counters measure the availability and response time for the active directory server. |
| adevl | Monitors Active Directly Event Logs. |
| email_response | Tests internet mail response by sending mail messages and reading a mailbox, using SMTP and pop3/imap. |
| exchange_monitor | Monitors Exchange Server health. |
| ews_response | Tests Exchange Server mail response times by sending test e-mail messages and reading a mailbox. |

Gateways

Gateway probes allow you to:

- Convert packets from one protocol to another
- Convert commands and/or data from one format to another
- Convert messages from one mail format to another

| Probe Name | Description |
|--------------|---|
| adogtw | Reads data from tables using user-defined SQL statements and posts messages and alarms into CA UIM. |
| ARCserve_D2D | Sends CA ARCserve D2D alerts and backup job status to CA UIM, where you can view the alerts within the CA UIM Operator Console (OC). You can also run CA ARCserve D2D commands such as full backup, incremental backup, and verify backup using the CA UIM Probe utility. |
| ARCserve_RHA | Sends RHA events to CA UIM. You can view these events as alerts within the Operator Console (OC). |
| casdgtw | Generates incidents in CA Service Desk. Incidents are generated when a CA UIM alarm is assigned to the designated CA Service Desk user. |
| cmdbgtw | Provides access to data residing in a CA UIM SLM database. The cmdbgtw probe is capable of exporting data from any table or set of tables. Data can be exported in either XML or CSV interchange formats. Exported data is written to files in a user-chosen location. |

| | |
|--------------|---|
| cuegtw | Integrates the alarms from an instance of CA UIM to an instance of CA UIM Cloud User Experience Monitor. |
| emailgtw | Receives messages with the subject EMAIL and sends them using SMTP protocol. The CA UIM Alarm Server (nas) can be set up to send alarms to the emailgtw probe. |
| file_adapter | Monitors the files defined in profiles. |
| hpsmgwtw | Generates incidents in the HP Service Manager (HPSM). Incidents are generated when a CA UIM alarm is assigned to the designated HPSM user. |
| jdbcgtw | Acts as a database gateway between CA UIM and a database. The Gateway reads data from tables using user-defined SQL statements and posts messages and alarms on the CA UIM bus. |
| nsdgtw | Generates incidents in Nimsoft Service Desk. Incidents are generated when a CA UIM alarm is assigned to the designated Nimsoft Service Desk user. |
| ovnm | Acts as a gateway between CA UIM and HP OpenView NNM. CA UIM Alarms are represented by dynamically created objects which can be used in Business Process Views. |
| remedygtw | Acts as a gateway for alarms into Remedy ARS. |
| smsgtw | Provides a means to send alerts/messages over the GSM digital cellular telephone networks. |
| sngtw | Generates incidents in ServiceNow. Incidents are generated when a CA UIM alarm is assigned to the designated ServiceNow user. |
| snmpgtw | Converts CA UIM alarm messages to SNMP Trap messages readable by any SNMP based event manager. A predefined set of profiles exist for transforming the CA UIM alarm message to some well-known event managers, like HP-OpenView, CA Service Operations Insight (CA SOI), and BMC CommandPost. |
| snmptd | Receives and converts SNMP traps into CA UIM alarms. |
| sysloggtw | Converts syslog messages from external devices into CA UIM alarms. |

IBM iSeries/AS400

IBM iSeries/AS400 probes allow for increased application visibility on the iSeries platform.

| Probe Name | Description |
|------------|---|
| diskstat | Monitors disks on the iSeries system. Alarm messages and performance metrics can be generated on a number of disk properties. |
| fetchmsg | Monitors an iSeries message queue. The fetchmsg probe enables handling of messages requiring operator response on the iSeries system. |
| jobqs | Monitors job queues on an iSeries system. |
| jobs | Monitors jobs on an iSeries system. |
| jobsched | Monitors scheduled jobs on an iSeries system. |
| journal | Monitors the journal messages on an iSeries computer hosting the probe. The QAUDJRN journal is configured to be monitored, and additional journals may be specified for monitoring. |

| | |
|---------|---|
| outqs | Monitors output queues on an iSeries system. Alarm messages can be generated there are too many entries in the output queue. The probe also supports QoS (Quality of Service) messages, directed towards the CA UIM SLA (Service Level Agreement) family. |
| history | Monitors history messages from the QHST logs on an iSeries system. |
| sysstat | Monitors iSeries systems statistics. |

Mainframe

Mainframe probes provide comprehensive end-to-end infrastructure visibility for business services that span mobile-to-mainframe environments.

| Probe Name | Description |
|------------|---|
| zops | Feeds metrics data from the z/OS operating system into CA UIM. |
| zstorage | Feeds metrics data for the mainframe storage environment into CA UIM. |
| zvm | Feeds metric data from the mainframe z/VM hypervisor into CA UIM. |

Network

Network probes provide complete network visibility and allow users to maintain the highest levels of business service quality.

| Probe Name | Description |
|-------------------|--|
| cisco_monitor | Monitors critical Cisco SNMP objects by using SNMP. |
| cisco_qos | Monitors Cisco devices supporting the Cisco Class-Based QoS MIB (cbQoS) by using SNMPv1/2c/3. |
| cisco_nxos | Monitors Cisco NX/MDS devices. |
| icmp | Tests network connectivity using ping and generates Quality of Service (QoS) messages based on the response data. |
| interface_traffic | Monitors network interface traffic. |
| net_connect | Measures network connectivity based on 'ping' (ICMP ECHO) and TCP connections to a list of user-defined services. |
| net_traffic | Measures network bandwidth usage in terms of packets per second, and bytes per second. You can profile network usage by defining your own profiles containing criteria such as source, destination (host/network) addresses, and port/service information. |
| snmpcollector | Provides next-generation SNMP collection capabilities within CA UIM. |
| pollagent | Enables SNMPCollector functionality. |
| snmptoolkit | Enables SNMP monitoring for any SNMP enabled device, with the specific ability to create monitoring templates for Table/Index heavy SNMP MIBS. |
| saa_monitor | Monitors Cisco devices supporting Service Assurance Agent (also known as IPSLA). |

Server

Server probes enable monitoring for your mission-critical server hardware.

| Probe Name | Description |
|------------|--|
| fsmounts | Monitors which file systems are mounted, and raises alarms when there are mismatches between what is currently mounted and what is configured on the system. |
| iostat | Collects disk activity statistics and metrics from the iostat command on Solaris, Linux and AIX servers. |
| ntevl | Generates alerts based on messages from the Windows event logs. |
| ntperf | Monitors performance counters on Windows. |
| ntservices | Monitors Windows services. The ntservices probe can report services not in the expected state and optionally start or stop them. |

Storage

Storage probes provide alarms and performance data that allow you to rapidly identify and correct storage related outages.

| Probe Name | Description |
|-----------------|--|
| clariion | Monitors EMC Clariion CX4 Storage systems using Navisphere CLI. |
| celerra | Monitors EMC Celerra Storage systems. |
| hitachi | Monitors Hitachi USP-V and USP-VM Series disk storage systems. |
| ibm-ds/ibm_ds4k | Monitors IBM DS3xxx and IBM DS4xxx storage arrays. |
| ibm_svc | Handles all common monitoring and data collection tasks for the IBM SAN Volume Controller. |
| netapp | Uses SNMP to communicate with storage arrays. |
| vmax | Monitors EMC Symmetrix Vmax storage systems. |

System

System probes point to computer systems and collect metrics.

| Probe Name | Description |
|------------|--|
| cdm | Monitors CPU, disk, and memory. |
| dirscan | Monitors files in specific directories. Alarms can be sent on number of files, age of files and space used by files. |
| logmon | Scans ASCII-based log files and looks for essential information in system and application log files. |
| nexec | Enables the CA UIM Alarm operator to execute a defined set of commands on a remote computer. |
| perfmon | Remotely fetches performance counter values from a set of Windows computers and makes these available for use by the cisco_unity, iis and exchange_monitor probes. |

| | |
|-----------|--|
| printers | Monitors printers defined on the computer. Remote printers are included when a user name/password is supplied for listing these. |
| processes | Monitors processes and windows owned by the processes to detect error situations. |
| reboot | Checks a configuration to determine if a reboot is needed and performs the reboot. |
| rsp | Monitors system metrics and collects performance data in an agentless manner without having to install proprietary software on the system. The probe gathers statistics on CPU utilization, disk and memory usage. |
| tcp_proxy | Allows a user to set up proxy connections to a set of defined TCP services, either locally or through an SSL tunnel. For example, this can be used to set up a Remote Desktop connection through a Firewall. |
| Xmlparser | Parses XML documents using xpath statements. The probe can take input from several sources, return result set to source for further processing or generate alarms, and QOS data directly from the probe. |

Virtualization

Virtualization probes automatically configure, deploy, and display monitoring for virtual infrastructure.

| Probe Name | Pack |
|--------------|---|
| applogic_mon | Monitors AppLogic Applications using the AppLogic MON Appliance APIs. The probe performs all discovery, monitoring, and data collection tasks on one or more MON Appliance targets. |
| applogic_ws | Monitors AppLogic Platform Grids using the AppLogic WS_API Appliance interface. The probe performs all discovery, monitoring and data collection tasks on one or more AppLogic Grid targets. |
| hyperv | Monitors Microsoft Hyper-V Servers. The probe collects and stores data and information from the monitored system at customizable intervals. |
| ibmvm | Monitors IBM PowerVM virtualization solutions. |
| pvs | Monitors Citrix provisioning services based Virtual Desktop Infrastructure (VDI) environments. The pvs probe automatically discovers virtual desktops, as well as hypervisor virtual machines that power the virtual desktops that may be using VMware vSphere, XenServer or hyper-v virtualization technologies. |
| rhev | Monitors RHEV environments. The rhev probe collects and stores information from the monitored RHEV environments including Data Centers, Host and VMs with various capacity and performance data at customizable intervals. |
| vcloud | Monitors virtual data centers, vCloud Director resources, and ESX environments. vApp networks, VLAN IDs, associated metrics can also be monitored with this probe. |
| vmware | Monitors VMware VC/ESX Servers. |

| | |
|------------|---|
| xendesktop | Monitors Citrix XenDesktop based Virtual Desktop Infrastructure (VDI) environments. The xendesktop probe automatically discovers virtual XenDesktops, as well as hypervisor virtual machines that power the virtual desktops. The probe communicates with the XenDesktop VDI environment using PowerShell commands and extracts key information for real-time monitoring. |
| xenserver | Monitors the health and performance of Virtualization solutions based on the XenServer open source project. |
| xenapp | Acts as a virtual user, exercising published applications and providing preemptive service level monitoring. The probe will remotely execute and measure the time required to open a Citrix ICA session, login to an application, and conduct any transaction. |
| zones | Monitors the health and performance of Solaris Zones virtualization-enabled systems. |

Bulk Probe Deployment with an XML File

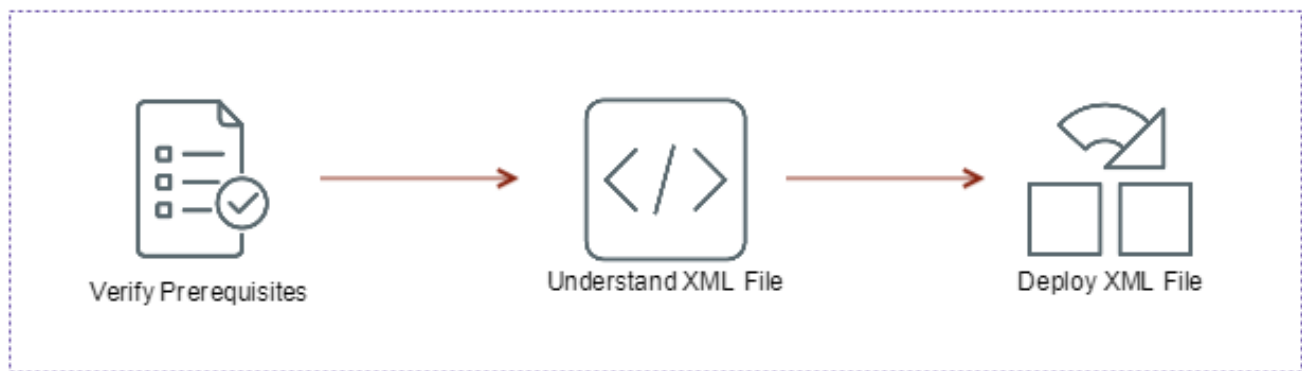
This article explains how to prepare an XML file to deploy probes in bulk. After the XML file is prepared, place it into the automatic_deployment_engine probe folder to process the file.

Contents

Process

The following diagram shows the overall process to deploy probes with an XML file:

Figure 10: Bulk Deployment of Probes with XML File



Bulk Deployment of Probes with XML File

Verify Prerequisites

Verify the following prerequisites before performing bulk deployment:

- Ensure that the probe is already downloaded in the archive.
- Ensure that the target robot is on the same UIM Server.
- Ensure that the target robot systems are supported. For supported software versions, see [Product Compatibility](#).

Understand the XML File

The following snippet shows an example of the XML file that you can use to deploy probes:

```
<hosts>
  <probe>
    <package>"Probe1 name"</package>
    <robot>"NimAddress for the robot"</robot>
  </probe>
  <probe>
    <package>"Probe2 name"</package>
    <robot>"NimAddress for the robot"</robot>
  </probe>
</hosts>
```

Required Attributes

The following table lists the attributes that are required when you deploy a probe:

| Attribute | Description |
|----------------|---|
| package | Specifies the name of the probe. For example, <code>cdm, processes</code> . |
| robot | Specifies the NimAddress for the robot. For example, <code>/domain/hub/robot</code> . |

Deploy the XML File

To deploy probes using `automated_deployment_engine`, copy the `host-profiles.xml` file into the `automated_deployment_engine` probe directory. By default this directory is:

- **Windows** — `C:\Program Files (x86)\Nimsoft\probes\service\automated_deployment_engine`
- **Linux, Solaris, AIX, and HP-UX** — `/opt/nimsoft/probes/service/automated_deployment_engine`

Once `host-profiles.xml` is updated, deployment begins automatically. After processing `host-profiles.xml`, `automated_deployment_engine` renames it as **host-profiles-YYYY-MM-DD_HH-mm-ss** to reflect the date and time of deployment. Renaming the file also ensures that if the `automated_deployment_engine` probe restarts, deployment does not automatically restart.

Deployment Notes

- The `automated_deployment_engine` probe cannot deploy robots from an unchanged `host-profiles.xml` file. To restart a distribution, remove the date and time from the file name and change the file size by a nominal amount (for example, edit the file and add an extra line). Deployment begins within 30 seconds of the change.

CA Business Intelligence with CA UIM

The CA Business Intelligence (CABI) dashboards within CA UIM use CA Business Intelligence JasperReports Server (CABI Server). CABI Server provides rich reporting and integrates in-memory analysis capabilities. The following table lists the software packages for a specific cabi probe version and type. The monitoring technology dashboard packages and report packages are required only when you monitor the specific technology.

NOTE

- After you install UIM 20.3.0, for any CABI related issues, see the [CABI troubleshooting](#) page.
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.
- Two different cabi probe packages are available from version 3.20. Choose the cabi probe that is appropriate for your environment.
- In an upgrade scenario, if you are upgrading CABI in a secure setup, ensure that you bring your CABI robot to the secure state by deploying the appropriate certificates and then updating the robot version to the secure version. After that, you upgrade CABI. For more information about the secure setup and how to deploy certificates, see [Secure Hub and Robot](#).

| Probe Package Options | Probe Description | CABI Packages | Monitoring Technology Dashboard Packages | Report Packages | CA UIM Version | Install and Upgrade Instructions |
|-----------------------|--|--|--|--|----------------|--|
| cabi version 4.30 | This probe configures CABI Server on a CA UIM robot. The CABI Server can only communicate with CA UIM. | <ul style="list-style-type: none"> • ump_cabi portlet version 4.21 • uim_core_dashboards_pack version 2.46 | <ul style="list-style-type: none"> • uim_aws_dashboards_pack version 2.40 • uim_azure_dashboards_pack version 2.40 • uim_sap_dashboards_pack version 1.00 • uim_citrix_dashboards_pack version 1.00 • uim_vmware_dashboards_pack version 1.1.1 • uim_mcs_dashboards_pack version 1.0.0 | <ul style="list-style-type: none"> • uim_aws_dashboards_pack version 1.04 • uim_azure_dashboards_pack version 1.31 • uim_sap_dashboards_pack version 1.00 | 20.3.0 | Install or Upgrade for a Bundled CA Business Intelligence JasperReports Server |
| cabi version 4.20 | This probe configures CABI Server on a CA UIM robot. The CABI Server can only communicate with CA UIM. | <ul style="list-style-type: none"> • ump_cabi portlet version 4.20 • uim_core_dashboards_pack version 2.45 | <ul style="list-style-type: none"> • uim_aws_dashboards_pack version 2.40 • uim_azure_dashboards_pack version 2.40 • uim_sap_dashboards_pack version 1.00 • uim_citrix_dashboards_pack version 1.00 • uim_vmware_dashboards_pack version 1.1.1 • uim_mcs_dashboards_pack version 1.0.0 | <ul style="list-style-type: none"> • uim_aws_dashboards_pack version 1.03 • uim_azure_dashboards_pack version 1.31 • uim_sap_dashboards_pack version 1.00 | 20.3.0 | Install or Upgrade for a Bundled CA Business Intelligence JasperReports Server |

| | | | | | | |
|----------------------------|--|---|--|--|---|--|
| cabi version 4.10 | This probe configures CABI Server on a CA UIM robot. The CABI Server can only communicate with CA UIM. | <ul style="list-style-type: none"> ump_cabi portlet version 4.10 uim_core_dashboards version 2.44 | <ul style="list-style-type: none"> uim_aws_dashboards version 2.40 uim_azure_dashboards version 2.40 uim_sap_dashboards version 1.00 uim_citrix_dashboards version 1.00 uim_vmware_dashboards version 1.1.1 uim_mcs_dashboards version 1.0.0 | <ul style="list-style-type: none"> boards_pack version 1.03 uim_cabi_health_report_pack version 1.31 uim_cabi_availability_report_pack version 1.00 | 0.2.0 | Install or Upgrade for a Bundled CA Business Intelligence JasperReports Server |
| cabi version 3.40 | This probe configures CABI Server on a CA UIM robot. The CABI Server can only communicate with CA UIM. | <ul style="list-style-type: none"> ump_cabi portlet version 3.40 uim_core_dashboards version 2.40 | <ul style="list-style-type: none"> uim_aws_dashboards version 2.40 uim_azure_dashboards version 2.40 uim_sap_dashboards version 1.00 uim_citrix_dashboards version 1.00 uim_vmware_dashboards version 1.0.0 uim_mcs_dashboards version 1.0.0 | <ul style="list-style-type: none"> boards_pack version 1.02 uim_cabi_health_report_pack version 1.31 | 0.0.2 (Apply the UMP 902 HF2 for CABI Task feature) | Install or Upgrade for a Bundled CA Business Intelligence JasperReports Server |
| cabi_external version 3.40 | This probe allows you to use a separate CABI Server instance. The CABI Server can communicate with CA UIM and other CA Agile Ops products. | <ul style="list-style-type: none"> ump_cabi portlet version 3.40 uim_core_dashboards version 2.40 | <ul style="list-style-type: none"> uim_aws_dashboards version 2.40 uim_azure_dashboards version 2.40 uim_sap_dashboards version 1.00 uim_citrix_dashboards version 1.00 uim_vmware_dashboards version 1.0.0 uim_mcs_dashboards version 1.0.0 | <ul style="list-style-type: none"> boards_pack version 1.02 uim_cabi_health_report_pack version 1.31 | 0.0.2 (Apply the UMP 902 HF2 for CABI Task feature) | Install or Upgrade for an External CA Business Intelligence JasperReports Server |
| cabi version 3.32 | This probe configures CABI Server on a CA UIM robot. The CABI Server can only communicate with CA UIM. | <ul style="list-style-type: none"> ump_cabi portlet version 3.32 uim_core_dashboards version 2.40 | <ul style="list-style-type: none"> uim_aws_dashboards version 2.40 uim_azure_dashboards version 2.40 uim_sap_dashboards version 1.00 uim_citrix_dashboards version 1.00 uim_vmware_dashboards version 1.0.0 uim_mcs_dashboards version 1.0.0 | <ul style="list-style-type: none"> boards_pack version 1.02 uim_cabi_health_report_pack version 1.31 | 0.0.2 | Install or Upgrade for a Bundled CA Business Intelligence JasperReports Server |

| | | | | | | |
|----------------------------|--|--|--|--|-------|--|
| cabi_external version 3.32 | This probe allows you to use a separate CABI Server instance. The CABI Server can communicate with CA UIM and other CA Agile Ops products. | <ul style="list-style-type: none"> ump_cabi portlet version 3.32 uim_core_dashboards_pack version 2.40 | <ul style="list-style-type: none"> uim_aws_dashboards_pack version 2.40 uim_azure_dashboards_pack version 2.40 uim_sap_dashboards_pack version 1.00 uim_citrix_dashboards_pack version 1.00 uim_vmware_dashboards_pack version 1.0.0 uim_mcs_dashboards_pack version 1.0.0 | boards_packified_report_pack version 1.02 cabihealth_report_pack version 1.31 | 6.0.2 | Install or Upgrade for an External CA Business Intelligence JasperReports Server |
| cabi_external version 3.30 | This probe allows you to use a separate CABI Server instance. The CABI Server can communicate with CA UIM and other CA Agile Ops products. | <ul style="list-style-type: none"> ump_cabi portlet version 3.30 uim_core_dashboards_pack version 2.40 | <ul style="list-style-type: none"> uim_aws_dashboards_pack version 2.40 uim_azure_dashboards_pack version 2.40 uim_sap_dashboards_pack version 1.00 uim_citrix_dashboards_pack version 1.00 uim_vmware_dashboards_pack version 1.0.0 uim_mcs_dashboards_pack version 1.0.0 | boards_packified_report_pack version 1.02 cabihealth_report_pack version 1.30 | 6.0.2 | Install or Upgrade for an External CA Business Intelligence JasperReports Server |
| cabi version 3.30 | This probe configures CABI Server on a CA UIM robot. The CABI Server can only communicate with CA UIM. | <ul style="list-style-type: none"> ump_cabi portlet version 3.30 uim_core_dashboards_pack version 2.40 | <ul style="list-style-type: none"> uim_aws_dashboards_pack version 2.40 uim_azure_dashboards_pack version 2.40 uim_sap_dashboards_pack version 1.00 uim_citrix_dashboards_pack version 1.00 uim_vmware_dashboards_pack version 1.0.0 uim_mcs_dashboards_pack version 1.0.0 | boards_packified_report_pack version 1.02 cabihealth_report_pack version 1.30 | 6.0.2 | Installing and Upgrading CA Business Intelligence JasperReports Server with CA UIM |
| cabi version 3.20 | This probe configures CABI Server on a CA UIM robot. The CABI Server can only communicate with CA UIM. | <ul style="list-style-type: none"> ump_cabi portlet version 3.20 uim_core_dashboards_pack version 2.40 | <ul style="list-style-type: none"> uim_aws_dashboards_pack version 2.40 uim_azure_dashboards_pack version 2.40 uim_sap_dashboards_pack version 1.00 uim_citrix_dashboards_pack version 1.00 | boards_packified_report_pack version 1.02 cabihealth_report_pack version 1.20 | 6.5.4 | Installing and Upgrading CA Business Intelligence JasperReports Server with CA UIM |
| cabi_external version 3.20 | This probe allows you to use a separate CABI Server instance. The CABI Server can communicate with CA UIM and other CA Agile Ops products. | <ul style="list-style-type: none"> ump_cabi portlet version 3.20 uim_core_dashboards_pack version 2.40 | <ul style="list-style-type: none"> uim_aws_dashboards_pack version 2.40 uim_azure_dashboards_pack version 2.40 uim_sap_dashboards_pack version 1.00 uim_citrix_dashboards_pack version 1.00 | boards_packified_report_pack version 1.02 cabihealth_report_pack version 1.20 | 6.5.4 | Install or Upgrade for an External CA Business Intelligence JasperReports Server |

NOTE

The UIM Server installer creates a .pem file (certificate.pem) in the <Nimsoft>\security folder. The .pem file is a symmetric key that is shared with the required robots, which is then used for communication with the data_engine probe. You copy this .pem file to the remote OC and CABI robots and provide the location of the file in the robot.cfg file (cryptkey = <.pem file location>). Furthermore, if any impacted probe is not on the same computer where data_engine is present, copy the generated .pem file to the robot computer (where data_engine is not available) and update the robot.cfg file with the .pem file location on that computer. For more information about the robot.cfg file configuration, see [Configure the robot.cfg File](#).

NOTE

1. The cabi 4.3 probe supports TLS 1.2 except if the Microsoft SQL Server 2012, 2014, 2016 database is installed on Windows Server 2016.
2. The cabi 4.10 probe supports TLS v1.2 when communicating with the UIM databases: Microsoft SQL Server - 2012, 2014, 2016 and Oracle - 11.2 and 12.1. However, CABI is not supported if Microsoft SQL Server 2012, 2014, or 2016 is installed on Windows Server 2016 and TLS v1.2 is enabled. Note that UIM 20.1 (and later) do not support Oracle 11.2.
3. The cabi 3.40 probe, available with UMP 9.0.2 HF2, supports TLS v1.2 when communicating with the UIM database: Microsoft SQL Server- 2012, 2014, and Oracle - 12.1. However, CABI is not supported if Microsoft SQL Server 2012 or 2014 is installed on Windows Server 2016 and TLS v1.2 is enabled. For more information about how to apply the UMP 9.0.2 HF2 for CABI TLS functionality, see [UMP 9.0.2 HF2](#). Note that UIM 20.1 (and later) do not support Oracle 11.2
4. The cabi 3.32 probe does not support TLS v1.2 when communicating with the UIM database: Microsoft SQL Server or Oracle. As a result, you cannot view the Operator Console home page, OOTB CABI dashboards, and OOTB CABI reports.
5. TLS v1.2 support is not enabled by default when you install CA UIM 9.0.2.

CABI Support Matrix

This section highlights the compatibility for the CABI and the UIM versions.

| CABI Version | Supported CABI Version for Upgrade | Released with UIM Version | Minimum UIM Version Supported |
|--------------|------------------------------------|---------------------------|-------------------------------|
| 4.30 | 3.40, 4.10, 4.20 | 20.3.0 | 20.3.0 |
| 4.20 | 3.32, 3.40, 4.10 | 20.1.0 | 20.1.0 |
| 4.10 | 3.32, 3.40 | 9.2.0 | 9.2.0 |
| 3.40 | 3.32 | 9.0.2 SP1 (9.1.0) | 9.0.2 |
| 3.32 | | 9.0.2 | 9.0.2 |

UIM CABI Compatibility Matrix

| UIM Version | Supported CABI Versions |
|-------------------|-------------------------|
| 20.3.0 | 4.20, 4.30 |
| 20.1.0 | 4.10, 4.20 |
| 9.2.0 | 4.10 |
| 9.0.2 SP1 (9.1.0) | 3.32, 3.40 |
| 9.0.2 | 3.32, 3.40 |

The CABI probe version is dependent on the UIM version. Therefore, in some cases, upgrading CABI requires you to upgrade the UIM environment as well.

For example, if you are on UIM 9.0.2 with CABI 3.32 and want to upgrade to UIM 20.3.0 with CABI 4.30, you can follow this path:

1. Upgrade UIM 9.0.2 to 20.3.0.
2. Upgrade CABI 3.32 to 4.20 because you cannot directly upgrade from 3.3.2 to 4.30.
3. Upgrade CABI 4.20 to 4.30.

NOTE

More Information:

- [CA Business Intelligence JasperReports Server with CA UIM Release Notes](#)
- [CA Business Intelligence Dashboards](#)
- [Extend your CA Products with Unified Dashboards and Reporting for Infrastructure Management](#)

Installing and Upgrading CA Business Intelligence JasperReports Server with CA UIM

The CA Business Intelligence (CABI) dashboards within CA UIM use CA Business Intelligence JasperReports Server (CABI Server). CABI Server provides rich reporting and integrates in-memory analysis capabilities. The dashboards are not available by default when you install CA UIM. You must install CABI Server.

NOTE

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

The type of cabi probe you deploy determines the type of CABI Server deployment. The two deployment options are:

- **Bundled CABI Server** - The **cabi probe** configures CABI Server to communicate only with CA UIM. This mode installs a CABI Server instance on a robot and simplifies the CABI Server installation process.
- **External CABI Server** - The **cabi_external probe** allows a separate CABI Server instance to communicate with CA UIM and other CA Agile Central products. If you previously deployed a bundled CABI Server, a migration process exists. This configuration allows you to reduce the number of CABI Server instances that you must deploy and maintain.

NOTE

You must determine which installation is most appropriate for your environment.

Before you upgrade, we recommend you to back up the CABI content by following steps 1 to 5 under *Migrate Custom Content* section in the [Migrate from Bundled to External Configuration](#) topic.

Installing or Upgrading of the CABI should be done by the user account with administrative privileges on all databases.

Before upgrading the CABI Server, the password for "superuser" account must be set to the default.

Before upgrading the CABI probe, remove the existing packages from the folder "../Nimsoft/probes/service/cabi/content/installed" to deploy the latest packages.

Install or Upgrade for a Bundled CA Business Intelligence JasperReports Server

There are two possible deployment paths for CA Business Intelligence JasperReports Server (CABI Server). This article describes a bundled CABI server deployment.

The bundled deployment installs and configures an instance of CABI Server on a robot. This configuration simplifies the CABI Server installation process if you only need to use a CABI Server instance with CA UIM. You *cannot* use this CABI Server instance with other CA Agile Operations products.

WARNING

- **Warning!** During the cabi probe package deployment, wasp restarts on the robot with CABI Server. The deployment can take approximately 20 to 30 minutes to complete. **Do not attempt to restart wasp before the deployment is complete.** If you try to restart wasp before the deployment is complete, CABI Server will not install successfully.
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

Contents

Software Requirements

The following table lists the minimum required software. For a matrix of software versions for a specific release, see [CA Business Intelligence with CA UIM](#).

| Software | Download | Notes |
|---|--|--|
| CA Business Intelligence JasperReports Server for Unified Dashboards and Reporting for Infrastructure Management | N/A | Installed by the cabi probe. |
| CA UIM | support.broadcom.com , Download Management | A CA support login is required. |
| cabi probe | support.nimsoft.com , Archive | Add to the CA UIM archive. A CA support login is required to download. |
| ump_cabi portlet | support.nimsoft.com , Archive | Add to the CA UIM archive. A CA support login is required to download. |
| uim_core_dashboards_pack | support.nimsoft.com , Archive | Add to the CA UIM archive. A CA support login is required to download. |
| Report packages: <ul style="list-style-type: none"> • uim_unified_reporter_pack • uim_cabi_health_report_pack | support.nimsoft.com , Archive | Add to the CA UIM archive. A CA support login is required to download. |

| | | |
|--|--|--|
| Dashboard packages: uim_<technology_name>_dashboards_pack | support.nimsoft.com , Archive | Add the appropriate dashboard packages to the CA UIM archive. A CA support login is required to download. The dashboard packages are only required if you need to view data for the specific technology. For example, the uim_aws_dashboards_pack dashboard package is only required if you must view data for your AWS environment. For a list of available dashboard packages, see CA Business Intelligence with CA UIM . |
|--|--|--|

Environment Requirements

This process requires the following environment:

- A CA UIM instance. For information about installation, see:
 - [Release Notes](#)
 - [Install UIM Server](#)
 - [Install the Operator Console \(OC\)](#)
- [Download, update, or import](#) the following packages to the Archive:
 - cabi probe
 - cabi portlet
 - dashboard packages
 - report packages
- A dedicated robot on the primary hub if a robot without OC does not exist. For more information, see the [Deploy Robots](#) article.
- (Optional) Secure Hub and Robot - The secure hub and robot provide robust hub-to-hub and robot-to-hub communication. To upgrade CABI in a secure setup, upgrade the CABI robot to a secure setup and then perform the CABI upgrade. For more information about the secure setup and how to deploy certificates, see [Secure Hub and Robot](#).
- **(MySQL Only)** If you are using MySQL for your CA UIM database, change the following default settings for your MySQL database so that the CA Business Intelligence dashboard deployment is successful:
 - Set **max_allowed_packet=500M**
 - Set **innodb_log_file_size=356M**
 - Set **table_definition_cache=2000**

NOTE

If you have a replication server configuration, the variable "gtid-mode" should be set to "OFF" and the variable "enforce-gtid-consistency" should be set to "0" in my.cnf or my.ini configuration as below:

```
gtid-mode=off
enforce-gtid-consistency=0
```

NOTE

Your dashboards import fails if the above-recommended settings are not updated for MySQL.

- **(Microsoft SQL Server Windows Authentication Only)** If you are using Microsoft SQL Server Windows Authentication, the CABI Server robot, and OC robot must have Windows operating systems. There are no requirements for matching operating systems if you are NOT using Microsoft SQL Server Windows Authentication.

Hardware Requirements for CABI Server

Ensure that your robot for CABI Server meets the following minimum hardware requirements:

- 10-GB free disk space
- 8-GB memory
- Four 2-GHz CPUs

JasperServer, Bundled CABI, and UIM Server Version Matrix

The following table shows the JasperServer, Bundled CABI, and UIM Server version matrix:

| JasperServer Version | Bundled CABI Version (probe) | UIM Server Version |
|----------------------|------------------------------|--------------------|
| 7.5 | 4.30 | 20.3 |
| 7.1.1 | 4.20 | 20.1 |
| 7.1.1 | 4.10 | 9.20 |
| 6.4.3 | 3.40 | 9.0.2 SP1 (9.1.0) |
| 6.3.0 | 3.32 | 9.0.2 |
| 6.3.0 | 3.20 | 8.51 |

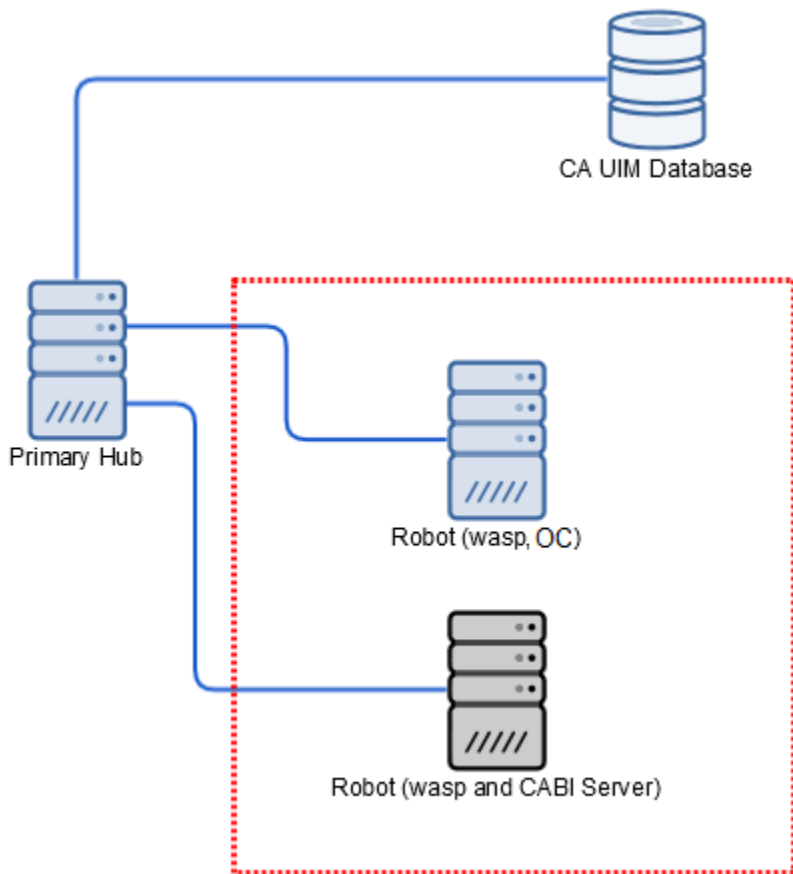
Deployment Configuration for CABI Server in a CA UIM Environment

Install CABI Server on a robot that is connected directly to the primary hub. **Do not deploy CABI Server on a robot running OC or on a secondary hub.** The separate robot is required to avoid scale and performance issues. CABI Server is deployed through the cabi probe.

WARNING

Do not install CABI server on a robot that is connected to a secondary hub or on a robot running OC. These configurations are not supported.

The following figure shows the supported deployment configuration to add CABI to a CA UIM environment.

Figure 11: CA UIM with CABI Deployment Diagram

High-Level Deployment Steps

This section includes high-level deployment steps that help you quickly understand the overall process. For detailed information about specific scenarios, you can review the appropriate sections in this article.

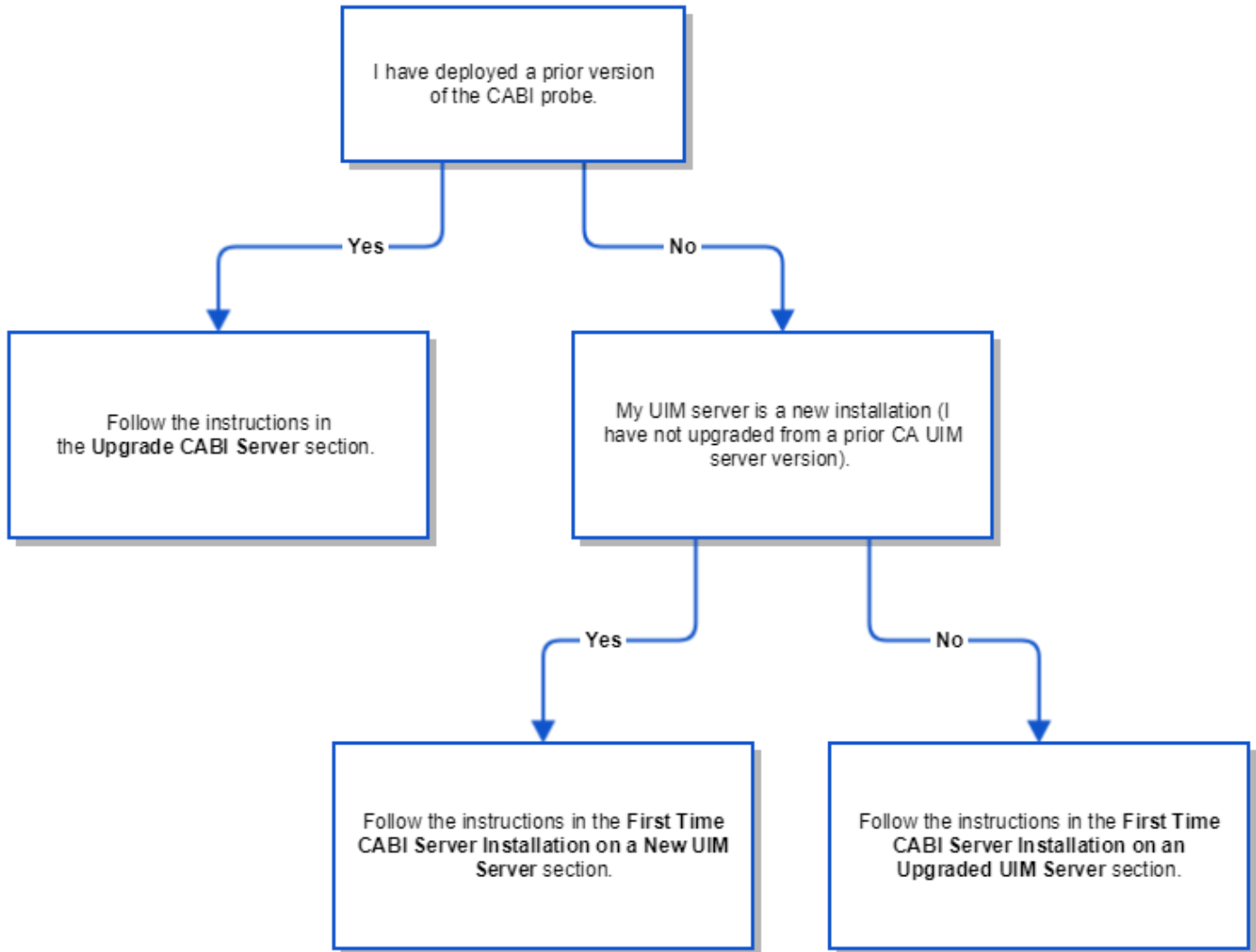
Follow these steps:

1. Install wasp to the CABI server.
2. Verify that wasp runs with a port and PID.
 - Your certificate.pem file must be in place and must be referenced in the robot.cfg file.
3. Edit the wasp configuration with the correct data_engine path (/domain/primaryhub/primaryhubrobot/data_engine).
4. Allow wasp to restart.
 - Verify the port and PID. Also, check that the wasp.log file does not contain any error.
5. Deploy the CABI probe to the CABI server.
6. Deploy the following packages to the CABI server:
 - uim_unified_reporter_pack
 - uim_cabi_health_report_pack
 - uim_core_dashboards_pack
7. Deploy the ump_cabi package to the OC server.

Determine Deployment Process

Use the following flowchart to determine which deployment process is required for your CA UIM environment.

Figure 12: cabi flow



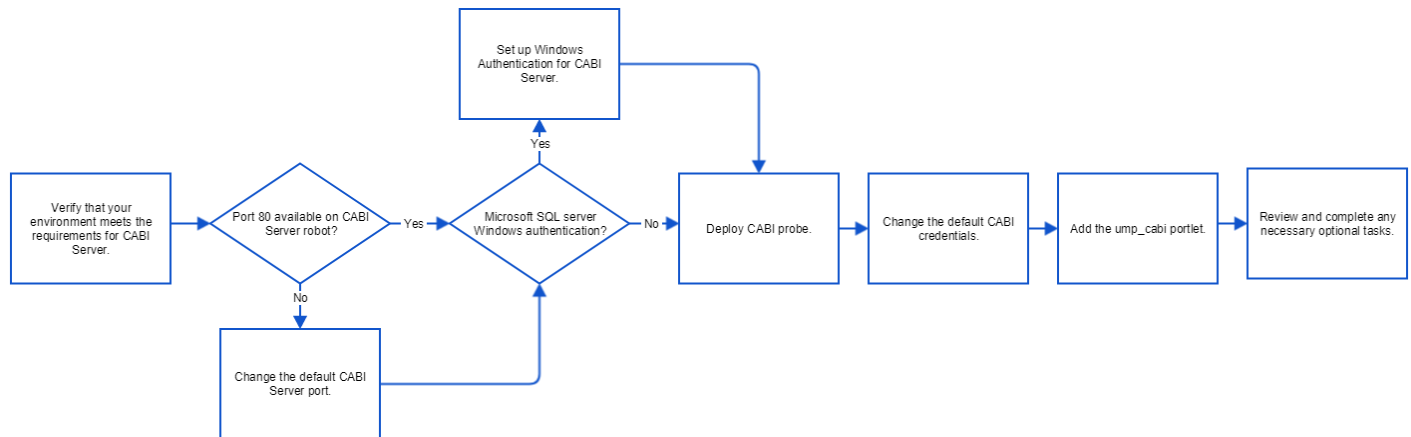
First Time CABI Server Installation on a New UIM Server

Use this procedure to install a new CABI Server in a new CA UIM environment.

Process Overview

The following diagram shows the sequence of tasks to complete.

Figure 13: New Install Flow CABI



(Optional) Change the Default CABI Server Port

Only follow these steps if port 80 is not available on the robot, or a non-standard http port is desired. Use the following steps to change the default CABI server port value.

1. Deploy wasp to the CABI Server robot if wasp is not currently installed.
2. Edit the wasp probe on the CABI Server robot using Raw Configure.
3. Select setup
4. Edit the http_port key value and update your configuration. A "Failed to restart probe" error message appears.
5. Select **Cancel** to close the window.
6. **Do NOT restart wasp.** The cabi probe installation restarts wasp.
7. Verify your change in raw configure for wasp.

(Microsoft SQL Server Windows Authentication Only) Set up Windows Authentication for CABI

WARNING

If you are using Microsoft SQL Server with Windows authentication, CABI cannot function until you configure Windows authentication on the CABI Server. Windows authentication must be set up in CA UIM, OC, and CABI.

Follow these steps:

1. On the robot for CABI Server, go to **Administrative Tools > Services** and double-click on **Nimsoft Robot Watcher**.
2. Select the **Log On** tab.
3. Change the account to the same account and password that is used in the **data_engine** and the primary UIM server.
4. Click **OK**.
5. Right-click on **Nimbus Robot Watcher** and select the **Restart** option.
6. Close the windows.
7. Restart the CABI Server robot.

Deploy the cabi Probe

During deployment, the cabi probe installs and configures an instance of CABI Server on a robot.

NOTE

The UIM Server installer creates a .pem file (certificate.pem) in the <Nimsoft>\security folder. The .pem file is a symmetric key that is shared with the required robots, which is then used for communication with the

data_engine probe. You copy this .pem file to the remote OC and CABI robots and provide the location of the file in the robot.cfg file (cryptkey = <.pem file location>). Furthermore, if any impacted probe is not on the same computer where data_engine is present, copy the generated .pem file to the robot computer (where data_engine is not available) and update the robot.cfg file with the .pem file location on that computer. For more information about the robot.cfg file configuration, see [Configure robot.cfg](#).

Follow these steps:

1. Verify that the cabi probe, uim_core_dashboards_pack, and report packages are in the archive.
2. Deploy the cabi probe package on a robot. The probe automatically deploys any package dependencies that exist in the archive. For example, the uim_core_dashboards_pack and report packages. For more information about how to deploy a probe package, see the [Deploy Packages](#) article.

WARNING

Warning! During the cabi probe package configuration, wasp restarts on the robot with CABI Server. The deployment can take approximately 20 to 30 minutes to complete. **Do not attempt to restart wasp before the deployment is complete.** If you try to restart wasp before the deployment is complete, CABI Server will not install successfully.

3. Verify that the CABI installation is complete. The cabi probe might be active, but the installation process might not be complete. Go to the cabi probe log file and look for the following messages:


```
<date_time> [main, cabi] cabi installed successfully.
...
<date_time> [UserSynchronizationThread, cabi] Finished synchronizing users between UIM and CABI
```

During installation, the cabi probe uploads the DataSource, domain, topic, and users. The uim_core_dashboards_pack and report packages are also deployed with the probe.

The wasp probe automatically starts when the process is complete.

Change the Default CABI Credentials

A default superuser account exists in CABI Server. You must change the credentials to maintain system security. You can use the superuser account to manage server settings.

WARNING

Change the default username and password as soon as possible to maintain system security.

Follow these steps:

1. Enter in a browser: **http://<CABI_Server_IP or hostname>:<port>/cabijs**
Where <port> is the port for the robot running wasp and CABI Server. The default port number is 80. For example, http://12.123.123.12:80/cabijs.
2. Enter the default username and password for CABI Server. The default username and password is superuser.
3. Select Manage, Users to view the Users list.
4. Select and edit the superuser entry to change the password.

Deploy the ump_cabi Portlet

Use this procedure to deploy the ump_cabi portlet package to view the predefined CABI dashboards in OC.

Follow these steps:

1. On the robot running OC, deploy the most current version of the ump_cabi package.
2. Verify that you can view the predefined dashboards. Go to the **Dashboards** in the left navigation of the Operator Console (OC) and select a CA Business Intelligence dashboard. For example, **Infrastructure Management Overview**.

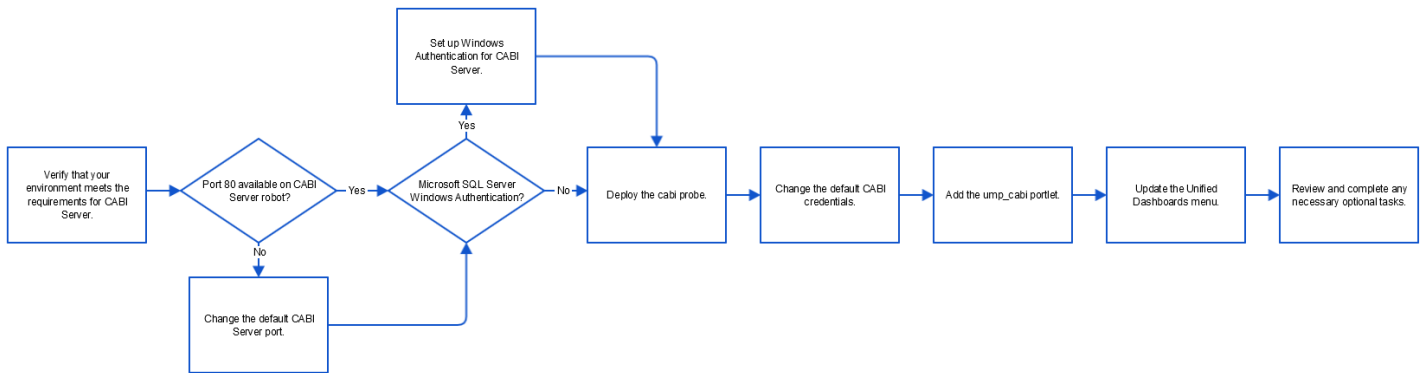
First Time CABI Server Installation on an Upgraded UIM Server

These instructions detail how to deploy CABI Server into an Upgraded CA UIM environment for the first time.

Process Overview

The following diagram shows the sequence of tasks to complete.

Figure 14: CABI Process flow - new server on upgrade UIM



(Optional) Change the Default CABI Server Port

Only follow these steps if port 80 is not available on the robot, or a non-standard http port is desired. Use the following steps to change the default CABI server port value.

1. Deploy wasp to the CABI Server robot if wasp is not currently installed.
2. Edit the wasp probe on the CABI Server robot using Raw Configure.
3. Select setup
4. Edit the http_port key value and update your configuration. A "Failed to restart probe" error message appears.
5. Select **Cancel** to close the window.
6. **Do NOT restart wasp.** The cabi probe installation restarts wasp.
7. Verify your change in raw configure for wasp.

(Microsoft SQL Server Windows Authentication Only) Set up Windows Authentication for CABI

WARNING

If you are using Microsoft SQL Server with Windows authentication, CABI cannot function until you configure Windows authentication on the CABI Server. Windows authentication must be set up in CA UIM, OC, and CABI.

Follow these steps:

1. On the robot for CABI Server, go to **Administrative Tools > Services** and double-click on **Nimsoft Robot Watcher**.
2. Select the **Log On** tab.
3. Change the account to the same account and password that is used in the **data_engine** and the primary UIM server.
4. Click **OK**.
5. Right-click on **Nimbus Robot Watcher** and select the **Restart** option.
6. Close the windows.
7. Restart the CABI Server robot.

Deploy the cabi Probe

During deployment, the cabi probe installs and configures an instance of CABI Server on a robot.

NOTE

The UIM Server installer creates a .pem file (certificate.pem) in the <Nimsoft>\security folder. The .pem file is a symmetric key that is shared with the required robots, which is then used for communication with the data_engine probe. You copy this .pem file to the remote OC, and CABI robots and provide the location of the file in the robot.cfg file (cryptkey = <.pem file location>). Furthermore, if any impacted probe is not on the same computer where data_engine is present, copy the generated .pem file to the robot computer (where data_engine is not available) and update the robot.cfg file with the .pem file location on that computer. For more information about the robot.cfg file configuration, see [Configure robot.cfg](#).

Follow these steps:

1. Verify that the cabi probe, uim_core_dashboards_pack, and report packages are in the archive.
2. Deploy the cabi probe package on a robot. For more information about how to deploy a probe package, see the [Deploy Packages](#) article.

WARNING

Warning! During the cabi probe package deployment, wasp restarts on the robot with CABI Server. The deployment can take approximately 10 to 20 minutes to complete. **Do not attempt to restart wasp before the deployment is complete.** If you try to restart wasp before the deployment is complete, CABI Server will not install successfully.

3. Verify that the CABI Server installation is complete. The cabi probe might be active, but the installation process might not be complete. Go to the cabi probe log file and look for the following messages:

```
<date_time> [main, cabi] cabi installed successfully.
```

```
...
```

```
<date_time> [UserSynchronizationThread, cabi] Finished synchronizing users between UIM and CABI
```

During installation, the cabi probe uploads the DataSource, domain, topic, and users. The uim_core_dashboards_pack and report packages are also deployed with the probe. The wasp probe automatically starts when the process is complete.

Change the Default CABI Credentials

A default superuser account exists in CABI Server. You must change the credentials to maintain system security. You can use the superuser account to manage server settings.

WARNING

Change the default username and password as soon as possible to maintain system security.

Follow these steps:

1. Enter in a browser: **http://<CABI_Server_IP or hostname>:<port>/cabijs**
Where <port> is the port for the robot running wasp and CABI Server. The default port number is 80. For example, http://12.123.123.12:80/cabijs.
2. Enter the default username and password for CABI Server. The default username and password is superuser.
3. Select Manage, Users to view the Users list.
4. Select and edit the superuser entry to change the password.

Deploy the ump_cabi Portlet

Use this procedure to deploy the ump_cabi portlet package to view the predefined CABI dashboards in OC.

Follow these steps:

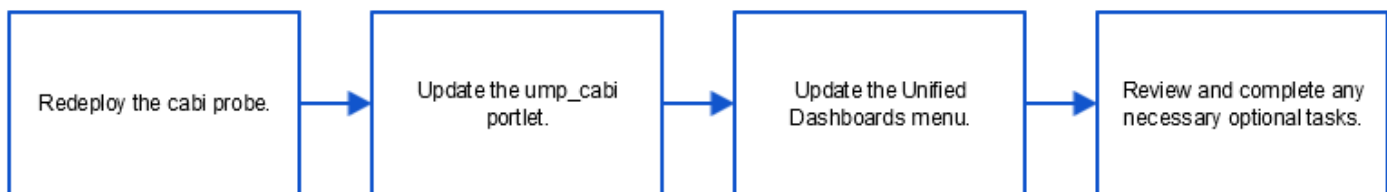
1. On the robot running OC, deploy the most current version of the `ump_cabi` package.
2. Verify that you can view the predefined dashboards. Go to the **Dashboards** menu in the left navigation of the Operator Console (OC) and select a CA Business Intelligence dashboard. For example, **Infrastructure Management Overview**.

Upgrade CABI Server

The instructions in this section are for users that have already deployed CABI Server and want to complete an upgrade.

Process Overview

The following diagram shows the sequence of tasks to complete.

Figure 15: cabi process flow - upgrade**NOTE**

In an upgrade scenario, if you are upgrading CABI in a secure setup, ensure that you bring your CABI robot to the secure state by deploying the appropriate certificates and then updating the robot version to the secure version. After that, you upgrade CABI. For more information about the secure setup and how to deploy certificates, see [Secure Hub and Robot](#).

NOTE

If you are using any older version of CABI that is prior to 3.40, you must first upgrade to CABI 3.40 or 4.10 or 4.20 and then you can upgrade to CABI 4.30.

NOTE

Always take a back-up of the custom reports (if any) before upgrading the CABI Server.

Change the CABI Credentials

Before you upgrade the cabi probe, ensure that you change the password of the superuser to the default password, which is superuser. You can then upgrade the cabi probe.

Follow these steps:

1. Enter in a browser: **http://<CABI_Server_IP or hostname>:<port>/cabijs**
Where **<port>** is the port for the robot running wasp and CABI Server. The default port number is 80. For example, `http://12.123.123.12:80/cabijs`.
2. Enter the credentials for CABI Server.
3. Select Manage, Users to view the Users list.
4. Select and edit the superuser entry to change the password to superuser.

After successful completion of the cabi probe upgrade, you can change the default password based on your requirements by following the above steps.

Redeploy the cabi Probe

To upgrade CABI Server, redeploy the latest version of the cabi probe.

NOTE

The UIM Server installer creates a .pem file (certificate.pem) in the <Nimsoft>\security folder. The .pem file is a symmetric key that is shared with the required robots, which is then used for communication with the data_engine probe. You copy this .pem file to the remote OC and CABI robots and provide the location of the file in the robot.cfg file (cryptkey = <.pem file location>). Furthermore, if any impacted probe is not on the same computer where data_engine is present, copy the generated .pem file to the robot computer (where data_engine is not available) and update the robot.cfg file with the .pem file location on that computer. For more information about the robot.cfg file configuration, see [Configure robot.cfg](#).

Follow these steps:

1. Verify that the cabi probe, uim_core_dashboards_pack, and report packages are in the archive.
2. Deploy the latest cabi probe package to the location of your existing cabi probe.
For more information about how to deploy a probe package, see the [Deploy Packages](#) article.

WARNING

Warning! During the cabi probe package deployment, wasp restarts on the robot with CABI Server. The deployment can take approximately 10 to 20 minutes to complete. **Do not attempt to restart wasp before the deployment is complete.** If you try to restart wasp before the deployment is complete, CABI Server will not install successfully.

3. Verify that the CABI Server installation is complete. Go to the cabi probe log file and look for the following message:
<date_time> [main, cabi] cabi installed successfully.

...

<date_time> [UserSynchronizationThread, cabi] Finished synchronizing users between UIM and CABI
The wasp probe automatically starts when the process is complete.

Deploy the ump_cabi Portlet

Use this procedure to deploy the ump_cabi portlet package to view the predefined CABI dashboards in OC.

Follow these steps:

1. On the robot running OC, deploy the most current version of the ump_cabi package.
2. Verify that you can view the predefined dashboards. Go to the **Dashboards** menu in the left navigation of the Operator Console (OC) and select a CA Business Intelligence dashboard. For example, **Infrastructure Management Overview**.

Configure the SMTP Email Setting for Emailing Scheduled Reports

Reports in UIM are managed by CABI; therefore, you must configure the SMTP settings on the CABI robot.

Follow these steps:

1. Stop the robot where CABI is running.
2. Navigate to the C:\Program Files (x86)\Nimsoft\probes\service\wasp\webapps\cabijs\WEB-INF folder.
3. Create a backup of the js.quartz.properties file.
4. Edit the js.quartz.properties file as shown below; edit the bold values to match with your setup:

- report.scheduler.web.deployment.uri=**http://CABI:port/cabijs** (**http(s)://<cabi-ip-or-fqdn>:<port>/cabijs**)
- report.scheduler.mail.sender.host=**smtp.corp.com** (**The name of the computer hosting the email server.**)
- report.scheduler.mail.sender.username=**smtp_user_name_** (**The name of the email server user that JasperReports Server can use.**)
- report.scheduler.mail.sender.password=**smtp_password_** (**The password of the email server user.**)
- report.scheduler.mail.sender.from=**sender_email_address@yourcompany.com** (**The address that appears in the From field on email notifications.**)
- report.scheduler.mail.sender.protocol=**smtp** (**The protocol that the email server uses. JasperReports Server supports only SMTP.**)
- If your email server does not require a user name or password, leave the values empty; for example:
 - report.scheduler.mail.sender.username=
 - report.scheduler.mail.sender.password=

NOTE

If you add # at the start of the above lines, it will corrupt the file and CABI will be unable to start.

5. Restart the CABI robot.

Optional Tasks

The following tasks are optional and not required for all CA UIM environments. After you have successfully installed your CABI server, review the following tasks. Complete any of the tasks that you need for your environment.

Upgrade Pre-existing Self-signed Certificates to Java 1.8

Perform this procedure if your version of CABI was previously configured to use HTTPS. The Java version was updated to Java 1.8 starting with CA UIM 8.5.1. You must upgrade any self-signed certificates that are generated by CA UIM from previous CA UIM versions. If you do not upgrade the pre-existing certificates, HTTPS connections to CABI Server will not work due to the change in security encryption levels in Java 1.8.

Follow these steps:

1. Repeat the following steps for each instance of wasp that you configured for HTTPS.
2. On the CABI Server robot with wasp, navigate to the wasp.keystore file in **<UIM_installation>\probes\service\wasp\conf\wasp.keystore**.
3. Delete the wasp.keystore file.
4. Go to Admin Console.
5. Restart wasp on the CABI Server robot. The wasp.keystore file is regenerated according to the SHA256 algorithm standard.
6. Verify that you can reestablish browser connectivity to the system. Accept any prompts to accept the new self-signed certificate in your browser.

Using an External URL to Access CABI Server

Use this procedure if you are an MSP that requires your customers to connect through an external URL to access the dashboards.

Follow these steps:

1. Obtain the Fully Qualified Domain Name (FQDN) for the external URL.
2. Go to the filesystem on the CABI Server.
3. Edit the hosts file. The location depends on the platform type:
 - Windows - c:\windows\system32\drivers\etc\hosts
 - Linux - /etc/hosts
4. Add an entry with the syntax: **<local IP of the cabi server> <FQDN of external url>**

For example, 123.123.123.12 my.externalcabiserver.com

5. Save the file.
6. Open raw configure for the cabi probe.
7. Go to **Setup** and add the key **cabi_url** with the value: **http://<FQDN of external url>/cabijs**
8. Restart the cabi probe and wait for the new port and pid before continuing with the next step. In cabi.log, the new path pointing to the FQDN URL appears.
9. Restart wasp on the OC robot.
10. You can access CABI Server using the new FQDN and the OC cabi dashboards resolve for the new URL.

NOTE

If using https, follow the instructions in [Configure CABI Server to Use HTTPS](#).

Configure CABI Server to Use HTTPS

We recommend that you consult your network security engineers and compliance specialists regarding your specific security requirements. In general, industry-standard security requirements mandate the use of SSL encryption for client/server communications on an untrusted network.

Follow these steps:

1. Configure wasp for HTTPS for UIM or OC as described in the article [Configure HTTPS in Admin Console or OC](#).
2. Go to the robot running wasp and CABI Server.
3. Configure wasp for HTTPS as described in the article [Configure HTTPS in Admin Console or OC](#).
4. Open raw configure for the cabi probe.
5. Go to **Setup** and add the key **cabi_url** with the value: **https://<CABI_Server_IP or hostname>:<port>/cabijs**
Where **<port>** is the HTTPS port.
6. Restart wasp on the OC robot.
7. Instruct users who access CABI Server directly to use the URL: **https://<CABI_Server_IP or hostname>:<port>/cabijs**
Where **<port>** is the port for https communications. The default HTTPS port number is 8443. For example, <https://12.123.123.12:8443/cabijs>.
8. Instruct users to accept any browser-specific security certificate warnings that are required to proceed to the CABI Server home page.

Change the Frequency of Backups

A backup of the dashboards pack is created when you upgrade the cabi probe or dashboard package. Use the auto-backup settings to control the frequency of backup file creation. You can use these options to save resources if you frequently upgrade the cabi probe and dashboards.

Follow these steps:

1. Go to raw configure for the cabi probe.
2. Set the value for the following keys as needed:
 - **auto_backup_fequency_in_hours** - The cabi probe only uses this key when a dashboard is available to import and the **auto_backup_on_import_enabled** key is set to **yes**. If the time of the last backup is less than the specified frequency, then a backup is created. A setting of 0 indicates no backup is created. The default setting is **24** hours.
 - **auto_backup_on_import_enabled** - This key indicates if a backup file is created for dashboard packages. A backup file is created when set to **yes**. The default setting is **yes**.
 - **auto_backup_on_import_max_time_in_secs** - This is the amount of time that is allowed to pass before an error message is generated in the cabi probe log file. The default setting is **1800** seconds.

Customize Report Logo

You can customize the appearance of your CABI Dashboard reports to match your organization's name and logo.

Follow these steps:

1. Login to OC using the administrator credentials.
2. **Open CABI Server Home** using the url **http(s)://<CABI_Server_IP or hostname>:<port>/cabijs** in another tab of the browser.
3. From the menu, select **View**, Repository and navigate to Public, ca, Unified Infrastructure Management, resources, library, health, images.
4. Select the company_logo.png and click **Edit** to replace with your logo.
5. Similarly, to change the logo for all reports globally, then navigate to Public, ca, Unified Infrastructure Management, resources, common, images.
6. Select the company_logo.png and click **Edit** to replace with your logo in all the reports.

Bundled CABI Server Firewall Rules

The following table defines the ports and directions that must be open through a firewall for a Bundled configuration. For additional information, see [Firewall Port Reference](#).

| Communication Required | Ports | Direction | Firewall Rules | Details |
|--|--|-------------------|--|---|
| Bundled CABI Server to UIM database | 1433 (Microsoft SQL Server); 1521 (Oracle); 3306 (MySQL) | Inbound | Allow inbound on respective port for UIM database. | Inbound from CABI Server to the chosen database. The port depends on the database type and configuration. |
| Bundled CABI Server to OC | 80 or 443; configurable | Inbound, outbound | Allow inbound on 80 or 443 to OC and CABI Server. | This connection provides browser and customer client connectivity to CABI Server and OC. Port 80 by default or port 443 for HTTPS. You can use another configured port value for HTTP or HTTPS. The port can vary from client/browser to CABI Server and OC. The value depends on your choice during the CABI Server and OC installation. For example, port 80 or port 443. The configurable range of ports is 1 through 65535. |

Troubleshooting

- If the dashboards are not auto-deployed after you install bundled CABI, you must increase the heap size for the cabi probe by using the raw configuration.
- While upgrading CABI probe, the probe may fail to start and you will get a "max restart alarm message". You will see a message about backup related content in the log and have partial java dump files in the cabi directory. This can happen if there are a large number of custom reports that require a larger amount of memory to backup then the probe is already configured for.

To resolve this issue:

- Increase the **java_mem_init** and **java_mem_max** options in startup->opt section of the cabi probe's raw configuration options.
- Start by setting the MIN to 1 GB and the MAX to 2 GB to try and resolve this issue, you may need to increase this depending on the number of custom reports. This can be done either from the Infrastructure Manager (IM) or from Admin Console (AC).
- Deactivate and activate the cabi probe which will continue with the upgrade process.
- Ensure that the Jasper Server is accessible after the installation by using URL **http(s)://<hostname/>IPAddress>:<port>/cabijs** and verify if the predefined dashboards are deployed. You can verify the dashboards by navigating to /public/ca/uim/dashboards/common folder in the CABI server.

| Name | Description | Type | Created Date | Modified Date |
|---------------------------|-------------------------------|-----------|--------------|---------------|
| Alarm Summary SaaS | UIM Alarm Summary SaaS | Dashboard | Today | August 13 |
| Alarm Summary | UIM Alarm Summary | Dashboard | Today | August 13 |
| Container Group Summary | UIM Container Group Summary | Dashboard | Today | August 13 |
| Device by Role SaaS | UIM Device by Role SaaS | Dashboard | Today | August 13 |
| Device Details SaaS | UIM Device Details SaaS | Dashboard | Today | August 13 |
| Device KPI SaaS | UIM Device KPI SaaS | Dashboard | Today | August 13 |
| Device Summary | UIM Device Summary | Dashboard | Today | August 13 |
| Group Summary | UIM Group Summary | Dashboard | Today | August 13 |
| Inventory Summary | UIM Inventory Summary | Dashboard | Today | August 13 |
| Probe Detail | UIM Probe Detail | Dashboard | Today | August 13 |
| Top Devices by Alarm SaaS | UIM Top Devices by Alarm SaaS | Dashboard | Today | August 13 |
| UIM Summary | UIM Summary | Dashboard | Today | August 13 |
| UIM Summary SaaS | UIM Summary SaaS | Dashboard | Today | August 13 |



If you are unable to see the above folder, deploy the dashboard packs manually.

- If the Operator Console is configured with HTTPS, then CABI must also be configured with HTTPS. See the following combinations that are not supported:
 - Operator Console is configured with HTTPS and CABI with HTTP
 - Operator Console is configured with HTTP and CABI with HTTPS
- If HTTPS for CABI is configured with a self-signed certificate or invalid certificate, then Operator Console may not load CABI page successfully.
 - As a temporary resolution, you may open the CABI URL (https://<cabirobot_IP>:<port>/cabijs and https://<cabirobot_hostname>:<port>/cabijs) and accept the exception and then open the Operator Console. Or add the certificate as a trusted certificate in the system cert store or browser cert store as appropriate.
- In certain cases, when the Operator Console page is left open for a long time, CABI pages may not load. You can try the following possible solutions:
 - Log off from the Operator Console session
 - Log in again
- While installing CABI on a named instance of any database server (MS SQL or Oracle), you may face an issue where CABI probe turns red and shows the user sync issue in the log file. Error log contains error messages related to 401 and 403 errors: "URL attempted http:<hostname>:80/cabijs/login.html, Response code :403" and "Error getting all organizations, got unexpected response code '401' and body """.
 - Perform the below steps to fix these errors:
 - Login to CABI server with superuser credentials.
 - Go to Manage -> Users. select on "CABI_REST_USER" and click on delete user.
 - Restart the CABI robot.

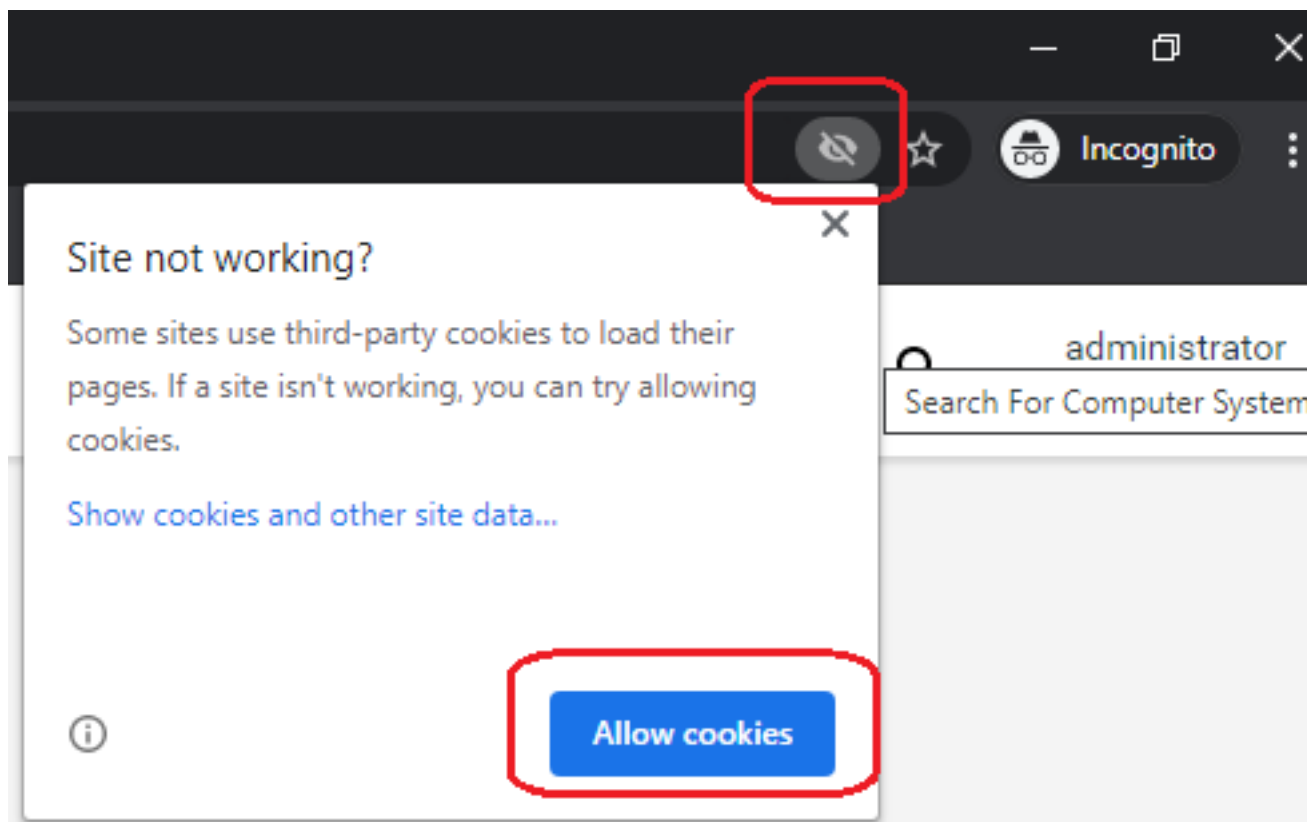
Third-party cookies and same-site cookies:

- When the Operator Console and the CABI are on different systems, there may be issues related to the same-site cookie or third-party cookie. If the Operator Console and the CABI URL do not have same sub-domain and domain (for example: IP Addresses are used), the cookies of CABI would be considered as third-party when accessing Operator Console in a browser. Few browsers may enforce blocking third-party cookies causing issues with loading of CABI pages. One such manifestation may be "Data-access error" on CABI-related pages in Operator Console. The following are few suggestions if you are using Chrome:
 - The latest Chrome browser enforces stringent same-site cookie rules (<chrome://settings>)

General settings

| | | |
|---|---|---|
| <input type="radio"/> | Allow all cookies | ▼ |
| <input checked="" type="radio"/> | Block third-party cookies in Incognito | ▲ |
|  | Sites can use cookies to improve your browsing experience, for example, to keep you signed in or to remember items in your shopping cart | |
|  | While in incognito, sites can't use your cookies to see your browsing activity across different sites, for example, to personalize ads. Features on some sites may break. | |
| <input type="radio"/> | Block third-party cookies | ▼ |
| <input type="radio"/> | Block all cookies (not recommended) | ▼ |

In these scenarios, you may need to allow the third-party cookies as shown below:



And, additionally choose to disable the below flags related to same-site cookie (<chrome://flags>)

Available

Unavailable

- **SameSite by default cookies**

Treat cookies that don't specify a SameSite attribute as if they were SameSite=Lax. Sites must specify SameSite=None in order to enable third-party usage. – Mac, Windows, Linux, Chrome OS, Android

[#same-site-by-default-cookies](#)

Disabled

- **Enable removing SameSite=None cookies**

Enables UI on chrome://settings/siteData to remove all third-party cookies and site data. – Mac, Windows, Linux, Chrome OS

[#enable-removing-all-third-party-cookies](#)

Disabled

- **Cookies without SameSite must be secure**

If enabled, cookies without SameSite restrictions must also be Secure. If a cookie without SameSite restrictions is set without the Secure attribute, it will be rejected. This flag only has an effect if "SameSite by default cookies" is also enabled. – Mac, Windows, Linux, Chrome OS, Android

[#cookies-without-same-site-must-be-secure](#)

Disabled

- (Optional settings) Only if the Operator Console URL and the CABI URL can be accessed with the **same domain and sub-domain**, you may decide to perform the below settings:
 - For example, Operator Console URL: `http://OpCon.subdomain.com/operatorconsole_portlet/overview` and CABI URL: `http://cabirobot.subdomain.com/cabijs` have same sub-domain and domain **subdomain.com**. Another example, if CABI and Operator Console are installed on the same system, Operator Console URL: `http://OpCon.subdomain.com/operatorconsole_portlet/overview` and CABI URL: `http://OpCon.subdomain.com/cabijs` have same sub-domain and domain **subdomain.com**.
 - You may change sameSiteCookies settings from "None" (default) to "Lax" and other changes as given below.
 - On the CABI robot:
 - Deactivate the cabi probe.
 - Set the CABI configuration parameter **cabi_url** to `http://<URLwithMatchingSubdomainAndDomain>:<port>/cabijs`.
 - Deactivate the wasp probe.
 - Modify `nimsoft/probes/service/wasp/webapps/cabijs/META-INF/context.xml` with `<CookieProcessor class="org.apache.tomcat.util.http.Rfc6265CookieProcessor" sameSiteCookies="Lax" />`.
 - Activate the cabi probe.
 - Activate the wasp probe
 - On the Operator Console robot:
 - Deactivate the wasp probe.
 - Modify `nimsoft/probes/service/wasp/webapps/cabi/META-INF/context.xml` with `<CookieProcessor class="org.apache.tomcat.util.http.Rfc6265CookieProcessor" sameSiteCookies="Lax" />`.
 - Activate the wasp probe.
- In the case of TLS 1.2, review the following example URL in the context.xml file and modify the required values based on your environment; for example, you might need to change the trustServerCertificate value to true if your configurations require so:

```
url="jdbc:tibcosoftware:sqlserver://
SV001:3000;databaseName=UIM_SQL;sendTimestampEscapeAsString=false;AuthenticationMethod=type2;encryptionMehtod=ssl;Cr
```

- For the TLS 1.2 setup in UIM, see the required articles: [Support for TLS v1.2 \(Microsoft SQL Server\)](#) and [Support for TLS v1.2 \(Oracle\)](#). These articles also include appropriate considerations for CABI.

NOTE

More information:

- [CA Business Intelligence Dashboards](#)
- [CA Business Intelligence JasperReports Server with CA UIM Release Notes](#)

Uninstall Bundled CA Business Intelligence JasperReports Server from CA UIM

Use this procedure to remove a bundled CA Business Intelligence JasperReports Server (CABI Server) from CA UIM. Perform this procedure if an installation or upgrade fails to bring the CA UIM environment back to a normal operating state or to uninstall the CA Business Intelligence (CABI) dashboards from the CA UIM environment. CABI Server is bundled with CA UIM when CABI Server is installed on a CA UIM robot by the cabi probe. This process removes CABI Server, related keystores, and the CABI tables from the database.

WARNING

- **Warning!** This process completely removes CABI Server. Any content created within CABI Server will not be accessible after reinstallation.
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

Requirements

This procedure has the following requirements:

- cabi probe.
- Access permissions to drop tables in the CA UIM database.

Uninstall the CABI Server Robot

Follow these steps:

1. Go to Admin Console and deactivate the wasp and cabi probes.
2. Copy the *js-pro-drop.ddl* script from the following location in the CABI Server robot:


```
<UIM_installation>/probes/service/cabi/config/scripts/drop_tables/1.2/<cabi_DB_type>
```
3. Use the execution environment of your choice to run the following script:


```
<UIM_installation>/probes/service/cabi/config/scripts/drop_tables/1.2/<cabi_DB_type>/
js-pro-drop.ddl
```
4. Go to Admin Console and delete the cabi and wasp probes from the CABI Server robot.

NOTE

If you have inadvertently installed CABI Server on your Operator Console (OC) server robot, do not delete the wasp probe.

5. Remove all the dashboard and report packages. To remove a package:

- a. Locate the controller probe.
 - b. Select the inline menu button (
 -
 -
 -
 next to the probe > **View Probe Utility in New Window.**
 - c. Select **inst_pkg_remove** from the **Command** column, and enter the package name. For example, **uim_core_dashboards_pack**.
 - d. Select the play button to run the command.
6. Delete the following directories on the CABI Server robot:
- <UIM_installation>/ probes/service/wasp
- NOTE**
If you have inadvertently installed CABI Server on your Operator Console (OC) server robot, do not delete the wasp folder.
- <UIM_installation>/probes/service/cabi
 - <UIM_installation>/c

Install or Upgrade for an External CA Business Intelligence JasperReports Server

There are two possible deployment paths for CA Business Intelligence JasperReports Server (CABI Server). This article describes a deployment with an external CABI Server.

Deploying the `cabi_external` probe allows a separate CABI Server instance to communicate with CA UIM and other CA Agile Central products. Select this deployment type if you want to use a CABI Server instance that is **NOT** deployed on a robot. You must deploy the CABI Server instance. If you want to share the CABI Server instance with multiple CA Agile Operations products, see [Unified Dashboards and Reporting for Infrastructure Management](#).

NOTE

- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.
- If you do not need to view dashboards and reports for other CA Agile Central products, we recommend [Install or Upgrade for a Bundled CA Business Intelligence JasperReports Server](#).
- You can migrate from a bundled CABI Server installation to an external CABI Server installation. For more information, see [Migrate from Bundled to External Configuration](#).
- Before proceeding with the integration of CABI JasperReports Server and UIM, make sure you have different servers for CABI Jasper server, CABI robot and Operator Console (OC).
- For more information on CA Business Intelligence JasperReports Server (to deploy `cabi_external` 3.32), review the [CABI installation article](#).
- For more information on CA Business Intelligence JasperReports Server (to deploy `cabi_external` 3.40), review the [CABI installation article](#).

Contents

Software Requirements

The following table lists the required software. For a matrix of software versions for a specific release, see [CA Business Intelligence with CA UIM](#).

| Software | Download | Notes |
|---|--|--|
| CA Business Intelligence JasperReports Server for Unified Dashboards and Reporting for Infrastructure Management | support.broadcom.com , Download Management. See Notes. | A Support login is required to download. <ul style="list-style-type: none"> Unified CABI 7.1.1 (Windows) -- Controlled release. Unified CABI 7.1.1.1 (Linux) -- GA release. Download the Linux GA release from the support.broadcom.com location. Jasper Server version is 7.1.1 |
| CA UIM | support.broadcom.com , Download Management | A CA support login is required to download. |
| cabi_external probe | support.nimsoft.com , Archive | Add to the CA UIM archive. A CA support login is required to download. |
| ump_cabi portlet | support.nimsoft.com , Archive | Add to the CA UIM archive. A CA support login is required to download. |
| uim_core_dashboards_pack | support.nimsoft.com , Archive | Add to the CA UIM archive. A CA support login is required to download. |
| Report packages: <ul style="list-style-type: none"> uim_unified_reporter_pack uim_cabi_health_report_pack | support.nimsoft.com , Archive | Add to the CA UIM archive. A CA support login is required to download. |
| Dashboard packages: uim_<technology_name>_dashboards_pack | support.nimsoft.com , Archive | Add the appropriate dashboard packages to the CA UIM archive. A CA support login is required to download. The dashboard packages are only required if you need to view data for the specific technology. For example, the uim_aws_dashboards_pack dashboard package is only required if you must view data for your AWS environment. For a list of available dashboard packages, see CA Business Intelligence with CA UIM . |

Hardware Requirements

The CABI Server (CA Business Intelligence JasperReports Server) software is installed on a system with the following minimum resources:

- CPU: 2.8-GHz quad-core processor
- Memory: 8-GB RAM
- Disk Size: 100-GB

NOTE

If you want to share a single CA Business Intelligence (CABI) server instance with multiple CA Agile Operations products, additional requirements exist. For more information, see [Extend your CA Products with Unified Dashboards and Reporting for Infrastructure Management](#).

Environment Requirements

This process requires the following environment:

- A server instance with the CA Business Intelligence JasperReports Server for Unified Dashboards and Reporting for Infrastructure Management (CABI Server) software. This instance is **NOT** a hub or robot.
 - The server must have a **new** installation of the [CA Business Intelligence JasperReports Server for Unified Dashboards and Reporting for Infrastructure Management](#).
 - The software installation should include:
 - An **embedded Tomcat web server**.
 - **(Recommended)** An **embedded PostgreSQL** database.
- A CA UIM instance. For information about installation, see:
 - [Release Notes](#)
 - [Install UIM Server](#)
 - [Install the Operator Console \(OC\)](#)
- [Download, update, or import](#) the following packages to the Archive:
 - cabi_external probe
 - cabi packages
 - dashboard packages
 - report packages
- (Optional) Secure Hub and Robot - The secure hub and robot provide robust hub-to-hub and robot-to-hub communication. To upgrade CABI in a secure setup, upgrade the CABI robot to a secure state and then perform the CABI upgrade. For more information about the secure setup and how to deploy certificates, see [Secure Hub and Robot](#).
- **(MySQL Only)** If you are using MySQL for your CABI Server database, you must change the default memory settings. This database is for the CABI users, reports, and dashboards. Change the following settings so that the CA Business Intelligence dashboard deployment is successful:
 - Set **max_allowed_packet=32M**
 - Set **innodb_log_file_size=356M**
 - Set **table_definition_cache=2000**

NOTE

Your dashboards import fails if the above recommended settings are not updated for MySQL.

- **(Microsoft SQL Server Windows Authentication Only)** If you are using Microsoft SQL Server Windows Authentication, the CABI Server system, cabi_external probe robot, and Operator Console (OC) robot must have Windows operating systems. No requirements exist for matching operating systems if you are NOT using Microsoft SQL Server Windows Authentication.

NOTE

Do not install or configure CABI Server using Cygwin.

Unified CABI and cabi_external Matrix

The following table explains the Unified CABI and cabi_external matrix:

| Jasper Server Version | Unified CABI Version | cabi_external version | UIM Server Version | Download Location |
|-----------------------|--|-----------------------|--------------------|---|
| 7.5 | NA | NA | NA | NA |
| 7.1.1 | <ul style="list-style-type: none"> 7.1.1 (Windows) - Controlled release 7.1.1.1 (Linux) - GA release | 4.20 | 20.1 and 20.3 | <ul style="list-style-type: none"> For the Linux GA release, Download the Business Intelligence JasperReport Server r7.1.1.1_LINUX.TAR.GZ package from support.broadcom.com. |
| 7.1.1 | <ul style="list-style-type: none"> 7.1.1 (Windows) - Controlled release 7.1.1 (Linux) - Controlled release | 4.10 | 9.20 | These are controlled releases. |
| 6.4.3 | 6.4.3 (Windows and Linux) | 3.40 | 9.0.2 SPI (9.1.0) | Download the CA Business Intelligence JasperReports Server 6.4.3 for CA Spectrum 10.3 & 10.4 for Windows & Linux.zip package from support.broadcom.com . |
| 6.3.0 | 6.3.0 | 3.32 | 9.02 | Download the Jaspersoft 6.3 for CA Spectrum for Windows, Solaris and Linux.tar.gz package from support.broadcom.com . |
| 6.3.0 | 6.3.0 | 3.30 | 9.02 | Download the Jaspersoft 6.3 for CA Spectrum for Windows, Solaris and Linux.tar.gz package from support.broadcom.com . |
| 6.3.0 | 6.3.0 | 3.20 | 8.51 | Download the Jaspersoft 6.3 for CA Spectrum for Windows, Solaris and Linux.tar.gz package from support.broadcom.com . |

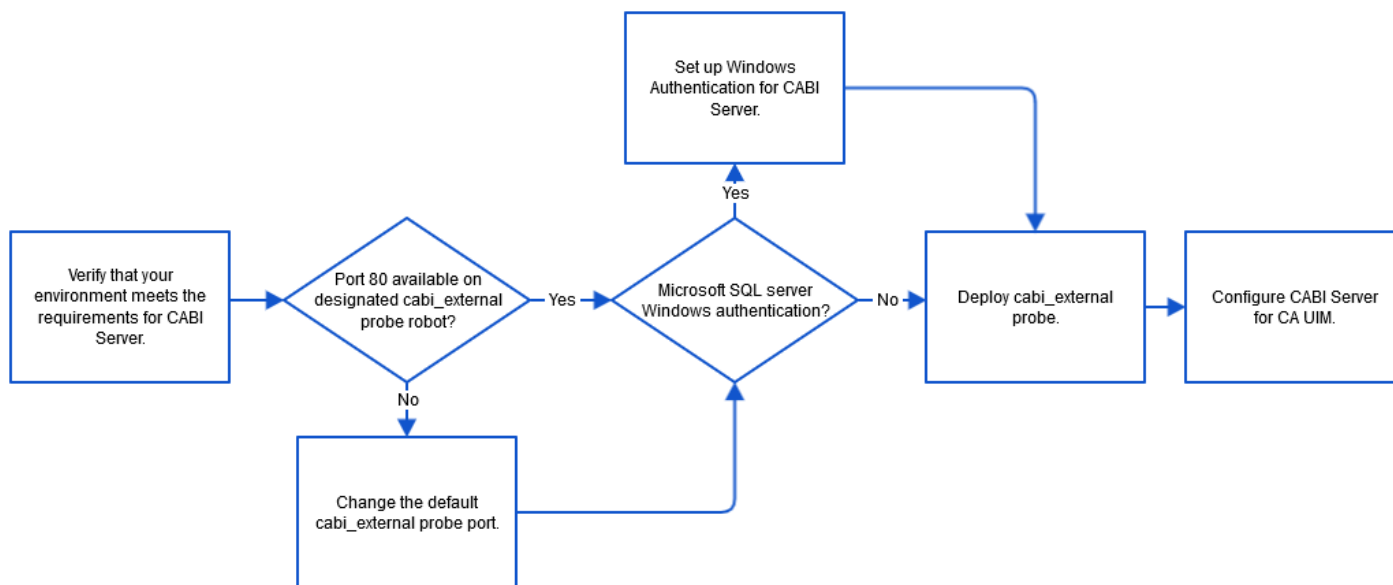
Configure CA UIM for an External CABI Server

Use this procedure to configure CA UIM to connect to a new CABI Server instance.

Process Overview

The following diagram shows the sequence of tasks to complete.

Figure 16: External CABI Process



(Microsoft SQL Server Windows Authentication Only) Configure Windows Authentication

Use this procedure if you must enable Windows authentication on the CABI Server.

Follow these steps:

1. Grant the Windows Authentication user full control of the following directories:
 - The CABI Server installation directory.
 - The CABI Tomcat installation directory if the **Apache-Tomcat** directory is not included in the CABI Server installation directory.
2. Modify the CABI Tomcat service to run as a Windows authentication user.
 - a. Open the Windows Services console.
 - b. Right click the Service and click **Properties**.
 - c. Select the **Log On** tab.
 - d. Select **This account**.
 - e. Enter the Account information for the Windows authentication user.
 - f. Click **Ok**.
 - g. Restart the CABI Tomcat service.
3. Install SQL Server drivers on the CABI Tomcat server. The **Apache-Tomcat** directory is usually in the CABI Server installation directory.
 - a. Find the Microsoft JDBC Driver for SQL Server files from the following location in your UIM installation folder:
 - sqljdbc6-6.2.2.jar file from `\\Nimsoft\probes\service\<probe>\lib`
 - sqljdbc_auth.dll from `\\Nimsoft\lib`
 - b. Extract the self-contained zip file.
 - c. Copy the `sqljdbc_auth.dll` (version: 6.2.2.1) in the extracted directory to the CABI Tomcat bin directory.
 - d. Copy the `sqljdbc6-6.2.2.jar` in the extracted directory to the CABI Tomcat lib directory.
 - e. Restart the CABI Tomcat server.
4. Run the `cabi_external` probe as a Windows authentication user.
 - a. On the robot with the probe, go to **Administrative Tools > Services** and double-click on **Nimsoft Robot Watcher**.

- b. Select the **Log On** tab.
- c. Change the account to the same account and password that is used in the **data_engine** and the primary UIM server.
- d. Click **OK**.
- e. Right-click on **Nimbus Robot Watcher** and select the **Restart** option.
- f. Close the windows.
- g. Restart the robot.

Deploy the cabi_external Probe

The `cabi_external` probe functions as a gateway for CA Business Intelligence JasperReports Server (CABI Server). This configuration allows you to share the CABI Server instance with multiple CA Agile Operations products. You view dashboards on the CABI Server.

NOTE

The UIM Server installer creates a `.pem` file (certificate.pem) in the `<Nimsoft>\security` folder. The `.pem` file is a symmetric key that is shared with the required robots, which is then used for communication with the `data_engine` probe. You copy this `.pem` file to the remote Operator Console (OC), UR, and CABI robots and provide the location of the file in the `robot.cfg` file (`cryptkey = <.pem file location>`). Furthermore, if any impacted probe is not on the same computer where `data_engine` is present, copy the generated `.pem` file to the robot computer (where `data_engine` is not available) and update the `robot.cfg` file with the `.pem` file location on that computer. For more information about the `robot.cfg` file configuration, see [Configure robot.cfg](#).

Follow these steps:

1. Verify that the `cabi_external` probe, `uim_core_dashboards_pack`, and report packages are in the archive.

NOTE

UIM 20.3.0 installer comes with `uim_core_dashboards_pack` version 2.46 and `uim_unified_reporter_pack` version 1.04 which are unsupported for the `cabi_external` probe version 4.20. Follow these steps for the `cabi_external` probe to work:

1. Remove `uim_core_dashboards_pack` version 2.46 and `uim_unified_reporter_pack` version 1.04.
 2. Deploy `uim_core_dashboards_pack` version 2.45 and `uim_unified_reporter_pack` version 1.03 from the Archive.
2. Deploy the packages on a robot. The probe automatically deploys any package dependencies that exist in the archive. For example, the `uim_core_dashboards_pack` and report packages. For more information about how to deploy a probe package, see the [Deploy Packages](#) article. The `cabi_external` probe turns red in admin console and a No Restart error appears in the probe log file. This error is expected behavior. Continue with the next step.
 3. Open **Raw Configure** for the probe. For more information, see [Configure a Probe](#).
 4. Go to **setup**.
 5. Change the `cabi_url` key value to the URL for the CABI Server. The format is `http://<cabi_server_name_or_IP>:<port>/<webapp>` where `<webapp>` is usually `jasperserver-pro`.
 6. Choose one of the following steps:
 - If the default superuser account is still in use on the CABI Server, no additional configuration is required.
 - If you modified the default superuser account, perform the following steps:
 - a. Enter the username as the value for the key `cabi_rest_user`.
 - b. Create the key `cabi_rest_password_cleartext`. Then enter the password for the user account as the key value. When the probe restarts, this password is encrypted and the `cabi_rest_password_cleartext` key is removed.
 7. Save your changes and activate the `cabi_external` probe.

- Verify that the installation is complete. The `cabi_external` probe might be active, but the installation process might not be complete. Go to the `cabi_external` probe log file and look for the following messages:

```
<date_time> [main, cabi_external] cabi installed successfully.
...
...
...
<date_time> [UserSynchronizationThread, cabi_external] Finished synchronizing users
between UIM and CABI
```

The wasp probe automatically starts when the process is complete.

Configure CABI Server for CA UIM

Additional installation steps are required to configure CABI Server to work with an instance of CA UIM.

Follow these steps:

- Log in to the CABI server as the user who is configured to run the CABI Tomcat service.
- Go to the filesystem of the robot with the `cabi_external` probe.
- Copy the **`uim-cabi-overlay-installer.jar`** file in `<UIM_installation>/probes/service/cabi_external/config/bin`.
- Add the file to the CABI Server root directory. Use the appropriate path for your operating system:
 - Windows: `<CABI_Server_installation>/Program Files/CA/SC/CA Business Intelligence`
 - Unix: `<CABI_Server_installation>/opt/CA/SharedComponents/CA Business Intelligence`
- Run the installer on CABI Server: `jre/bin/java -jar uim-cabi-overlay-installer.jar`
- Restart the CABI web server.

NOTE

New packages for predefined reports and dashboards are released periodically.

Upgrade cabi_external Probe

The instructions in this section are for users that want to upgrade the `cabi_external` probe. You can upgrade `cabi` version 4.10 to `cabi_external` version 4.20.

NOTE

- The UIM Server installer creates a `.pem` file (certificate.pem) in the `<Nimsoft>\security` folder. The `.pem` file is a symmetric key that is shared with the required robots, which is then used for communication with the `data_engine` probe. You copy this `.pem` file to the remote Operator Console (OC), UR, and CABI robots and provide the location of the file in the `robot.cfg` file (`cryptkey = <.pem file location>`). Furthermore, if any impacted probe is not on the same computer where `data_engine` is present, copy the generated `.pem` file to the robot computer (where `data_engine` is not available) and update the `robot.cfg` file with the `.pem` file location on that computer. For more information about the `robot.cfg` file configuration, see [Configure robot.cfg](#).
- In an upgrade scenario, if you are upgrading CABI in a secure setup, ensure that you bring your CABI robot to the secure state by deploying the appropriate certificates and then updating the robot version to the secure version. After that, you upgrade CABI. For more information about the secure setup and how to deploy certificates, see [Secure Hub and Robot](#).

Redeploy the cabi_external Probe

Follow these steps:

1. Verify that the latest cabi version, cabi_external probe, uim_core_dashboards_pack, and report packages are in the archive.
2. Deploy the packages to the location of your existing cabi_external probe.
For more information about how to deploy a probe package, see the [Deploy Probes with Admin Console](#) article.
3. Verify that the installation is complete. Go to the cabi_external probe log file and look for the following message:

```
<date_time> [main, cabi] cabi installed successfully.
```

```
...
```

```
...
```

```
...
```

```
<date_time> [UserSynchronizationThread, cabi] Finished synchronizing users between  
UIM and CABI
```

Add Predefined CA Business Intelligence Dashboard Content

The dashboard packages for a specific monitoring technology are only required if you have a business need to monitor the specific technology. For example, you only need the uim_aws_dashboards_pack if you plan to view dashboards for an Amazon Web Services environment. If you are using specific monitoring technology dashboards, you should update the packages when a new package version is available.

Follow these steps:

1. Verify that you are running the most current version of the cabi or cabi_external probe. If you are not using the current version, update your probe, uim_core_dashboards_pack packages, and any package dependencies. We recommend that you use the most current packages for your probe version. For more information about supported packages and versions, see [CA Business Intelligence with CA UIM](#).
2. Deploy the desired uim_<probe name>_dashboards_pack packages to the robot running the cabi or cabi_external probe.

View Dashboards

You view dashboards on the CABI Server.

Enter in a browser: **http://<CABI_Server_IP or hostname>:<port>/<web_app>**

Where **<port>** is the port for the CABI Server Apache Tomcat server instance, and **<web_app>** is the CABI Server web application name. The default port value is 8080 and the default web application name is jasperserver-pro. An example of a URL is, http://localhost:8080/jasperserver-pro.

Configure the SMTP Email Setting for Emailing Scheduled Reports

Reports in UIM are managed by CABI; therefore, you must configure the SMTP settings on the CABI server.

Follow these steps:

1. Stop the CABI server.
2. Navigate to the ..\CA Business Intelligence\apache-tomcat\webapps\jasperserver-pro\WEB-INF folder.
3. Create a backup of the js.quartz.properties file.
4. Edit the js.quartz.properties file as shown below; edit the bold values to match with your setup:

- report.scheduler.web.deployment.uri=**http(s)://<cabi-ip-or-fqdn>:<port>/jasperserver-pro**
- report.scheduler.mail.sender.host=**smtp.corp.com** (The name of the computer hosting the email server.)
- report.scheduler.mail.sender.username=**smtp_user_name_**(The name of the email server user that **JasperReports Server** can use.)
- report.scheduler.mail.sender.password=**smtp_password_** (The password of the email server user.)
- report.scheduler.mail.sender.from=**sender_email_address@yourcompany.com** (The address that appears in the **From** field on email notifications.)
- report.scheduler.mail.sender.protocol=**smtp** (The protocol that the email server uses. **JasperReports Server** supports only **SMTP**.)
- If your email server does not require a user name or password, leave the values empty; for example:
 - report.scheduler.mail.sender.username=
 - report.scheduler.mail.sender.password=

NOTE

If you add # at the start of the above lines, it will corrupt the file and CABI will be unable to start.

5. Restart the CABI server.

Optional Tasks

The following tasks are optional and not required for all CA UIM environments. After you have successfully installed your CABI server, review the following tasks. Complete any of the tasks that you need for your environment.

Configure CABI Server to Use HTTPS

We recommend that you consult your network security engineers and compliance specialists regarding your specific security requirements. In general, industry-standard security requirements mandate the use of SSL encryption for client/server communications on an untrusted network.

Follow these steps:

1. Configure wasp for HTTPS for UIM or Operator Console (OC) as described in the article [Configure HTTPS in Admin Console or Operator Console \(OC\)](#).
2. Configure HTTPS for your external CABI Server as described in the 'Configuring SSL' article in the [CABI JasperServer documentation](#).
3. Open raw configure for the cabi_external probe.
4. Go to **Setup** and add the key **cabi_url** with the value: **https://<CABI_Server_IP or hostname>:<port>/<webapp>**Where **<port>** is the HTTPS port and **<webapp>** is usually jasperserver-pro.
5. Restart wasp on the Operator Console (OC) robot.
6. Instruct users who access CABI Server directly to use the URL: **https://<CABI_Server_IP or hostname>:<port>/<webapp>**
Where **<port>** is the port for https communications **<webapp>** is usually jasperserver-pro. The default HTTPS port number is 8443. For example, https://12.123.123.12:8443/jasperserver-pro.
7. Instruct users to accept any browser-specific security certificate warnings that are required to proceed to the CABI Server home page.

Change the Frequency of Backups

A backup of the dashboards pack is created when you upgrade the cabi_external probe or dashboard package. Use the auto-backup settings to control the frequency of backup file creation. You can use these options to save resources if you frequently upgrade the cabi_external probe and dashboards.

Follow these steps:

1. Go to raw configure for the cabi_external probe.

2. Set the value for the following keys as needed:
 - auto_backup_fequency_in_hours - The cabi_external probe only uses this key when a dashboard is available to import and the auto_backup_on_import_enabled key is set to **yes**. If the time of the last backup is less than the specified frequency, then a backup is created. A setting of 0 indicates that no backup is created. The default setting is **24** hours.
 - auto_backup_on_import_enabled - This key indicates if a backup file is created for dashboard packages. A backup file is created when set to yes. The default setting is **yes**.
 - auto_backup_on_import_max_time_in_secs - This key is the amount of time that is allowed to pass before an error message is generated in the cabi_external probe log file. The default setting is **1800** seconds.

View CABI dashboards in Operator Console (OC)

Use this procedure to view the predefined CABI dashboards for CA UIM in Operator Console (OC).

Update the ump_cabi Portlet

Use this procedure to deploy the ump_cabi portlet package to view the predefined CABI dashboards in Operator Console (OC).

Follow these steps:

1. On the robot running Operator Console (OC), deploy the most current version of the ump_cabi package.
2. Verify that you can view the predefined dashboards. Go to the **Dashboards** in the left navigation of the Operator Console (OC) and select a CA Business Intelligence dashboard. For example, **Infrastructure Management Overview**.

Customize the Report Logo

You can customize the appearance of your CABI Dashboard reports to match your organization's name and logo.

Follow these steps:

1. Login to Operator Console (OC) using the administrator credentials.
2. Open CABI Server Home using the url **http(s)://<CABI_Server_IP or hostname>:<port>/cabijs** in another tab of the browser.
3. From the menu, select **View**, Repository and navigate to Public, ca, Unified Infrastructure Management, resources, library, health, images.
4. Select the company_logo.png and click **Edit** to replace with your logo.
5. Similarly, to change the logo for all reports globally, then navigate to Public, ca, Unified Infrastructure Management, resources, common, images.
6. Select the company_logo.png and click **Edit** to replace with your logo in all the reports.

External CABI Server Firewall Rules

The following table defines the ports and directions that must be open through a firewall for an external configuration. For additional information, see [Firewall Port Reference](#).

| Communication Required | Ports | Direction | Firewall Rules | Details |
|--|--|-----------|---|--|
| cabi_external Probe to CABI Server | 80 or 443; configurable | Outbound | Allow outbound to CABI Server. | Port 80 by default or port 443 for HTTPS. You can use another configured port value for HTTP or HTTPS. The value depends on your choice during the cabi_external probe installation. The configurable range of ports is 1 through 65535. |
| cabi_external Probe to UIM Database | 1433 (Microsoft SQL Server); 1521 (Oracle); 3306 (MySQL) | Outbound | Allow outbound on respective port for UIM database. | The port depends on the database type and configuration. |
| External CABI Server | 80 or 443; configurable | Inbound | Allow inbound from cabi_external probe. | Port 80 by default or port 443 for HTTPS. You can use another configured port value for HTTP or HTTPS. The value depends on your choice during the CABI Server installation. The configurable range of ports is 1 through 65535. |
| UIM Database to cabi_external Probe | 1433 (Microsoft SQL Server); 1521 (Oracle); 3306 (MySQL) | Inbound | Allow inbound from cabi_external probe on respective port for UIM database. | The port depends on the database type and configuration. |

Troubleshooting

- While upgrading CABI probe, the probe may fail to start and you will get a "max restart alarm message". You will see a message about backup related content in the log and have partial java dump files in the cabi directory. This can happen if there are a large number of custom reports that require a larger amount of memory to backup then the probe is already configured for.

To resolve this issue:

- Increase the **java_mem_init** and **java_mem_max** options in startup->opt section of the cabi_external probe's raw configuration options.
- Start by setting the MIN to 1 GB and the MAX to 2 GB to try and resolve this issue, you may need to increase this depending on the number of custom reports. This can be done either from Infrastructure Manager (IM) or from Admin Console (AC).
- Deactivate and activate the cabi_external probe which will continue with the upgrade process.

NOTE

More information:

- [CA Business Intelligence Dashboards](#)
- [Extend your CA Products with Unified Dashboards and Reporting for Infrastructure Management](#)

Uninstall External CA Business Intelligence JasperReports Server from CA UIM

Use this procedure to remove CA UIM from an external CA Business Intelligence JasperReports Server (CABI Server). Perform this procedure if an installation fails to bring the CA UIM environment back to a normal operating state. CABI Server is external to CA UIM when CABI Server is NOT installed on a robot by the cabi probe. This process removes CA UIM content from CABI Server.

WARNING

- **Warning!** This process completely removes CA UIM data from CABI Server. Any CA UIM content that is created within CABI Server will not be accessible.
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

Requirements

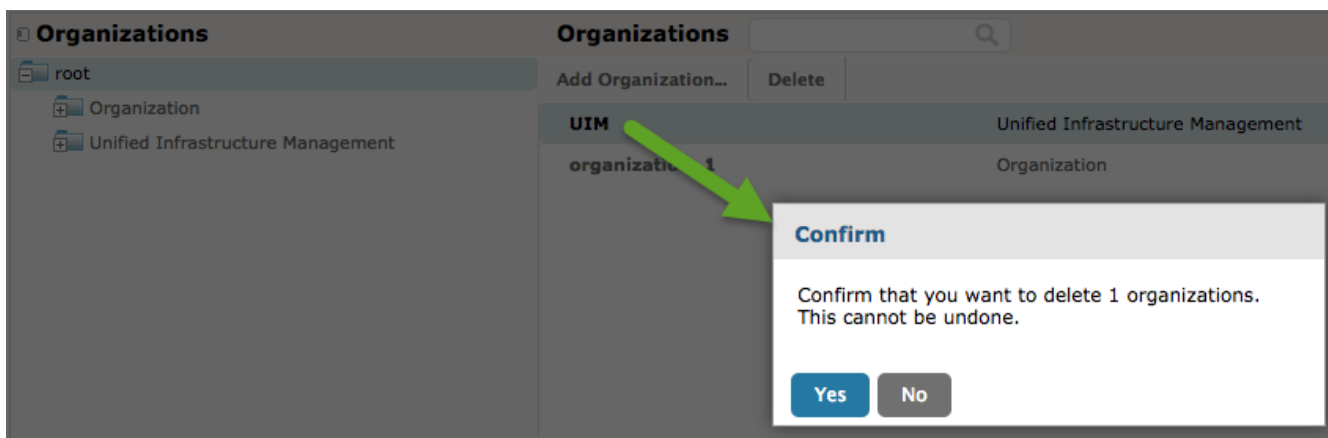
This procedure has the following requirements:

- cabi_external probe.
- A login with ROLE_SUPERUSER on CABI Server.

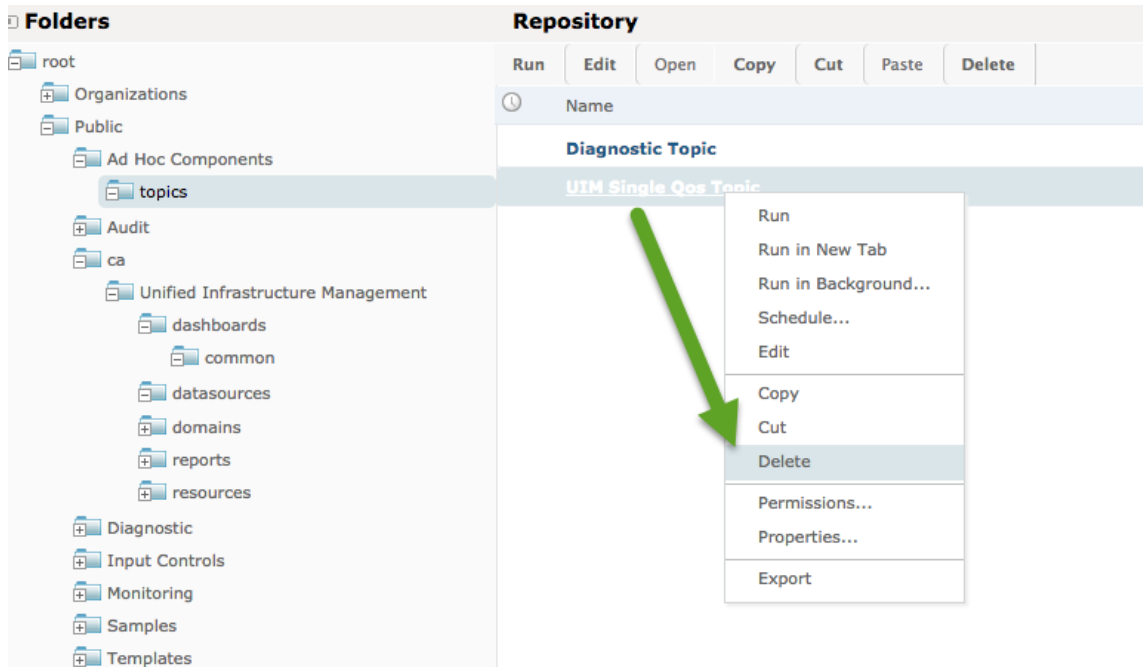
Remove CA UIM from CABI Server

Follow these steps:

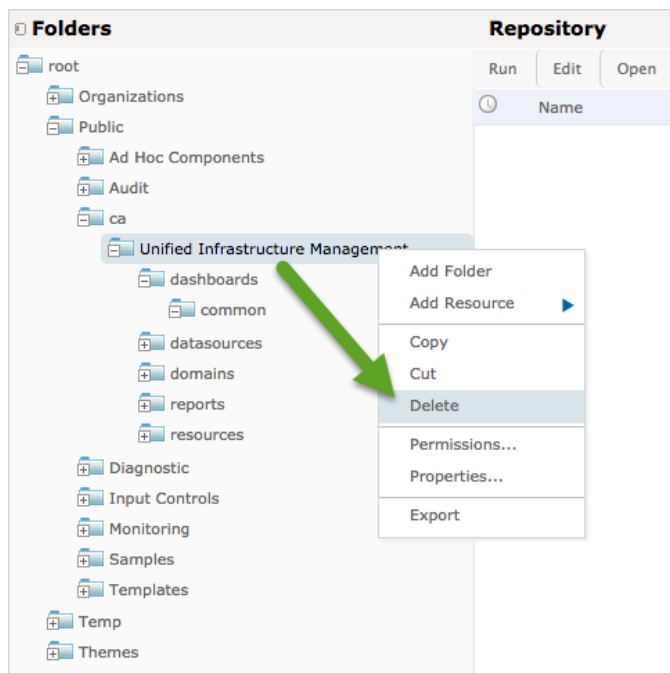
1. Log in to CABI Server.
2. Click **Manage, Organizations**.
3. Delete the **UIM** organization.



4. Remove the UIM resource reference from any custom resources (dashboard, ad hoc view, or report) that reference a resource (reports, data source, ad hoc topic, etc.) in root/Public/ca/Unified Infrastructure Management.
5. Click **View, Repository**.
6. Go to the folders list.
7. Expand root, Public, Ad Hoc Components, and then click **Topics**.
8. Delete **UIM Single Qos Topic** in the folder.



9. Expand root, Public, ca, and then right-click **Unified Infrastructure Management**.
10. Delete the **Unified Infrastructure Management** folder.



11. Stop CABI Server.
12. Run the following command to uninstall CA UIM components from CABI Server: `<unified_cabi_home>\java -jar uim-cabi-overlay-installer.jar uninstall`
 Logs are produced in the directory where you run the installer: `<unified_cabi_home>\uim-cabi-overlay-installer.log`

- **(Optional)** You can also pass another command line argument: `log.level=[1-5]` to specify the logging level (1-FATAL, 2-WARNING, 3-INFO, 4-DEBUG, 5-TRACE). For example, enter `<unified_cabi_home>\java\bin\java -jar uim-cabi-overlay-installer.jar uninstall log.level=5` for trace level logging.

13. Restart CABI Server.

Uninstall the Probe

Follow these steps:

1. Log in to Admin Console and locate the robot with the `cabi_external` probe.
2. Deactivate the probe and wait a minute for the process to complete.
3. Delete the probe from the CABI Server robot.
4. Remove all the dashboard and report packages. To remove a package:
 - a. Locate the controller probe.
 - b. Select the inline menu button (
 -
 -
 -
 next to the probe > **View Probe Utility in New Window**.
 - c. Select **inst_pkg_remove** from the **Command** column, and enter the package name. For example, **uim_core_dashboards_pack**.
 - d. Select the play button to run the command.
5. Delete the following directories on the CABI Server robot:
 - `<UIM_installation>/probes/service/cabi_external`
 - `<UIM_installation>/cabi`

(Optional) Remove Unified CABI JasperReports Server

To remove the unified CA Business Intelligence JasperReports Server (Unified CABI). This process removes all your content from the CABI Server.

WARNING

Warning! This process completely removes the Unified CABI Server.

For detailed steps on uninstalling CA Business Intelligence JasperReports Server 7.1.1, see the related [documentation](#).

Migrate from Bundled to External Configuration

Use this process to migrate custom dashboard content from a bundled CA Business Intelligence JasperReports Server (CABI Server) configuration to an external CABI Server configuration. The external configuration allows you to share a single CA Business Intelligence (CABI) server instance with CA UIM and multiple CA Agile Operations products. For more information, see [Extend your CA Products with Unified Dashboards and Reporting for Infrastructure Management](#).

Environment Requirements

This process requires the following environment:

- Deploy an instance of CABI Server if an instance does not already exist in your environment. For information, see [CA Business Intelligence JasperReports Server](#).
- Complete an external deployment. For more information, see [Install or Upgrade for an External CA Business Intelligence JasperReports Server](#).

Migrate Custom Content

Use this process to migrate your custom dashboard content. This process creates a complete backup of CABI Server. The file that is created includes information such as custom dashboards, users, organizations, and data sources.

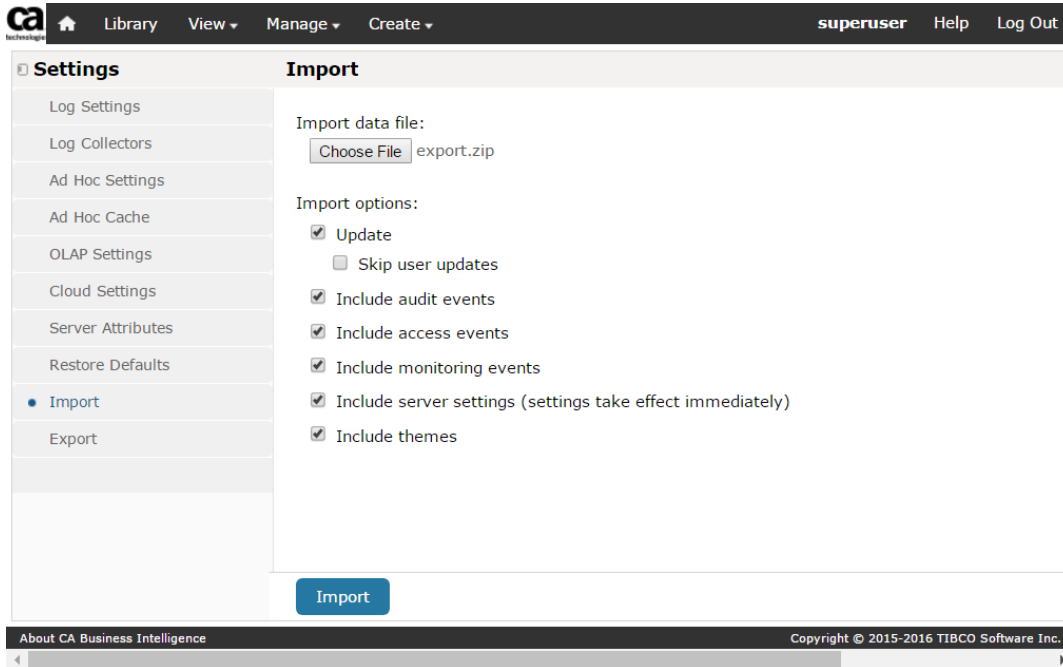
Follow these steps:

1. Verify that your environment meets the minimum requirements to migrate content.
2. Log in to the old CABI Server instance as a user with superuser permissions.
3. Go to the Manage menu and click **Server Settings**.
4. Click **Export** in the Settings list.
5. Leave the default settings. You want to export everything.

The following figure shows an example export page.

The screenshot displays the 'Export' configuration page in the CABI Server interface. The top navigation bar includes 'Library', 'View', 'Manage', and 'Create' menus, along with a 'superuser' profile and 'Help'/'Log Out' links. The left sidebar shows a 'Settings' menu with 'Export' highlighted. The main panel is titled 'Export' and is divided into three sections: 'File Properties' with a text input for 'Export Data File Name (required)' containing 'export.zip'; 'Export Options' with a checked checkbox for 'Export Everything'; and 'Roles and Users to Export' with radio buttons for 'Selected roles and users', 'Users with selected roles', and 'Roles with selected users'. Below this, a 'Roles:' section has a text input containing 'ROLE_ADMINISTRATOR', 'ROLE_ANONYMOUS', and 'ROLE_DOMAIN_DESIGNER'. A blue 'Export' button is positioned at the bottom of the form. The footer of the page contains 'About CA Business Intelligence' and 'Copyright © 2015-2016 TIBCO Software Inc.'.

6. Log in to the new CABI Server instance as a user with superuser permissions.
7. Go to the Manage menu and click **Server Settings**.
8. Click **Import** in the Settings list.
9. Select the import data file from the old CABI server instance.
The following figure shows an example import page.



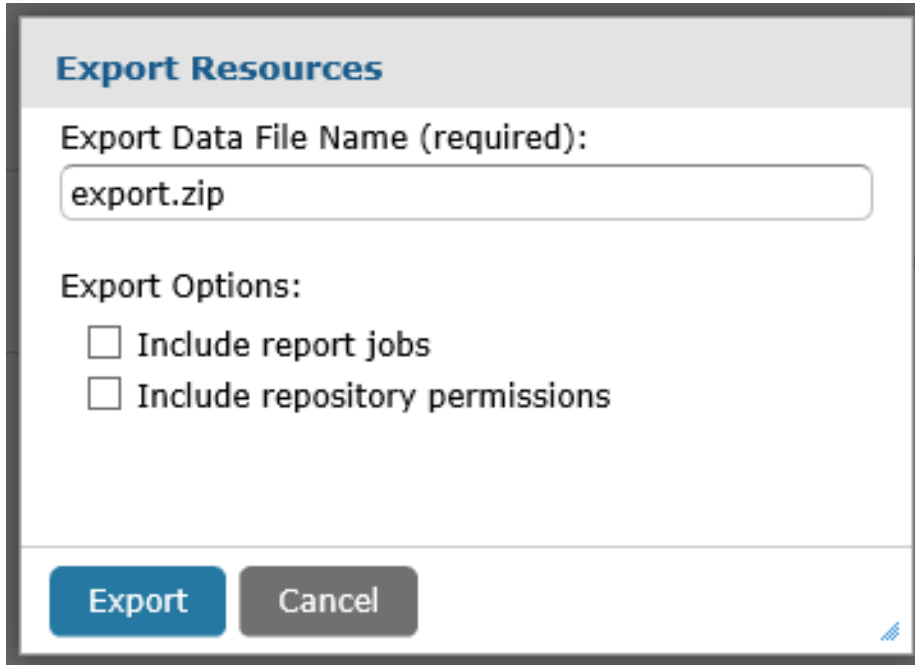
10. Import the file.

Migrate Reports from Unified Reporter

Use this procedure to migrate your custom Unified Reporter (UR) reports to the CA Business Intelligence JasperReports Server repository. You can use these reports to create your own [custom dashboards](#). If you are only using the out-of-box UR reports, there is no need to migrate. You can use the same [out-of-box reports in the CABI Dashboards](#).

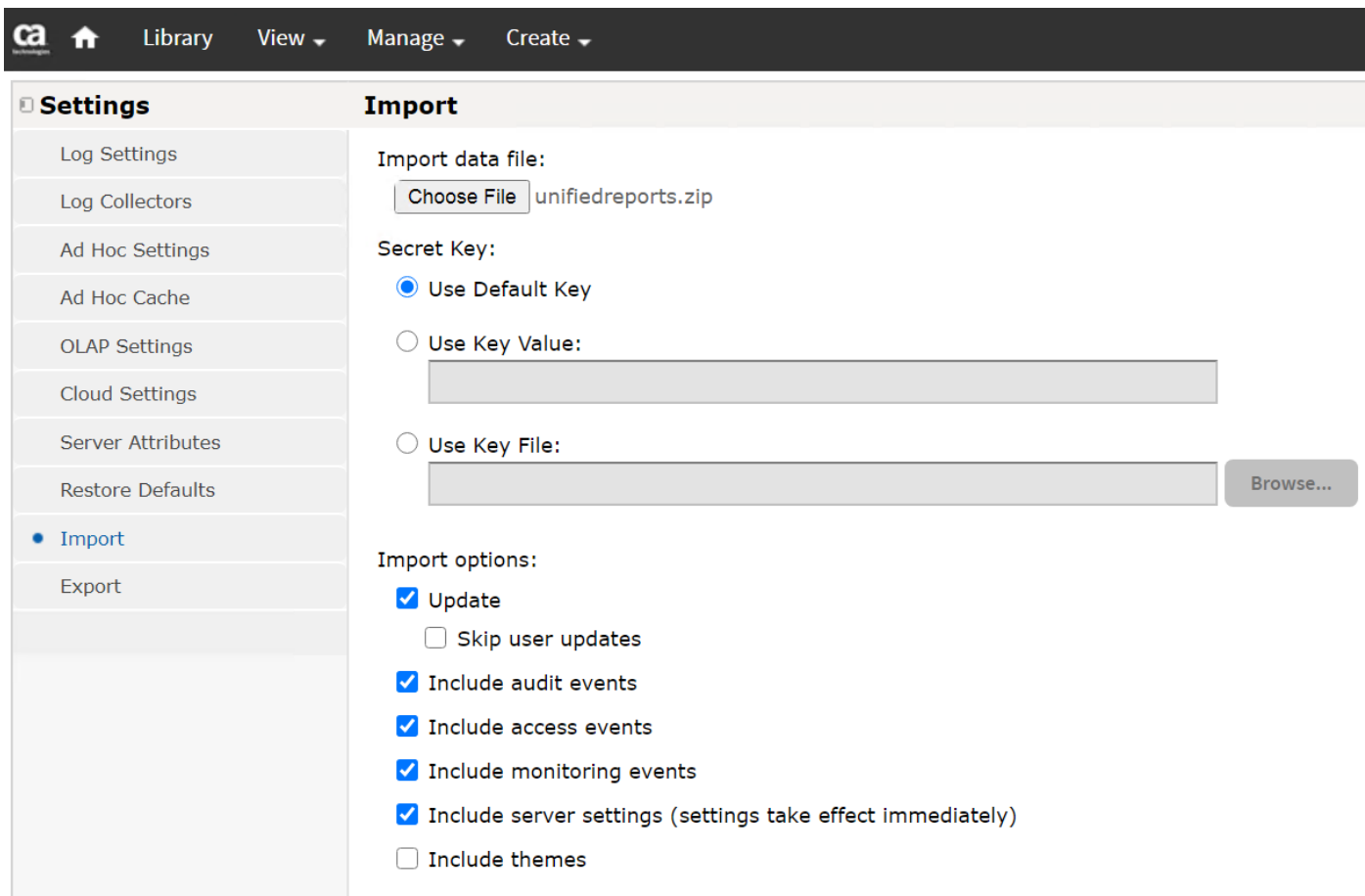
Follow these steps:

1. Verify that your environment meets the minimum requirements to migrate content.
2. Log in to the old UR JasperReports Server instance as a user with superuser permissions.
3. Click **View > Repository**.
4. Right-click the folder with your custom reports and click **Export**.
5. Clear the Export Options.



The image shows a dialog box titled "Export Resources". It has a header bar with the title. Below the header, there is a label "Export Data File Name (required):" followed by a text input field containing "export.zip". Underneath, there is a section labeled "Export Options:" with two checkboxes: "Include report jobs" and "Include repository permissions", both of which are currently unchecked. At the bottom of the dialog, there are two buttons: "Export" (highlighted in blue) and "Cancel".

6. Export the file to an appropriate location.
7. Log in to the new CA Business Intelligence JasperReports Server instance as a user with superuser permissions.
8. Click **Manage > Server Settings**.
9. Click **Import** in the Settings list.
10. Select the import file from the old UR JasperReports Server instance.
11. Clear the Import Options.



Settings

- Log Settings
- Log Collectors
- Ad Hoc Settings
- Ad Hoc Cache
- OLAP Settings
- Cloud Settings
- Server Attributes
- Restore Defaults
- Import**
- Export

Import

Import data file:

unifiedreports.zip

Secret Key:

Use Default Key

Use Key Value:

Use Key File:

Import options:

Update

Skip user updates

Include audit events

Include access events

Include monitoring events

Include server settings (settings take effect immediately)

Include themes

12. Import the file.

13. Go to the CA Business Intelligence JasperReports Server Repository and verify that the reports appear in the list.

Changing the JNDI Password for CABI Server

As part of your organizations security policies, it might be necessary to change database passwords. Use the procedures in this article to change the password for the JNDI DataSource in CABI Server. CABI Server connects to a JDBC DataSource and a JNDI DataSource. The passwords for each of these Datasources must be the same.

- The password for the JDBC DataSource can be changed through the CABI Server UI administrator functions. For more information, see the CABI Server help.
- The password for the JNDI DataSource must be changed manually in the CABI Server property files. Choose one of the following procedures depending on your configuration.

Change the JNDI Password for External CABI Server

Use this procedure to change the password that is used for the UIM JNDI DataSource when you deploy an external CABI Server.

Follow these steps:

1. Go to your CABI server installation directory:

```
$cabi_install\buildomatic
```

2. Open the file:

- ```
default_master.properties
```
3. Locate the dbPassword property, and set the password in plain text.
  4. Change the property
 

```
encrypt.done=true
```

 to **encrypt=true**.
  5. Save the file.
  6. Use a Command Prompt window and go to:
 

```
$cabi_install\buildomatic
```
  7. Run the command: **js-ant refresh-config**
  8. Re-open the file:
 

```
default_master.properties
```
  9. Copy the value encrypted dbPassword.
  10. Go to your CABI server tomcat installation:
    - If CABI was installed with a bundled tomcat server, enter: **\$cabi\_install\apache-tomcat\webapps\<web\_app>\META-INF**
    - If CABI was installed with an existing tomcat server, enter: **\$existing\_tomcat\webapps\<web\_app>\META-INF**
 The variable **<web\_app>**, is the CABI Server web application name. The default web application name is jasperserver-pro.
  11. Open the
 

```
context.xml
```

 file.
  12. Locate the Resource section for
 

```
jdbc/uim
```

```
.
```
  13. Replace the password with the encrypted dbPassword you previously copied.
  14. Restart the Tomcat server.

### **Change the JNDI Password for Bundled CABI Server**

Use this procedure to change the password that is used for the UIM JNDI DataSource when you deploy CABI Server with CA UIM.

#### **Follow these steps:**

1. Go to your CABI server installation directory:
 

```
$NIM_ROOT\c\buildomatic
```
2. Copy the
 

```
$NIM_ROOT\c\buildomatic\build_conf\default\master.properties
```

 file to
 

```
$NIM_ROOT\c\buildomatic\default_master.properties
```

```
.
```
3. Open the file:
 

```
default_master.properties
```
4. Locate the dbPassword property and set the password in plain text.
5. Change the property
 

```
encrypt.done=true
```

 to **encrypt=true**.
6. Save the file.
7. Use a Command Prompt window to go to:

```
$NIM_ROOT\c\buildomatic
```

8. Run the command: **js-ant refresh-config**

9. Re-open the file:

```
default_master.properties
```

10. Copy the value encrypted dbPassword.

11. Open the file:

```
context.xml
```

12. Locate the Resource section for

```
jdbc/uim
```

13. Replace the password with the encrypted dbPassword you previously copied.

14. Restart the wasp probe.

## Reinstalling UIM Server

If you are reinstalling UIM Server over an existing installation, complete the following steps before rerunning the UIM Server installer:

### NOTE

No additional steps are required to reinstall Operator Console (OC), you can just run the Operator Console (OC) installer again.

### Follow these steps:

1. Deactivate then delete the trellis probe in either Admin Console or Infrastructure Manager.
2. Remove the trellis file directory (<UIM\_Installation>/probes/services/trellis).

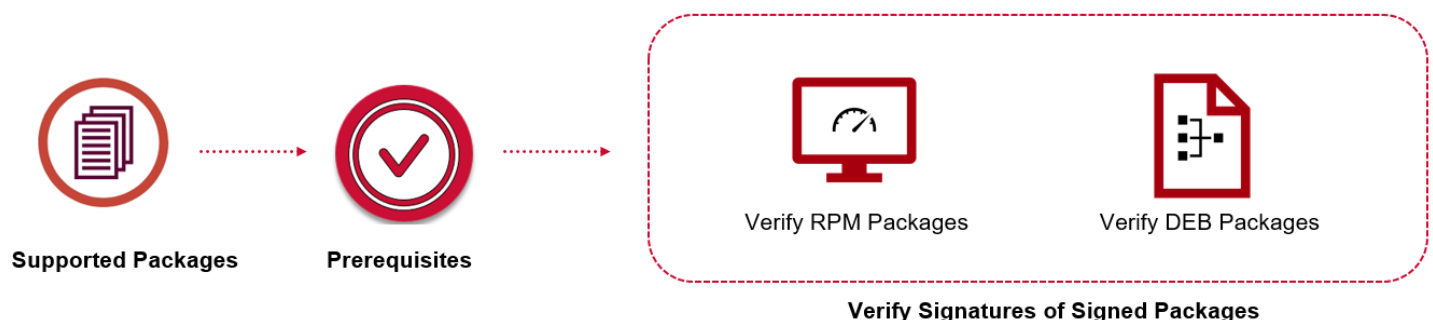
## Additional Topics

This section provides additional information that you might find useful:

### Packages Signed with GPG-Enabled Keys

(From UIM 20.3.3) This release of UIM provides the .rpm and .deb packages that are signed with the GNU Privacy Guard (GPG)-enabled keys. With this enhanced security mechanism, the integrity of the packages is maintained. This helps you verify that the packages that you are using for installation are the same ones that you have downloaded from the Support site. You can, therefore, be assured that no modifications have occurred in the packages after they were signed, thereby providing the quality and security assurance of the delivered package.

The following illustration outlines the process:



The following topics provide the detailed information:

## Supported RPM and DEB Packages

The following packages have been signed with the GPG-enabled keys:

- nimsoft-robot.i386.rpm
- nimsoft-robot.x86\_64.rpm
- nimsoft-robot+debian\_amd64.deb
- nimsoft-robot+ubuntu\_amd64.deb

### NOTE

Note that the previous versions of these packages are not signed with the GPG-enabled keys.

## Verify Prerequisites

Ensure that your environment meets the following requirements:

- GPG version 2.2.4 (or later)
- RPM version 4.0 (or later)
- dpkg-sig (for Debian/Ubuntu binaries)

## Verify the Signature of Signed RPM and DEB Packages

To verify the signature of the signed RPM and DEB packages, follow the appropriate procedure that is outlined in this section:

- [Verify the Signature of Signed RPM Packages](#)
- [Verify the Signature of Signed DEB Packages](#)

## Verify the Signature of Signed RPM Packages

Before you install the packages, you can verify the signature of the packages to ensure that they have not been tampered with. To do so, you must import the GPG public key into the GPG keyring and RPM database, and then verify the signatures.

### Follow these steps:

1. Verify that the signed .rpm packages and the GPG public key are available on your computer.

### NOTE

Download the GPG public key file from the [UIM Hotfix Index](#) site.

2. Use the following command to import the GPG public key into the GPG keyring:

```
[root@localhost ~]# gpg --import GPG-KEY-UIM-001
```

When you execute the command, you get the following response. Note that **imported: 1** in the command output signifies that the file has been imported successfully:

```
gpg: key 8B4FDD0849C0B447: public key "uimbuild (UIM GPG signing key) <uimbuild@example.net>" import
gpg: Total number processed: 1
gpg: imported: 1
```

3. Use the following command to import the GPG public key into the RPM database:

```
[root@localhost ~]# rpm --import GPG-KEY-UIM-001
```

This command does not display any output on the screen. Therefore, you can use the following command to verify that the public key file has been imported:

```
[root@localhost ~]# rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
```

When you execute this command, the following output is generated. Note that the segment *uimbuild (UIM GPG Signing) <uimbuild@example.net>* in the output shows that the public key file has been imported:

```
gpg-pubkey-fd431d51-4ae0493b --> gpg(Red Hat, Inc. (release key 2) <security@redhat.com>)
```

```
gpg-pubkey-2fa658e0-45700c69 --> gpg(Red Hat, Inc. (auxiliary key) <security@redhat.com>)
gpg-pubkey-b74246ce-58d281c9 --> gpg(uimbuild (UIM GPG Signing) <uimbuild@example.net>)
```

#### 4. Use the following command to verify the signature:

```
[root@localhost ~]# rpm -K nimsoft-robot.x86_64.rpm
```

When you execute the command, you get the following response. This response shows that the signature has been verified successfully:

```
nimsoft-robot.x86_64.rpm: rsa sha1 (md5) pgp md5 OK
```

You have successfully verified the RPM packages.

### Installing RPM Packages After Verification

Depending on your setup, you can then use the appropriate command to install the packages after they are verified:

- If you want to manually (directly) install the package, you can use the following command:

```
[root@localhost ~]# rpm -ivh nimsoft-robot.x86_64.rpm
```

When you execute the command, you get the following response. The response shows the successful installation of the package:

```
Preparing... ##### [100%]
Updating / installing...
 1:nimsoft-robot-9.31-1 ##### [100%]
```

- If the RPM package is part of the repository, you can use the following command to install the package:

```
[root@localhost ~]# yum install nimsoft-robot
```

When you execute the command, the following output is generated. The output shows that the installation is successful:

```
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.
Resolving Dependencies
--> Running transaction check
---> Package nimsoft-robot.x86_64 0:9.31-1 will be installed
--> Finished Dependency Resolution
```

Dependencies Resolved

```
=====
Package Arch Version Repository Size
=====
Installing:
nimsoft-robot x86_64 9.31-1 nimsoft-remote-repo 10 M
```

Transaction Summary

```
=====
Install 1 Package
```

```
Total download size: 10 M
Installed size: 64 M
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Warning: RPMDDB altered outside of yum.
```

```
Installing : nimsoft-robot-9.31-1.x86_64
1/1
Verifying : nimsoft-robot-9.31-1.x86_64
1/1
```

```
Installed:
nimsoft-robot.x86_64 0:9.31-1
```

```
Complete!
```

## Install RPM Packages without Verifying Signatures

If you do not want to verify the signatures of the signed RPM packages, you can proceed with the package installation without any verification. Depending on your setup, you can use the appropriate command to install the packages:

- If you want to manually (directly) install the package, you can use the following command. When you execute this command, the output of the command displays a warning that the signature has not been verified. You can ignore that warning and continue with the installation:

```
[root@localhost ~]# rpm -ivh nimsoft-robot.x86_64.rpm
```

The following response first shows the warning message and then proceeds with the installation:

```
warning: nimsoft-robot.x86_64.rpm: Header V4 RSA/SHA256 Signature, key ID 49c0b447: NOKEY
Preparing... ##### [100%]
Updating / installing...
1:nimsoft-robot-9.31-1 ##### [100%]
```

- If your package is part of the repository and you want to install from your repository, use the following command with the `--nogpgcheck` filter:

```
[root@ev022836 ~]# yum install --nogpgcheck nimsoft-robot
```

When you execute the command, you get the following response. Note that the package is installed successfully:

```
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.
Resolving Dependencies
--> Running transaction check
---> Package nimsoft-robot.x86_64 0:9.31-1 will be installed
--> Finished Dependency Resolution
```

```
Dependencies Resolved
```

```
=====
Package Size Arch Version Repository
=====
Installing:
nimsoft-robot 10 M x86_64 9.31-1 nimsoft-remote-
repo
```

```
Transaction Summary
```

```
=====
Install 1 Package
```

```
Total size: 10 M
Installed size: 64 M
Is this ok [y/d/N]: y
Downloading packages:
```

```
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Warning: RPMDB altered outside of yum.
 Installing : nimsoft-robot-9.31-1.x86_64
 1/1
 Verifying : nimsoft-robot-9.31-1.x86_64
 1/1

Installed:
 nimsoft-robot.x86_64 0:9.31-1
```

Complete!

If you do not use the `--nogpgcheck` filter, you are not allowed to proceed with the installation if the package signature is not verified. Note that the output displays a warning message and the installation does not proceed further:

```
Resolving Dependencies
--> Running transaction check
---> Package nimsoft-robot.x86_64 0:9.31-1 will be installed
--> Finished Dependency Resolution
```

Dependencies Resolved

```
=====
```

| Package<br>Size       | Arch   | Version | Repository          |
|-----------------------|--------|---------|---------------------|
| Installing:           |        |         |                     |
| nimsoft-robot<br>10 M | x86_64 | 9.31-1  | nimsoft-remote-repo |

Transaction Summary

```
=====
```

Install 1 Package

Total download size: 10 M

Installed size: 64 M

Is this ok [y/d/N]: y

Downloading packages:

```
warning: /var/cache/yum/x86_64/7Server/nimsoft-remote-repo/packages/nimsoft-robot.x86_64.rpm: Header V3
RSA/SHA256 Signature, key ID 4b4b47fd: NOKEY=====] 39 kB/s | 10 MB 00:00:00 ETA
```

Public key for nimsoft-robot.x86\_64.rpm is not installed

nimsoft-robot.x86\_64.rpm

| 10 MB 00:07:23

Public key for nimsoft-robot.x86\_64.rpm is not installed

### Verify the Signature of Signed DEB Packages

Before you install the DEB packages, you can verify the signature of the packages to ensure that they have not been tampered with. To do so, import the GPG public key into the GPG keyring and APT database, and then verify the signature.

**Follow these steps:**

1. Verify that the signed .deb packages and the GPG public key file are available on your computer.

**NOTE**

Download the GPG public key file from the [UIM Hotfix Index](#) site.

2. Use the following command to import the GPG public key into the GPG keyring:

```
[root@localhost ~]# gpg --import GPG-KEY-UIM-001
```

When you execute the command, you get the following response. Note that **imported: 1** in the command output signifies that the file has been imported successfully:

```
gpg: key 8B4FDD0849C0B447: public key "uimbuild (UIM GPG signing key) <uimbuild@example.net>" import
gpg: Total number processed: 1
gpg: imported: 1
```

3. Use the following command to import the GPG public key into the APT database:

```
[root@localhost ~]# apt-key add GPG-KEY-UIM-001
```

When you execute the command, you get the following response. Note that **OK** in the command output signifies that the file has been added successfully:

```
OK
```

4. Use the following command to verify the signature:

```
[root@localhost ~]# dpkg-sig --verify nimsoft-robot+debian_amd64.deb
```

When you execute the command, you get the following response. Note that **GOODSIG** in the command output signifies that the verification is successful:

```
Processing nimsoft-robot+debian_amd64.deb...GOODSIG _gpgbuilder B16265877A80C8FB40327C4A681EFD1DE5124174
1523440651
```

You have successfully verified the signature.

**Install DEB Packages After Verification**

Depending on your setup, you can use the appropriate command to install the packages after they are verified:

- If you want to manually (directly) install the package, you can use the following command:

```
[root@localhost ~]# dpkg -i nimsoft-robot+ubuntu_amd64.deb
```

When you execute the command, you get the following response. The response shows the package installation:

```
Selecting previously unselected package nimsoft-robot.
(Reading database ... 121866 files and directories currently installed.)
Preparing to unpack nimsoft-robot+ubuntu_amd64.deb ...
Unpacking nimsoft-robot (9.31) ...
Setting up nimsoft-robot (9.31) ...
Processing triggers for ureadahead (0.100.0-20) ...
```

- If the DEB package is part of the repository, you can use the following command to install the package:

```
root@ev02252:~# apt-get install nimsoft-robot
```

When you execute the command, the following output is generated. The output shows the installation:

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
 grub-pc-bin
Use 'apt autoremove' to remove it.
The following NEW packages will be installed:
 nimsoft-robot
0 upgraded, 1 newly installed, 0 to remove and 99 not upgraded.
Need to get 9051 kB of archives.
```

```

After this operation, 12.3 MB of additional disk space will be used.
Get:1 http://10.xx.xxx.xxx trusty/main amd64 nimsoft-robot amd64 9.20 [9051 kB]
Fetched 9051 kB in 1s (17.5 MB/s)
Selecting previously unselected package nimsoft-robot.
(Reading database ... 123945 files and directories currently installed.)
Preparing to unpack .../nimsoft-robot_9.20_amd64.deb ...
Unpacking nimsoft-robot (9.20) ...
Processing triggers for ureadahead (0.100.0-20) ...
Processing triggers for systemd (237-3ubuntu10.38) ...
Setting up nimsoft-robot (9.20) ...
update-rc.d: warning: start and stop actions are no longer supported; falling back to defaults

```

### **Install DEB Packages without Verifying Signatures**

If you do not want to verify the signatures of the signed DEB packages, you can proceed with the package installation without any verification. Depending on your setup, you can use the appropriate command to install the package:

- If you want to manually (directly) install the package, you can use the following command:

```
[root@localhost ~]# dpkg -i nimsoft-robot+ubuntu_amd64.deb
```

The following response shows the installation process:

```

Selecting previously unselected package nimsoft-robot.
(Reading database ... 121866 files and directories currently installed.)
Preparing to unpack nimsoft-robot+ubuntu_amd64.deb ...
Unpacking nimsoft-robot (9.31) ...
Setting up nimsoft-robot (9.31) ...
Processing triggers for ureadahead (0.100.0-20) ...

```

#### **NOTE**

This command was executed on the Ubuntu 8.04.2 LTS version. In that version, no specific warning that the signature of the package has not been verified is displayed.

- If your package is part of the repository and you want to install from your repository, use the following command with the `--allow-unauthenticated` filter:

```
root@ev02252:~# apt-get --allow-unauthenticated install nimsoft-robot
```

## **Addressing CVE-2018-13820 and CVE-2018-13819 Vulnerabilities**

This release of CA UIM addresses CVE-2018-13820 and CVE-2018-13819 vulnerabilities. CVE-2018-13820 is about a hard-coded passphrase, which is now externalized to `data_engine`. The probes that connect to the database now use the externalized passphrase. CVE-2018-13819 is about a hard-coded secret key in the ppm probe, which is also addressed as a part of this release. The minimum versions of the probes updated for this functionality are below:

- ace 9.03



**NOTE**

The ace probe has been deprecated in UIM 20.3.3.

- alarm\_routing\_service 10.20
- apmgw 3.22
- audit 9.03
- axagateway 1.35
- cabi 3.32
- cisco\_ucm 2.00
- cm\_data\_import 9.02
- data\_engine 9.02
- discovery\_agent 9.02
- discovery\_server 9.02
- ems 10.20
- maintenance\_mode 9.02
- mon\_config\_service 9.02
- mpse 9.02
- nas 9.06
- nis\_server 9.03
- ppm 3.49
- qos\_processor 9.02
- sla\_engine 9.02
- telemetry 1.22
- trellis 9.02
- udm\_manager 9.02
- uimapi 9.02
- usage\_metering 9.21
- wasp 9.02
- webservices\_rest 9.02

## Upgrading to Microsoft Visual C++ Redistributable for Visual Studio 2017

UIM uses Microsoft Visual C++ Redistributable for Visual Studio 2017 (VS 2017) for the following affected probes and packages:

- audit 9.03
- cdm 6.33
- data\_engine 9.02
- dirsrv 3.17
- distsrv 7.96
- hub 7.96
- logmon 4.00
- nas 9.06
- net\_connect 3.36
- ntevl 4.32
- ntperf 2.09
- ntservices 3.42
- processes 4.63
- pu 7.96
- robot\_exe 7.96
- robot\_update 7.96
- rsp 5.353

The above-listed probe versions use the VS 2017 package 1.0 (vs2017\_vcrist\_x86 1.0 and vs2017\_vcrist\_x64 1.0) as a dependency. This dependency on the 1.0 package causes Windows operating system to restart on the robot where the probe is deployed. In the VS 2017 package version 1.0, there is no "norestart" option specified in the Post Install command. Therefore, the Post Install might trigger operating system reboot as part of the package installation. We recommend you to download the vs2017\_vcrist\_x86 1.01 and vs2017\_vcrist\_x64 1.01 package (as required) from the Nimsoft archive to avoid the computer auto-restart for the dependent probes. For a detailed workaround, see the KB Article [Windows OS Reboot After Probe Deployment](#).

### **Considerations**

Review the following considerations:

- Some of these impacted probes have newer versions available that are no longer dependent on the VS 2017 1.0 package. These updated versions are, by default, dependent on the VS 2017 1.01 package (vs2017\_vcrist\_x86 1.01 and vs2017\_vcrist\_x64 1.01). This support helps ensure that the minimum version of the VS 2017 package is equal to or greater than 1.01. With this dependency on the version 1.01, the computer is no longer getting restarted automatically when installing the VS 2017 package. That is, with v1.01, no auto-restart of the computer happens. These probes are audit 9.04, cdm 6.34, distsrv 7.97, hub 7.97, pu 7.97, robot\_exe 7.97, and robot\_update 7.97.
- For other probes (not listed) that use the EOL Microsoft Visual C++ Redistributable or for older versions of the impacted probes, you must download and deploy the required EOL Microsoft Visual C++ Redistributable package (for example, vs2008\_redist\_x86) from the Archive.
- If you want to use the above-listed probes with the older UIM releases (for example, prior to 9.0.2), ensure that you download and deploy the required Microsoft Visual C++ 2017 Redistributable package 1.01 that is available in the Nimsoft web archive.
- Infrastructure Manager is not in the scope for the EOL Microsoft Visual C++ Redistributable dependency removal.
- Hub is not supported on 32-bit Windows and Linux platforms in this case.
- If you use the automated\_deployment\_engine (ADE) probe to deploy the new robot available in this release onto your Windows computers, the robot is deployed successfully but the new "Microsoft Visual C++ Redistributable for Visual

Studio 2017" might not be installed. To address this issue, we recommend that you follow the information in the article [Update for Universal C Runtime in Windows \(KB2999226\)](#) before you try to install the new robot using ADE.

- Though 9.0.2 removes the dependency on the EOL Microsoft Visual C++ Redistributable for the affected UIM components, it does not delete them from the computer. It is possible that some other application in your environment is using those old redistributables.
- In UIM releases prior to 9.0.2, if you want to upgrade a secondary robot to 7.96, you must import robot 7.96 and Microsoft Visual C++ 2017 Redistributable package 1.01 (for example, vs2017\_vccredist\_x86 1.01)
- In UIM releases prior to 9.0.2, if you want to upgrade your secondary hub to 7.96, you must import and deploy hub 7.96, robot 7.96, and Microsoft Visual C++ 2017 Redistributable package 1.01 (for example, vs2017\_vccredist\_x86 1.01). Also, upgrade any robots that point to the secondary hub.

## Addressing Jackson Vulnerabilities

This release addresses the common vulnerabilities and exposures by updating the jackson-databind libraries. Jackson-databind is a Java library used to parse JSON and other data formats. The vulnerability occurs when the user input is improperly validated, which may allow an attacker to perform code execution by providing maliciously crafted input. The following Common Vulnerabilities and Exposures have been addressed:

- CVE-2017-17485
- CVE-2018-14720
- CVE-2018-14721
- CVE-2017-7525
- CVE-2017-15095
- CVE-2018-14718
- CVE-2018-14719
- CVE-2018-19360
- CVE-2018-19361
- CVE-2018-19362
- CVE-2018-7489
- DSA-4037
- DSA-4004
- DSA-4190
- DSA-4114
- CVE-2018-5968
- CVE-2018-1000873

The following are the minimum versions of the items that have been explicitly updated for this functionality:

- adminconsoleapp 9.10
- ad\_response\_mcs\_templates 1.82
- alarm-routing-service 9.03
- apache\_mcs\_templates 1.72
- automated\_deployment\_engine 9.10
- cdm\_mcs\_templates 6.42
- ems 10.21
- exchange\_monitor\_mcs\_templates 5.33
- iis\_mcs\_templates 1.92
- mcs\_usm\_patch 9.10
- mcs\_ws 9.10
- mcs 9.03
- mcs-cli 9.10
- mps\_webapp 8.5.6
- mysql\_mcs\_templates 1.53
- net\_connect\_mcs\_templates 3.38
- oracle\_mcs\_templates 5.35
- ppm 3.51
- restmon-uim 1.38
- rsp\_mcs\_templates 5.35
- sharepoint\_mcs\_templates 1.84
- sqlserver\_mcs\_templates 5.42
- telemetry 1.23
- uimapi 9.10
- wasp 9.10
- webservices\_rest 9.10

## Enhanced security.cfg

CA UIM 20.3.0 provides the following enhancements in the security.cfg file:

- Uses a strong hashing algorithm PSV2 (PBKDF2) for password hashing in hub 9.31/9.31S.
- Encrypts user information (for example, email ID, phone, profile, permissions) in hub 9.31/9.31S for users available in the security.cfg file.

The complete information is covered as follows:

### Parameters

The following parameters let you control the user password hashing and user information encryption behavior:

- **psv2\_password:** Lets you specify whether you want to convert the user passwords created with PSV1 (MD5) to PSV2 (PBKDF2). The applicable parameter values are *yes* and *no*. You add this parameter to 9.31/9.31S hub.cfg.
- **encrypt\_user\_info:** Lets you specify whether you want to encrypt the user information. The applicable parameter values are *yes* and *no*. You add this parameter to 9.31/9.31S hub.cfg.

#### **NOTE**

- You **MUST** take a backup of the security.cfg and security.dta files before enabling this functionality.
- You **cannot** revert the changes in security.cfg after the password hashing is changed to PSV2. Therefore, you must back up the existing files.

**Considerations**

Review the following considerations:

- When the encrypt\_user\_info parameter is enabled, the user information in security.cfg is propagated in a non-encrypted format to the hubs that are lower than 9.31/9.31S. For 9.31/9.31S hubs, the user information is propagated in the encrypted format.
- When you enable the encrypt\_user\_info parameter on any 9.31/9.31S hub, then all 9.31/9.31S (and above) hubs will get the encrypted security.cfg file irrespective of the fact whether this parameter is enabled on those hubs or not. However, security propagation must be enabled on those hubs. Furthermore, in the case of primary hubs, security propagation always happens.
- Once you enable the encrypt\_user\_info parameter on any 9.31/9.31S hub and the user information is encrypted, it is recommended that you do not go back to the decrypted state unless it is very important to do so. The reason is that the encrypted security.cfg file is already propagated to all the hubs (9.31/9.31S and above)
- If you do not add these parameters to 9.31/9.31S hub.cfg, CA UIM follows the **no-no** scenario, which is the first row in the table.

**Scenarios**

The following table summarizes the information based on the values of the two parameters:

| psv2_password | encrypt_user_info | Behavior                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no            | no                | <p>In this case:</p> <p><b>psv2_password=no</b></p> <ul style="list-style-type: none"> <li>• PSV1 password is not converted to PSV2 when a user logs in to hub 9.31/9.31S because psv2_password is set to no. <ul style="list-style-type: none"> <li>– Any new user created in hub 9.31/9.31S uses PSV2 for password by default. This user cannot log in to 7.97 (or earlier).</li> <li>– Users coming from hub 7.97 (or earlier) use PSV1 password. Their password is not converted to PSV2.</li> </ul> </li> </ul> <p><b>encrypt_user_info=no</b></p> <ul style="list-style-type: none"> <li>• Other user information is not encrypted in hub 9.31/9.31S because encrypt_user_info is set to no. <ul style="list-style-type: none"> <li>– For all hub versions, security.cfg includes user information in a non-encrypted format because encrypt_user_info is set to no. This file is propagated to all hub versions with the same non-encrypted user information.</li> </ul> </li> </ul> |

|     |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no  | yes | <p>In this case:</p> <p><b>psv2_password=no</b></p> <ul style="list-style-type: none"> <li>• PSV1 password is not converted to PSV2 when a user logs in to hub 9.31/9.31S because psv2_password is set to no. <ul style="list-style-type: none"> <li>– Any new user created in 9.31/9.31S uses PSV2 for password by default. This user cannot log in to 7.97 (or earlier).</li> <li>– Users coming from hub 7.97 (or earlier) use PSV1 password. Their password is not converted to PSV2.</li> </ul> </li> </ul> <p><b>encrypt_user_info=yes</b></p> <ul style="list-style-type: none"> <li>• User information is encrypted while propagating the security.cfg file to hub 9.31/9.31S.</li> <li>• For hub versions lower than 9.31/9.31S, the user information is decrypted while propagating the security.cfg file to the lower hub versions (7.97 or earlier).</li> </ul>                                                                                                                                                                                                                                                                                           |
| yes | no  | <p>In this case:</p> <p><b>psv2_password=yes</b></p> <ul style="list-style-type: none"> <li>• PSV1 password is converted to PSV2 when a user with PSV1 password logs in to hub 9.31/9.31S because the parameter is set to yes. <ul style="list-style-type: none"> <li>– Any new user created in hub 9.31/9.31S uses PSV2 for password by default. This user cannot log in to 7.97 (or earlier).</li> <li>– Users coming from hub 7.97 (or earlier) use PSV1 password. Now, their password is converted to PSV2 when they log in to hub 9.31/9.31S. After logging in to 9.31/9.31S, they cannot log in back to 7.97 (or earlier) because of the PSV1 to PSV2 conversion.</li> </ul> </li> </ul> <p><b>encrypt_user_info=no</b></p> <ul style="list-style-type: none"> <li>• Other user information is not encrypted in hub 9.31/9.31S because encrypt_user_info is set to no. <ul style="list-style-type: none"> <li>– For all hub versions, security.cfg includes user information in a non-encrypted format because encrypt_user_info is set to no. This file is propagated to all hub versions with the same non-encrypted user information.</li> </ul> </li> </ul> |

|     |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| yes | yes | <p>In this case:</p> <p><b>psv2_password=yes</b></p> <ul style="list-style-type: none"> <li>• PSV1 password is converted to PSV2 when a user with PSV1 password logs in to hub 9.31/9.31S. <ul style="list-style-type: none"> <li>– Any new user created in hub 9.31/9.31S uses PSV2 for password by default. This user cannot log in to 7.97 (or earlier).</li> <li>– Users coming from hub 7.97 (or earlier) use PSV1 password. Now, their password is converted to PSV2 when they log in to hub 9.31/9.31S. After logging in to 9.31/9.31S, they cannot log in back to 7.97 (or earlier) because of the PSV1 to PSV2 conversion.</li> </ul> </li> </ul> <p><b>encrypt_user_info=yes</b></p> <ul style="list-style-type: none"> <li>• User information is stored in an encrypted format while propagating the security.cfg file to hub 9.31/9.31S. <ul style="list-style-type: none"> <li>– For hub versions lower than 9.31/9.31S, the user information is decrypted while propagating the security.cfg file to the lower hub versions (7.97 or earlier).</li> </ul> </li> </ul> |
|-----|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example Snippet

The following example shows that the user information is now available in the encrypted format in security.cfg for hub 9.31/9.31S:

```
<users>
<phal>
password =
 $psv2$250406$wm21yEX93qHfSpnjfnzykUQQZ411SLbIOClbh0ikSJ3vyzJ0VrKcaWmd8H3HLaiMRRQJMFbVd4soZWY
+4tFJdwCL5nYDYan7WIKyo6e18tT3x/xguQ==
mobile = cUkLtAi5N59wz9fX7Q==
email = 9Ou/8qEA/O/8sYAJRw==
profile = GL9SVrpTnj46UB6igg==
phone = cUkLtAi5N59wz9fX7Q==
acl = FLKl1R+JomZPgag==
</phal>
...
</users>
```

### Restore the Backed-Up security.cfg File

If you want to restore the backed-up security.cfg file, you can do so.

#### NOTE

The secdit file is applicable only for Windows. For Linux, the only way to restore the setup is to manually copy the backed-up files (security.cfg and security.dta).

#### Follow these steps:

1. Get the secdit file from Support and put it in the ..\Nimsoft\hub folder.

2. Disable both the parameters (*psv2\_password* and *encrypt\_user\_info*) in the *hub.cfg* file.
3. Stop the Nimsoft Robot watcher service.
4. Close all instances of IM, Admin Console, and other components, if any.
5. Delete the *hubs.sds* and *robot.sds* files from the *..\Nimsoft\hub* folder.
6. Start the Nimsoft Robot watcher service.
7. Run *secedit.exe*.
8. Enter the CA UIM administrator user and password. A notepad with the name *security.txt* is opened. This includes security information.
9. Copy the contents of the backed-up *security.cfg* file into the opened notepad.
10. Save the notepad.
11. Restart the Nimsoft Robot watcher service.
12. Log in to IM to verify the configuration changes, ACLs, users, and other settings.

## Adopting OpenJDK

CA Technologies, a Broadcom Company, is moving towards adopting more open source technologies in its products. As a part of this strategy, various products have started using open-source implementations of Java. To align with this corporate direction, UIM 9.2.0 (or later) has adopted OpenJDK, replacing Oracle JDK.

Review the following sections to quickly understand the OpenJDK adoption:

### Upgrading UIM Server

- When you upgrade the UIM Server, the upgrade process automatically updates the existing Oracle JDK to OpenJDK on the primary hub.
- The upgrade process removes the existing Oracle JDK.
- The *java\_jre* probe package is made available in the archive.

### Upgrading Operator Console

- When you upgrade the Operator Console (OC), the upgrade process automatically updates the existing Oracle JDK to OpenJDK on the Operator Console (OC) server.
- Restart the Operator Console (OC) robot so that the new OpenJDK is picked up.

### Deploying OpenJDK on Robots

- A new version of the *java\_jre* probe package is available for download from the web archive.

#### **NOTE**

For robots deployed in Solaris, a separate package *jre\_solaris 2.00* is available.

- Download and deploy the *java\_jre* probe to the robot to replace the existing Oracle JDK with OpenJDK.
- Verify that the update is complete by ensuring that the following parameter values are updated to *jre/jre8u252b09* (for example) in the *robot.cfg* file:
  - `NIM_JRE_HOME = jre/jre8u252b09`
  - `NIM_JRE_HOME_1_8 = jre/jre8u252b09`
- Restart the robot. Restarting the robot ensures that all the Java probes that are deployed on the robot start using the new OpenJDK.
- You can manually delete the older *java\_jre* (Oracle-licensed JRE) after successfully upgrading to OpenJDK run-time environment, if required.



# Upgrading

Upgrading to the most current release of UIM is critical to your success and staying ahead of the competition. Your decision to upgrade should be part of your overall plan to achieve the best customer experience, achieve product development goals, allocate resources, and appropriate budget over time.

## Top Reasons to Upgrade

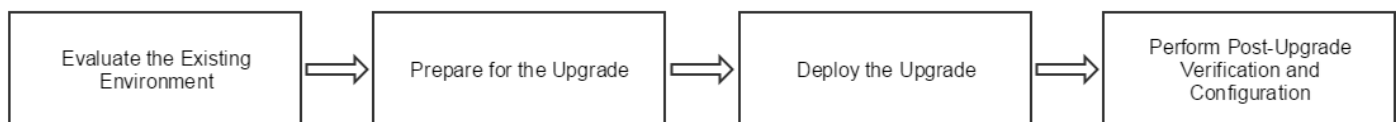
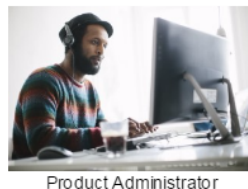
Here are the top reasons and benefits for you to adopt and upgrade to the latest software release:

- **Take advantage of the new and enhanced features.** Your team wants to use the UIM capabilities that are only available with the new release. For example, this release provides an enhanced web-based user interface for both Operator and Administrator personas.
- **Get the latest compatibility updates.** Development can create, innovate, and integrate knowing that UIM is compatible with the latest releases of operating systems, browsers, client applications, and third-party solutions. For example, your current UIM version does not support Java 8 and you need to pass internal audits for security compliance. Therefore, you make the business decision to upgrade.
- **Keep current.** Software releases can only be supported for a limited time. By upgrading, you ensure that you have the technical expertise and support when it is needed. For example, your current version of UIM is end of service soon and you want to take advantage of new enhancements such as CA Business Intelligence reporting and the new architecture for hub scalability.

The latest version of UIM gives you more of what you need to support key role and cross role relationships in fast-paced IT environments. The following image shows how the Product Administrator upgrades UIM.

**Figure 17: Image showing the upgrade process**

### CA UIM Upgrade Process



[Next Step: Evaluate the Existing Environment >](#)

## Upgrade Step 1: Evaluate the Existing Environment

### NOTE

As part of the upgrade process, the installer runs an SQL query to verify that your environment is ready for the upgrade. This query is run by the installer whether you are an MCS user or not.

If your SQL query results in the message, 'Contact CA support before upgrading to UIM x.xx,' contact Support before proceeding. Attach to the case, in csv format, extracts of the following tables:

- ssrv2template
- ssrv2devicegroup
- ssrv2field
- ssrv2profile
- ssrv2ConfigValue

If your SQL query results in the message, 'It is safe to upgrade to UIM x.xx,' continue with the upgrade.

In this first step of the upgrade process, you review the existing UIM environment and determine that you are ready to upgrade. Review your UIM components to determine the following:

- What databases you have.
- What environment you have (standalone mode or failover mode).
- What customizations you have.

### **Gather the Appropriate Information**

Check the various areas of your environment. Gather and note the appropriate information, which is used later when you run the upgrade.

1. Identify the target environment to be upgraded. For example, you might upgrade your deployment environment. Complete these steps.
  - a. Determine whether the environment runs on Windows or Linux.
  - b. Determine whether the UIM environment runs in standalone or failover mode.
  - c. Identify the number of servers in the UIM setup that need to be upgraded, including any failover servers.
  - d. Identify the components that need to be upgraded. For example, you need to upgrade one primary hub, one secondary hub, the Reporting Portal, and the robots.
  - e. Identify whether the upgrade will occur on existing servers, or on new servers.
2. Identify where the UIM database is installed and what type of database server is used. Verify whether you want to migrate the UIM database or the platform operating system from an existing platform.
3. Identify applications that are configured for monitoring.
4. Verify what type of probes are being used. Identify how many probes, if any, that must be upgraded to help resolve any existing issues.
5. Identify and note any customizations that you have implemented in your environment

### **Create the Health Check Remediation Plan**

A health check is a detailed diagnostic exercise that evaluates the existing health of UIM products and their underlying infrastructure. The health check report identifies all known problems and provides a suggested remediation plan for all problems that need to be fixed before the upgrade can successfully run. The health check helps you verify that you are upgrading in a working system. The health check reviews the current system inventory by environment, the current state sizing, any performance issues, customizations, and integrations.

You can use the health check report and fix the issues. You can engage CA Services to help you.

#### **TIP**

We recommend that you contact your CA Services representative and let them know that you are starting the upgrade process. Discuss with your representative your unique upgrade challenges and gather information and best practices that you can use for your specific environment.

For more information about the health check and how you can benefit during your upgrade, work with the [CA Services Support](#).

[Next Step: Prepare for the Upgrade >](#)

## Upgrade Step 2: Prepare for the Upgrade

In this second step of the upgrade process, you complete the following two important tasks:

1. Plan for the upgrade. When planning for the upgrade, you refer to the compatibilities and other important documents to ensure that your components, environment, hardware, and operating system requirements are prepared and are compliant for a successful upgrade. Then, a sizing plan is created using sizing calculators.
2. Complete important pre-upgrade tasks. Verify custom configurations and integrations, and define a backup, recovery, and failover plan.

### Plan for the Upgrade

After the existing UIM environment is evaluated, you plan for the upgrade. Use the following documents and reference information to prepare and plan.

1. [Unified Infrastructure Management Compatibility Matrix](#). This important document provides a compatibility matrix to help you identify the components that are compatible with the different versions of UIM.

#### **NOTE**

You should carefully read all sections of the compatibility matrix. You should pay close attention to the following highlighted sections.

- **Component Support Matrix.** Identifies new components that are supported and other components that are no longer supported.
  - **Supported Upgrade Paths.** Highlights supported upgrade paths for each UIM component. Some component versions required that you upgrade to a previous version before upgrading to the most current version.
2. [UIM Release Notes](#), available in the product documentation. This important document provides the latest information about new features, enhancements to existing features, and defects fixed.

#### **NOTE**

You should carefully read all sections of the UIM Release Notes. You should pay close attention to the following highlighted sections.

- **New Features.** Highlights the new features. New product functionality can impact the existing functionality. Review this section so you are aware of any actions that you might need to take so that your existing functionality works as expected.
  - **Support Updates.** Highlights software support updates. Be aware of any software that is no longer supported.
  - **Updated Probes and Packages List.** Be aware of the component version number for the probes and packages that are installed.
  - **Resolved Issues.** Be aware of the issues resolved and how that can impact your upgrade.
  - **Known Issues.** Be aware of known issues and how that can impact your upgrade.
3. [CA Business Intelligence JasperReports Server with UIM Release Notes](#), available in the product documentation.

#### **NOTE**

You should carefully read all sections of the CA Business Intelligence Release Notes. You should pay close attention to the following highlighted sections.

- **Installation and Upgrade Procedures.** Read this section and be aware of the correct upgrade procedures.
  - **UIM Environment Requirements.** CA Business Intelligence requires certain components that you should be aware of for a successful upgrade.
  - **Hardware Requirements for CABI Server.** Be aware of any CA Business Intelligence hardware requirements.
  - **New Features and New Packages.** Be aware of the new features and packages that can impact your upgrade.
  - **Resolved Issues.** Be aware of the issues that are resolved and how that can impact your upgrade.
  - **Known Issues.** Be aware of known issues and how that can impact your upgrade.
4. [Probe-Specific Release Notes](#), available in the product documentation.

#### NOTE

For any probe that you have deployed, carefully read their Release Notes. You should pay close attention to the following highlighted sections.

- **Installation Considerations.** Be aware of any probe-specific installation considerations.
  - **Upgrade Considerations.** Be aware of any probe-specific upgrade considerations.
5. [Knowledge base \(KB\) articles](#), available on the Unified Infrastructure Management page of Broadcom Support Online. Become knowledgeable and be aware of any upgrade-related KB articles on Broadcom Support Online that can impact your upgrade.
6. Identify factors affecting the capacity of each UIM component and size the resources to be allocated. For example, consider the following information:
- Hubs. The capacity of the hubs depends on how they will be deployed. Determine if you need to deploy the hub as a standalone system or install it in a multi-tiered environment. In addition, there are multiple factors to consider when planning hub deployment. For example, the number of devices, scalability, the number of metrics and alarms that robots report, probe-specific requirements, and the geographic locations including DMZ telling requirements.
  - UIM Database. The UIM database stores device inventory, alarms, and QoS data. Determine if you need to perform capacity planning for the UIM database. If so, understand that the UIM database stores many statistics-based inputs. The Database Disk Space Calculator, which is part of the health check, sizes the UIM database and estimates the total metric load. This information can help you estimate the number of metrics that hubs, probes, and the database can handle based on your environment. The health check makes recommendations, provides the future sizing criteria, and delivers a roadmap to that future state.
7. We recommend that you contact your CA Services representative and let them know that you are starting the upgrade process. Discuss with your representative your unique upgrade challenges and gather information and best practices that you can use for your specific environment.

### **Complete Important Pre-Upgrade Tasks**

A backup and recovery plan is crucial when planning for the upgrade.

#### **Follow these steps:**

1. Gather, note, and keep in a safe place the UIM Administrator and UIM Database accounts.
2. Note any custom configurations that are made to the hub. If necessary, you can restore to the previous version in case you encounter unexpected issues or behavior.
3. Take a snapshot of the server.
4. Make a copy of the key directories. For example, directories for any integrated products, and the UIM infrastructure servers and their directories. After the hubs are upgraded, this information will help you set up the UIM environment that is part of the post-upgrade configuration.
5. Note any custom scripts that were deployed.

6. Back up the appropriate systems. For example, you previously took a snapshot of the server as part of the recovery plan. Now, back up and rename the previous UIM directory.
7. Remove any custom probes in the probe archive, but leave the infrastructure probes. After the upgrade is complete, you will selectively move the customized probes back into the archive.
8. Back up the UIM database.
9. Take a backup of the existing licenses before upgrading to UIM 20.3.0. In UIM 20.3.0, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with UIM 20.3.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required). For more information about how to take a backup of the licensing information, see [Back Up the Licensing Information](#).

[Next Step: Deploy the Upgrade >](#)

## Upgrade Step 3: Deploy the Upgrade

In this third step of the upgrade process, you obtain the new versions of the UIM installers and upgrade to the new version.

### Upgrade UIM and All Associated Components

To successfully upgrade UIM and all associated components, complete the steps that are explained in the following articles.

#### NOTE

- For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.
- UIM 20.3.1 is a patch release. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes separate standalone artifacts that you can use to upgrade the respective components. For more information about the artifacts that are available as a part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article
- If you are upgrading from UIM 9.0.2/9.2.0 to UIM 20.3.0 and want to use the [secure hub and robot](#) option that is available in the UIM 20.3.0 server upgrade installer, we recommend that you first upgrade UMP to OC and CABI before you start the secure hub and robot upgrade process.
- UIM uses OpenJDK instead of Oracle JDK. For more information about the OpenJDK usage in UIM, see [Adopting OpenJDK](#).

### I do not want to upgrade because I have multiple hub tiers and thousands of probes

In this situation, we recommend a phased upgrade approach. First, upgrade your primary hub and failover hubs, if deployed, the Unified Management Portal (UMP) to Operator Console (OC). You can schedule the upgrade of secondary hubs, and then gradually upgrade your robots and probes based on your business needs.

[Next Step: Upgrade the UIM Server >](#)

## Upgrade UIM Server

This article describes the process for upgrading UIM Server.

---

## Contents

### **Before You Begin**

Complete the following tasks before you upgrade UIM Server.

### **Verify Your Upgrade Path**

Ensure that you follow a supported upgrade path described in the [Compatibility Support Matrix](#).

### **Verify Your RESTful Web Services Requirements**

Your UIM RESTful web services might require a specific version of UIM to function properly. Refer to the [RESTful web services](#) documentation in Probes Documentation to see if an update is required for this version of UIM.

### **Back up the Primary Hub Configuration**

Save a copy of the hub.cfg file in the <UIM\_Server>\hub folder. Optimal timeout parameters for the updated hub are set during the update, overwriting existing timeout settings. CA recommends running the updated hub with these optimal values for improved performance. However, if you wish to revert to the old timeout settings for any reason, keep a backup of the old Hub configuration file.

### **Remove Any Customized Probes in Your Probe Archive**

If you have developed custom probes using one of the UIM probe SDKs, move or delete them from your archive before starting an upgrade. After your upgrade is complete, you can move your custom probes back into the archive.

### **Deactivate distsrv Forwarding**

If you have package forwarding set up for the distsrv probe, deactivate it before upgrading. Also, ensure that the forwarding on the distsrv probe is disabled until the complete UIM upgrade is done for primary hub, UMP to OC, and CABI.

### **Follow these steps:**

1. In Admin Console, click the 3-dot menu next to the distsrv probe, select **Configure**.
2. Click the **Forwarding** folder. If any Forwarding records have **All** in the **Type** column, deactivate forwarding. For other types of records (**Specific**, **Update**, or **Licenses**) you do not need to deactivate forwarding.
3. Deselect **Forwarding active**.

#### **NOTE**

From UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with the latest UIM to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).

### **Turn off Anti-Virus Scanning**

Turn off any anti-virus scanners running on the server. These scanners can significantly slow down the installation. You can turn your anti-virus scanner back on after the upgrade is complete.

### **Prepare Your UIM Database**

Depending on the database software you are using to host the UIM database, you may have additional requirements.

## Microsoft SQL Server

Turn off index maintenance in data engine. On very large tables (over 10 GB), running index maintenance will take longer than expected. We recommend that users disable this feature when upgrading to a newer release of UIM, then re-enable it to run during off-peak hours, carefully monitoring the index maintenance processes. This configuration can be done in Admin Console or Infrastructure Manager.

## Oracle

- If you are upgrading to this release, as the Oracle database administrator, execute the following command to grant permission to the UIM user:  

```
Grant execute on DBMS_CRYPTO TO <UIM_USER>;
```
- (Upgrade from NMS 7.6 only) If you are upgrading from NMS v7.6 to UIM 8.0 or later, complete the following procedure. If you are running a version of UIM and are upgrading to a newer release, you are not required to complete the following procedure.

### Follow these steps:

1. a. As SYSDBA, execute:
 

```
grant execute on dbms_redefinition to <UIM_USER>;
grant create type to <UIM_USER>;
grant execute any type to <UIM_USER>;
grant under any type to <UIM_USER>;
grant select any table to <UIM_USER>;
grant alter any table to <UIM_USER>;
grant create any table to <UIM_USER>;
grant drop any table to <UIM_USER>;
grant lock any table to <UIM_USER>;
```
- b. Turn off and purge the Oracle recycle bin.

### WARNING

If you are upgrading from NMS 7.6, the upgrade will fail if you do not purge the recycle bin.

- a. Use a tool such as SQL Developer to connect to the Oracle database.
- b. Purge the recycle bin. Execute:
 

```
PURGE DBA_RECYCLEBIN
```
- c. Disable the recycle bin. Execute:
 

```
ALTER SYSTEM SET recyclebin = OFF DEFERRED;
ALTER SESSION SET recyclebin = off;
```
- d. Verify that the recycle bin is off. Execute:
 

```
show parameter recyclebin;
```

## Considerations

Review the following considerations:

- For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.
- UIM 20.3.1 is a patch release. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes separate standalone artifacts that you can use to upgrade the respective components. For more information about the artifacts that are available as a part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.
- UIM 9.2.0 (or later) uses OpenJDK instead of Oracle JDK. Upgrading to UIM Server automatically updates the existing Oracle JDK to OpenJDK in the CA UIM environment. Additionally, this upgrade also deletes the older Oracle JDK instances. For more information about the OpenJDK usage in CA UIM, see [Adopting OpenJDK](#).
- UIM 20.3.0 upgrade installer installs the *uimesdplatelemetry web service* on the uimserver wasp when you upgrade from UIM 9.0.2 to UIM 20.3.0. This service is introduced for the PLA customers as it is mandatory for such customers to upload the customer information and usage data to Segment. For more information about how to configure telemetry properties, see [Configure Telemetry for the PLA Model](#).
- UIM also provides you with the secure and non-secure hub and robot options while upgrading UIM Server. Enabling the secure option implies that you want to use the secure version of the hub and robot. If you do not enable the secure option, it implies you want to use the non-secure version of the hub and robot, which is based on the legacy security model. For more information about the secure hub and robot, see [Secure Hub and Robot](#).
- If the `mon_config_service_ws` package is installed on the UIM Server and Operator Console (OC) is installed on another robot, review the following points while performing the upgrade:
 

**Scenario 1:** Before you upgrade the existing UIM Server to 20.3.0 (UIM Server):

  - a. Take a backup of the wasp folder available on the existing UIM Server.
  - b. Delete the wasp probe from the existing UIM Server.
  - c. Start the process to upgrade the existing UIM Server to 20.3.0 (UIM Server).  
After you complete the UIM Server upgrade, you can now upgrade the existing UMP to 20.3.0 (OC). Without performing these steps, if you try to upgrade UMP to 20.3.0 (OC), you will face issues.

**Scenario 2:** If you do not delete the wasp probe before upgrading the UIM Server to 20.3.0:

  - a. Take a backup of the wasp folder available on the upgraded UIM Server.
  - b. Delete the wasp probe from the upgraded UIM Server.
  - c. Upgrade existing UMP to 20.3.0 (OC).
  - d. Deploy wasp that is available with 20.3.0 on the upgraded UIM Server.
  - e. Deploy the `adminconsole`, `mps`, and `telemetry` packages that are available with 20.3.0.  
Without performing these steps, if you try to upgrade the existing UMP to 20.3.0 (OC), you will face issues.
- As part of the installation process, the installer runs an SQL query to verify that your environment is ready for the upgrade. If an issue is found, a message appears:  
Duplicate MCS database entries have been detected. Please contact CA UIM support to continue with your upgrade. Contact CA UIM Support to validate your environment for installation. Attach to the case, in csv format, extracts of the following tables:
  - `ssrv2template`
  - `ssrv2devicegroup`
  - `ssrv2field`
  - `ssrv2profile`
  - `ssrv2ConfigValue`
 If your SQL query results in the message, 'It is safe to upgrade to UIM x.x.x,' continue with the installation of version x.x.x.
- The `discovery_agent` and some other probes might send a single information alarm when upgrading to the latest version of UIM Server. This alarm is benign and can be safely ignored.
- For `data_engine` released with versions prior to UIM 9.0.2, the `S_QOS_DATA` table contains the object data for each unique combination of QoS, source, and target attributes. It does not include the origin value in identifying the unique combination. However, the `data_engine` probe in UIM 9.0.2 has been enhanced to use the unique combination of QoS, source, target, and origin attributes. Therefore, when you upgrade UIM Server from a previous version to UIM 9.0.2, the upgrade process might take some time because `data_engine` uses the origin value to recalculate the unique combination. This recalculation results in updating the existing values in the checksum column of the `S_QOS_DATA`



table. The data\_engine probe runs database scripts during the upgrade process to update the existing records. For example, for Microsoft SQL Server and MySQL, the respective scripts take approximately 20-30 seconds to update 700,000 records in the S\_QOS\_DATA table. In this case, the computer has 16 GB of memory and 8 cores processor.

- The UIM Server installer creates a .pem file (certificate.pem) in the <Nimsoft>\security folder. The .pem file is a symmetric key that is shared with the required robots, which is then used for communication with the data\_engine probe. You copy this .pem file to the remote Operator Console (OC), and CABI robots and provide the location of the file in the robot.cfg file (cryptkey = <.pem file location>). Furthermore, if any impacted probe is not on the same computer where data\_engine is present, copy the generated .pem file to the robot computer (where data\_engine is not available) and update the robot.cfg file with the .pem file location on that computer. For more information about the robot.cfg file configuration, see [Configure robot.cfg](#).
- UIM 9.2.0 removes dependency on the end-of-life (EOL) Microsoft Visual C++ Redistributables for a [few probes and packages](#). Because of this dependency removal, UIM installation deploys the Microsoft Visual C++ 2017 Redistributables package (for example, vs2017\_vccredist\_x86) by default. With this package deployment, only the listed probes can work. For other probes that use the EOL Microsoft Visual C++ Redistributables or for older versions of the impacted probes, you must download and deploy the required EOL Microsoft Visual C++ Redistributable package (for example, vs2008\_redist\_x86) from the Archive. Furthermore, if you want to use the impacted probes with UIM releases prior to UIM 9.2.0, ensure that you download and deploy the required Microsoft Visual C++ 2017 Redistributables package that is available in the Archive.
- In Linux environment, after you upgrade UIM 9.0.2/9.2.0 Server to 20.3.0, the access permission on the nimsoft directory in the CA UIM installation path is changed to 750. This ensures that only the root user can access the directory contents. Other users are not allowed to access the contents. If required, the root user can change the access permissions.

## **Download the UIM Server Install Package**

### **Follow these steps:**

1. Log on to the primary hub server as administrator.
2. Log in to [support.broadcom.com](http://support.broadcom.com), [Download Management](#).

#### **NOTE**

A CA support login is required.

3. Download the following installation packages for your operating system:
  - The UIM Installer (**setupCAUIMServer** executable)
  - The UIM Server Packages (**uimserverpackages** zip file)

#### **WARNING**

Both files are required on the system that hosts the UIM server. If the uimserverpackages zip file is not present, the installation fails.

4. **(Silent Mode Upgrade Only)** Download the **Silent Install Templates for UIM Server** zip package.
5. **(Linux Only)** Run the **chmod 755** command on the setupCAUIMServer executable file.

## **Run the UIM Server Installer**

You can run the installer in three modes. Graphical user interface (GUI) mode walks you through the installation process. Console mode provides an interactive command-line interface. In silent mode, the installer reads configuration information from a response file you create, then runs with no further interaction.

### **GUI Mode Upgrade**

#### **WARNING**

All fields in the installer are case-sensitive.

To complete a GUI mode upgrade, run the installer and follow the prompts to complete the installation. Where possible, the installer displays the current configuration values for your confirmation.

### **Console Mode Upgrade**

#### **Follow these steps:**

1. Run the installer. From a command line, execute:
  - Windows: **setupCAUIMServer.exe -i console**
  - Linux: **setupCAUIMServer\_linux.bin -i console**
2. Follow the prompts to complete the installation. Where possible, the Installer displays the current configuration values for your confirmation.
3. When the upgrade is complete, make sure you:
  - Turn the anti-virus scanners on again if necessary
  - Enable package forwarding
  - Move customized probes back into your probe archive if necessary

### **Silent Mode Upgrade**

#### **Follow these steps:**

1. Prepare your response file:
  - a. Extract the silent install templates.
  - b. Locate the **installer.upgrade.properties** file and save it as **installer.properties** in the same directory as the installer.
  - c. Add your UIM administrator password to the **NMS\_PASSWORD=** line in **installer.properties**.
  - d. Save the file, ensuring the file type is still *PROPERTIES*. If the file type is *Text Document*, remove the **.txt** extension (which may not be displayed in the folder).
2. Run the installer. From a command line, execute:
  - Windows: **setupCAUIMServer.exe -i silent**
  - Linux: **setupCAUIMServer\_linux.bin -i silent**
3. The installer unpacks the files and completes the installation. This process can take several minutes or more.
4. UIM Server launches. If for some reason it does not, execute:
  - Windows: **net start "Nimsoft Robot Watcher"**
  - Linux: **/etc/init.d/nimbus start**

### **Microsoft Cluster Server Upgrade**

Use the following procedure to upgrade UIM Server on a Microsoft Server 2012 failover cluster.

#### **Follow these steps:**

1. Upgrade the primary (active) node using either the GUI mode or silent mode procedure.
2. Make the secondary (passive) node active, then upgrade the node using the same process you used on the primary node.

This ensures that registry keys on both the primary (active) and secondary (passive) nodes are updated for the new version.

### **Post-Upgrade Tasks**

Once the upgrade is complete:

- Turn your anti-virus software back on.
- Enable package forwarding.
- Move your customized probes back into the probe archive if necessary.
- If necessary, [upgrade UMP to OC](#).
- If necessary, upgrade the UIM RESTful web services.

#### NOTE

CA provides newer versions of certain probes between server package releases. During an upgrade, the installer overwrites currently installed probes and components. If you downloaded "hot fix" or updated probes, upgrading UIM Server can result in component downgrades. If this happens, go to the **Archive** page of the [Support](#) website and download the overwritten components again.

[Next Step: \(Optional\) Upgrade the Infrastructure Manager](#)

## Secure Hub and Robot

With newer security issues coming up every single day, organizations cannot ignore the focus on the continuous enhancement of their product's security. Understanding the importance of heightened security, UIM further enhances its security by allowing its customers to seamlessly move to secure hub and robot. Now, two types of hubs and robots are available—*secure* and *non-secure*. In this UIM version, secure hub (hub\_secure) and secure robot (robot\_update\_secure) are available, which further improve the security in UIM. Secure hub and robot provide robust hub-to-hub and robot-to-hub communication. UIM 9.0.2 and prior releases ship with the *non-secure* hub and robot, which use the legacy security model.

A UIM hub serves as the communication center for a group of robots. A hub binds robots into a logical group with the hub as the central connection point. Hubs are typically set up based on a location (such as a lab or a building) or by service (such as development). A hub can connect other hubs into a hierarchy of hubs. UIM lets you decide whether you want to use the secure hub and robot setup. You can use the UIM installer to convert your existing regular UIM setup to a secure setup. You can do this by selecting the secure option while installing UIM Server. Based on your selection, appropriate configurations are performed in your UIM environment.

The following topics cover the required information:

### Introduction

#### General Architecture

The general architecture applies to both non-secure and secure hubs and robots. Architecturally, a hub is a robot that gains management capabilities through the presence of the *hub probe*. Configure the probe to modify how the hub handles the following UIM services:

- **Message distribution**

Messages from robots are routed through the hub. Messages are routed to other hubs, or dispatched to local subscribers (users and probes).

- **Name service**

The hub translates a `/domain/hub/robot/probe` address into an IP address and port. The service registers TCP/IP addresses at startup. Registration allows applications to connect to the service using TCP/IP.

#### NOTE

This is not applicable for secure hub and robot. In a secure setup, this functionality is achieved by using tunnels.

- **Authentication**

The hub handles logins to the domain.

- **Authorization**

The hub verifies user access rights to probes and the infrastructure (hub, robot, and spooler).

- **Tunneling**

Hub-to-hub tunnels enable secure communication from one site to another site, much like a VPN.

### **Secure Hub and Robot Architecture**

In addition to the general architectural components above, the secure hub and robot:

- Establish a strong trust relationship between hubs, and between hubs and robots.
- Proxy the communications to and from all probes, including the hub and controller.
- Use encrypted, trusted transport.
- Ensure that probes listen only on the loopback address. Non-encrypted and non-trusted inter-server probe-to-probe communication is prevented.
- Support third-party certificate authorities and PKI. Self-signed certificates are supported, but are not recommended.
- Replace the legacy Secure Sockets Layer (SSL) mode, proxy mode, and passive mode.
- Support mixed-mode implementations. Mixed mode allows non-secure and secure hubs and robots to coexist.
- Provide secure access to the UIM message bus. For example, callbacks above READ level from remote robots are not allowed.
- Implement enhanced password hashing with the [Password Based Key Derivation Function 2 \(PBKDF2\)](#) hashing algorithm.
- Do not support any communication between hub-to-hub without tunnels.

### **Secure Hub and Robot Version Format**

The secure hub and robot package names follow a format that is different from the non-secure ones. Review that the package names have been suffixed with `_secure` to distinguish them from the non-secure ones:

- `hub_secure 9.31S`
- `robot_update_secure 9.31S`

The non-secure hub and robot packages follow the same format that is applicable for the previous releases:

- `hub 9.31`
- `robot_update 9.31`

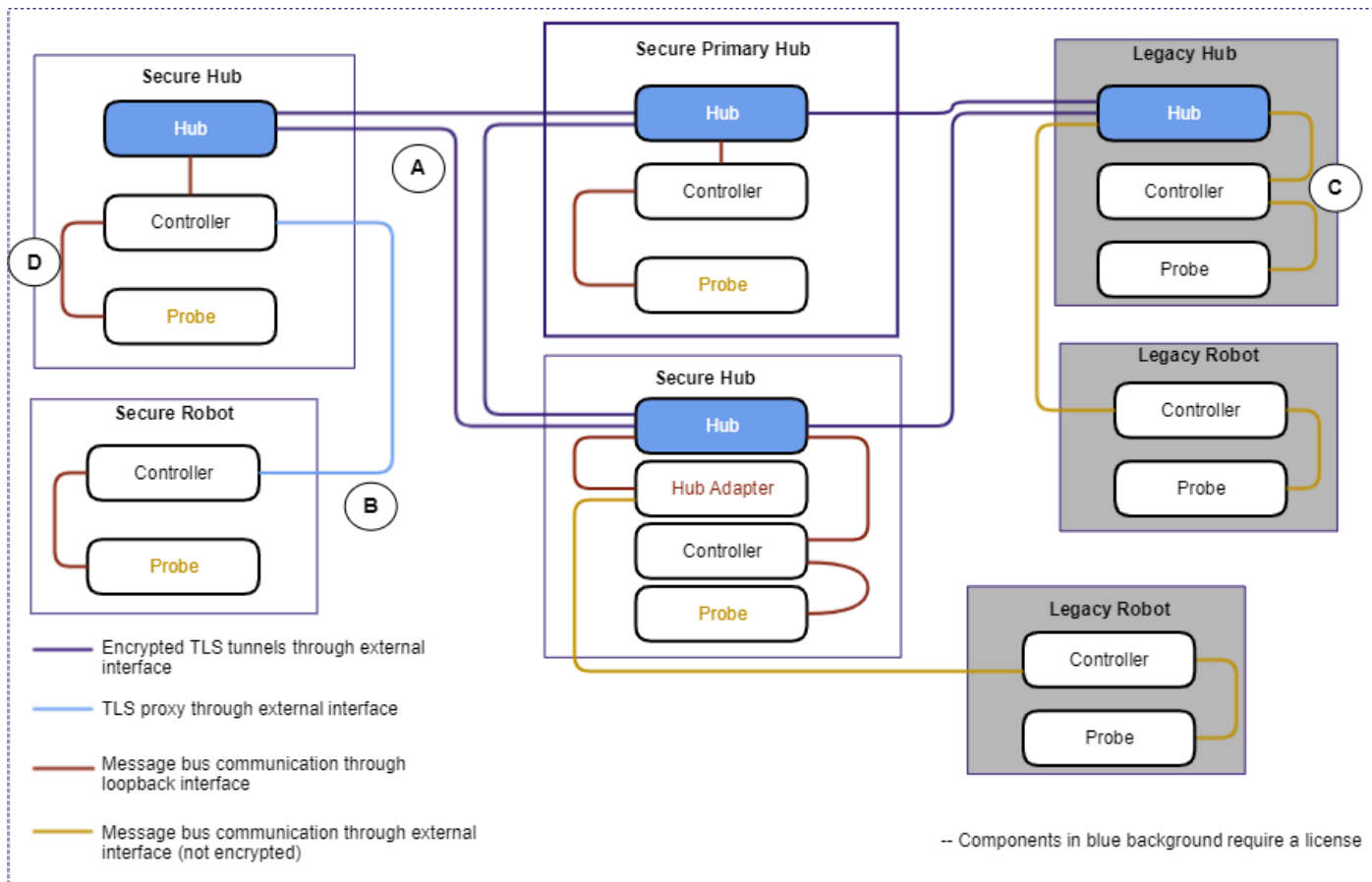
### **Mixed Mode**

In large installations, where many hubs connect to many robots, upgrading all the hubs and robots at once is impractical. To avoid a loss of communication during the conversion, incremental conversions are supported. Secure hubs can communicate with non-secure robots when the `hub_adapter` probe is installed on the secure hubs. A mixed-mode environment consists of both secure and non-secure hubs and robots in a UIM domain.

The following diagram illustrates an example of mixed-mode implementation.

- **A** Secure hubs communicate only through tunnels.
- **B** The controller handles communication between secure hubs and robots. The communication is encrypted.
- **C** Non-secure hubs and robots continue to use non-encrypted transport.
- **D** All internal communication between components that are installed on a secure server occur over the loopback.

**Figure 18: Mixed\_Mode\_Secure\_NonSecure**



**Considerations**

Review the following considerations:

**Existing UIM Environment**

- Before you convert to secure hub and robot, review the [Supported Upgrade Path](#) article to know the correct upgrade path.
- In an existing UIM setup, if your primary hub is not a tunnel server or tunnel client, the installer converts the primary hub into a tunnel server (if the secure option is used). Additionally, all other hubs that point to the primary hub are made tunnel clients to that primary hub. It is not ideal to have a primary hub as a tunnel server, but it might be useful in very small environments or for demonstrating proof of concepts (PoCs). However, in production environments, it is recommended that you always make your primary hub as a tunnel client.

**Hubs and Robots**

- In a secure environment, it is recommended that the latest distsrv probe is installed on all the hubs that you want to change to secure hubs. This helps in recovering from any failure. Once moved to a secure setup, there is a possibility

of losing connection with the primary hub. When you have distsrv, you can directly connect to the IM of the failing hub and restore to the older version.

- To avoid losing connectivity, the tunnel server hub is upgraded first, followed by tunnel client hubs. All hubs require hub-to-hub tunnel connections. Use tunnels for communication between secure hubs, and for communication between non-secure and secure hubs. Static routes between hubs are not supported.
- The hub\_adapter probe is added to a hub before upgrading the hub robot.
- After making your environment secure, if you want to add more robots or hubs to your secure environment, you can do so. For more information about how you can add a new robot or hub, see the [Add a New Robot or Hub to a Secure Environment](#) sections.
- Tunnel security is enhanced with the secure hub. It is possible to maintain a mixed-mode environment, where some hubs are secure and some are non-secure.
- A secure hub can communicate with a non-secure hub provided both the hubs share the same certificates (for example, signed by the same certificate authority (CA)).
- Do not install any hub on a Dynamic Host Configuration Protocol (DHCP) client.
- We recommend that all hubs and robots (pointing to those hubs) use the same certificate authority (CA).
- The cipher security setting on the tunnel server must be set to High. Otherwise, no communication happens if any hub in the domain is made secure.
- In a *regular to secure* conversion scenario, when you deploy the hub\_secure or robot\_update\_secure packages, an error message is shown that states that the deployment has been aborted. However, the deployment completes without any issue. If you receive this error, you can ignore it.

### ssl\_mode Support (Deprecated)

- The parameter ssl\_mode is deprecated. With 9.2.0, by default, SSL communication is enabled between robot and hub through secure bus, if the secure option is selected during the 9.2.0 upgrade. Therefore, secure bus can be considered as an alternative to ssl\_mode. If the non-secure option is selected, ssl\_mode will not have any impact.

### Fully Qualified Domain Names (FQDNs)

- Fully Qualified Domain Names (FQDNs) are required for validation. If short hostnames are used, the validation fails. If Domain Name System (DNS) is not properly configured, you need to explicitly provide FQDNs and create hosts file entries. Ensure that you add FQDNs of OC, CABI, and other independent robots to the etc/hosts file on the hub from which you are performing the deployment. Similarly, you also need to add FQDNs of the respective hubs to the OC, CABI, and other independent robots. FQDN name resolutions need to be set in the hosts file on the first line.

### Package Renaming

- We recommend that you do not rename the package name in the archive. If you rename the package name in the archive and try to deploy the package to the hub after logging into the same hub, an unexpected error can appear. However, deployment is completed correctly. For example, if you rename the robot\_update package in the archive and try to deploy it to the hub after logging into that hub, you get the following error: `Aborted, retry limit exceeded, unknown status`, but the deployment completes successfully.

### Backup

- Back up security.cfg and security.dta before the conversion process.

### Certificate Package

- (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the required robots (hub robots, UMP/OC robot, CABI robot, and other independent robots) pointing to that hub.
- (Prior to 20.3.3) The create\_robot\_cert\_package callback has a dependency on the latest version of the distsrv probe or automated\_deployment\_engine (ade) probe released with 20.3.0. This callback is used to generate the UIMRobotCert package. Ensure that the latest version of distsrv or ade is already deployed to the secure tunnel server hub where you run the callback to create the package. If the latest version of both the probes is available, the callback uses distsrv by default. If distsrv is not available, it uses the ade probe.

## Infrastructure Manager

The following considerations are related to Infrastructure Manager (IM). Infrastructure Manager is a configuration interface for UIM. IM is supported only on Windows platforms. Typically, you log in to the primary hub on IM.

- In a secure UIM environment, you can use IM only on a Windows system that is converted to a secure hub. IM can connect to the loopback address (127.0.0.1) of the local system and can navigate to other hubs. This implies that remote IM connections are no longer available.
- To use IM in a mixed-mode UIM domain:
  - If the primary hub is secured, and is *non-Windows*, log in to any non-secure hub in the domain.
  - If the primary hub is secured, and is *Windows*, install IM on the Windows primary hub. Connect to the domain using the Windows loopback IP address of 127.0.0.1.
  - If a secondary Windows hub is secured, install IM on the Windows secondary hub. Connect to the domain using the Windows loopback IP address of 127.0.0.1.
- To use IM in a secured UIM domain:
  - If the primary hub is on a Windows platform, install IM on the Windows primary hub. Connect to the domain using the Windows loopback IP address of 127.0.0.1.
  - If the primary hub is non-Windows, install IM on a Windows secondary hub. Connect to the domain using the Windows loopback IP address of 127.0.0.1.
- In a secure environment, the **Alarm Window** section (**View, Alarm Window**) does not open in IM. Furthermore, after clicking **View, Alarm Window**, if you refresh your IM (**View, Refresh**), you will lose the connectivity to all the hubs. You must log in again to view all the hubs in IM.

### NOTE

If you want to view the **Alarm Window** section in a secure environment, you can install IM on a secure (or non-secure) secondary hub and point the alarm window to the primary hub nas. To do so, select **Tools, Options** from the menu bar and then select the primary hub nas option (for example, `/<domain_name>/<primary_hub_name>/<primary_hub_robot_name>/nas`) from the **Alarm Server** drop-down list.

## UMP/OC and CABI

- For converting your UMP/OC and CABI to a secure state, ensure that you bring your UMP/OC and CABI robots to the secure state by deploying the appropriate certificates and then updating the version to the secure versions. After that, you upgrade UMP/OC and CABI.

## Convert Existing UIM Setup to Secure Hub and Robot

### NOTE

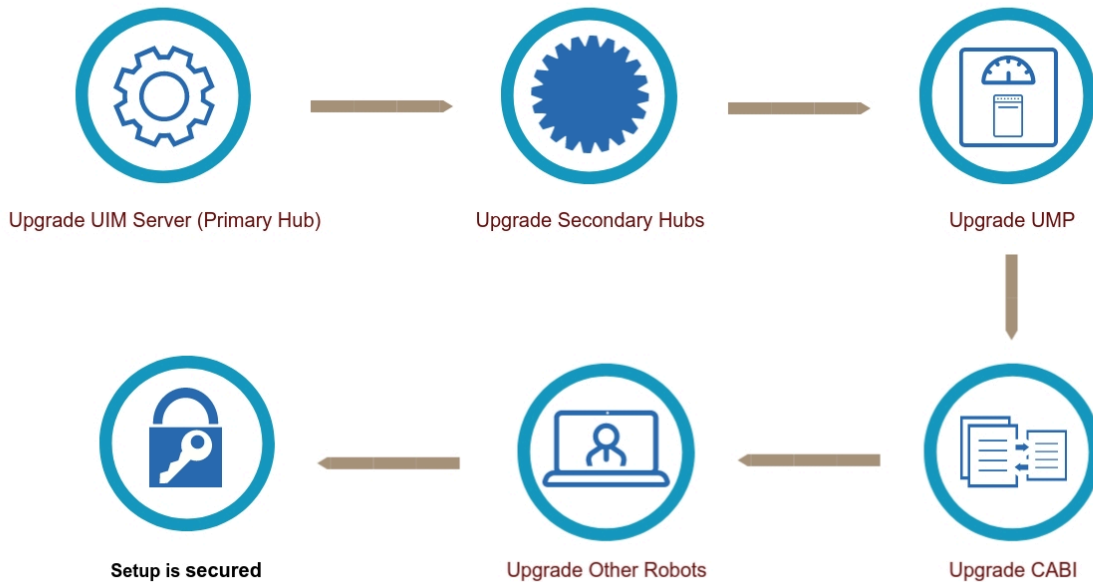
If your primary hub is not a tunnel server or tunnel client, the installer converts your primary hub into a tunnel server (when the secure option is used). It also converts other hubs that are pointing to that primary hub into tunnel clients. It is not ideal to have a primary hub as a tunnel server, but it might be useful in very small environments or for demonstrating proof of concepts (PoCs). However, in production environments, it is recommended that you always make your primary hub as a tunnel client.

UIM supports the following scenarios for the secure bus:

- Existing Environment Configured without Tunnels
- Existing Environment Configured with Tunnels (Primary Hub as Tunnel Server)
- Existing Environment Configured with Tunnels (Primary Hub as Tunnel Client)

The process to convert your existing UIM environment to a secure setup involves the following tasks:

## Secure Upgrade Process



### NOTE

After securing your setup, if you want to add more robots or hubs to the secure environment at a later stage, you can do so. For more information about how you can add a new robot or hub, see the [Add a New Robot or Hub to a Secure Environment](#) sections.

### Convert Existing Environment Configured without Tunnels

In this scenario, your existing environment is not configured with tunnels. The steps are as follows:

1. Upgrade UIM Server (Primary Hub)
2. Upgrade Secondary Hubs
3. Upgrade UMP/OC
4. Upgrade CABI
5. Upgrade Other Robots

#### Upgrade UIM Server (Primary Hub)

The installer (UIM Server) provides an option that lets you automatically deploy secure hub and robot binaries to the primary hub in your existing setup. When you run the installer, you get a secure option to convert your existing hub and robot to secure hub and robot. When the conversion completes, depending on your existing setup, the upgrade performs the appropriate tasks outlined in this section.

#### Follow these steps:

1. Run the setupCAUIMServer.exe file on the computer where your existing UIM Server is installed. The **Upgrade Detected** screen appears.
2. Review the installed version and upgrade version information, and click **Next**. The **License Agreement** screen appears.
3. Review the license information, accept the agreement, and click **Next**.



The **Secure Bus Configuration** screen appears. You use this screen to provide information that performs secure hub- and robot-related configurations in your environment.

4. Perform the following actions on this screen to convert to secure hub and robot:

– **Enable**

Specifies whether you want to convert to secure hub and robot.

• When this option is selected:

- The **Tunnel Server Configuration** section is displayed if the existing environment does not have a tunnel setup.

As no tunnels are configured in this scenario, this section is displayed in the UI.

- The **Tunnel Server Configuration** section is not displayed if the existing setup is already configured with tunnels.

For more information about the scenario where tunnel setup is available, see [Existing Environment Configured with Tunnels \(Primary Hub as Tunnel Server\)](#) and [Existing Environment Configured with Tunnels \(Primary Hub as Tunnel Client\)](#).

• If you do not select the **Enable** option, the normal (non-secure) deployment process is followed.

– **Tunnel Server Configuration**

Lets you specify configuration settings for the tunnel server. This information configures the primary hub as a tunnel server, makes tunnel server as a certificate authority (CA), creates \* tunnel certificates.

- **Tunnel Server Port**

Enter the tunnel server port number, and click **Test** to verify the port availability. The default port is 48003.

- **CA/Server Password**  
Enter the password that you want to use for generating the certificate authority (CA) and tunnel server certificate (CN: IP address).
- **Confirm CA/Server Password**  
Confirm the password that you entered in the **CA/Server Password** field.
- **Client Password**  
Enter the password that you want to use for the tunnel client certificate. This password is used to generate the \* (wildcard) tunnel client certificates.
- **Confirm Client Password**  
Confirm the password that you entered in the **Client Password** field.

5. Click **Next**.

The **Upgrade Preparation** screen appears.

6. Enter the password associated with the UIM administrator, and click **Run Upgrade Preparation**. During this phase, the following tasks are performed based on the existing setup. More information about these scenarios is explained after the procedure steps:

- a. If the primary hub is configured as a tunnel server in the existing setup, a duplicate of the certificate is copied to the `<Nimsoft>\robot\certs` folder and `robot.cfg` is appropriately configured with the certificate location.
- b. If the primary hub is configured as a tunnel client in the existing setup, a duplicate of the certificate is copied to the `<Nimsoft>\robot\certs` folder and `robot.cfg` is appropriately configured with the certificate location.
- c. If no tunnels exist in the existing setup, the primary hub is configured as a tunnel server and all secondary hubs pointing to that primary hub are configured as tunnel clients.

When the upgrade preparation is done, the **Pre-Install Summary** screen appears.

7. Review the information; for example, verify **Secure Bus Configuration** section.

8. Click **Install** to start the upgrade process.

When the upgrade process is completed, the **Install Complete** screen appears.

9. Click **Done**.

In this scenario, when you enable the secure option, the behavior is as follows:

- The installer configures the primary hub as a tunnel server.
- The installer configures all secondary hubs that are pointing to the primary hub as tunnel clients.
- The installer makes tunnel server (primary hub) as the certificate authority (CA), creates a tunnel server certificate, and \* tunnel client certificate (signed by the created CA) in the `<Nimsoft>\hub\certs` folder. An example snippet is as follows:

```
ca.pem
cert01.pem
server.ca.ec.cert.pem
server.ec.cert.pem
server.ec.key.pem
....
```

- The installer updates the tunnel server (primary hub) `hub.cfg` with the created tunnel server certificates location. An example snippet is as follows:

```
<server>
...
ca_location = certs/server.ca.ec.cert.pem
public_cert = certs/server.ec.cert.pem
private_key = certs/server.ec.key.pem
password = +2U4jzflzhj011oXVWQ==
```

```
</server>
```

- The installer updates the tunnel server (primary hub) robot.cfg with the created tunnel certificates location. An example snippet is as follows:

```
<controller>
...
proxy_ca_location = C:\Program Files (x86)\Nimsoft\.\hub\certs\server.ca.ec.cert.pem
proxy_cert = C:\Program Files (x86)\Nimsoft\.\hub\certs\server.ec.cert.pem
proxy_private_key = C:\Program Files (x86)\Nimsoft\.\hub\certs\server.ec.key.pem
proxy_private_key_password = +2U4jzflzhj01loXVWQ==
proxy_check_ip_first = 1
</controller>
```

- The installer creates a \* tunnel client certificate in the tunnel clients (secondary hubs) <Nimsoft>\hub\certs folder. An example is as follows:

```
client1.pem
...
```

- The installer updates the tunnel clients (secondary hubs) hub.cfg with the created certificate location. An example is as follows:

```
...
cert = certs/client1.pem
password = +2U4jzflzhj01loXVWQ==
```

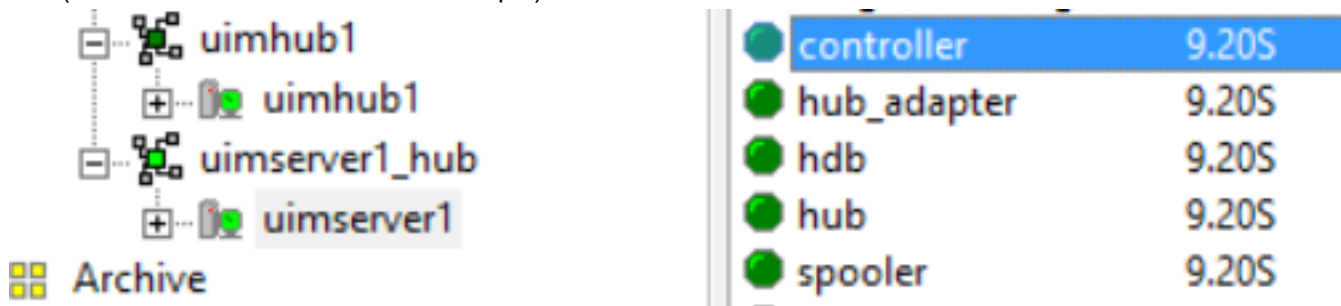
- The installer creates the <Nimsoft>\robot\certs folder on the tunnel clients (secondary hubs) and creates the \* tunnel client certificate in this location. An example snippet is as follows:

```
robotclient1.pem
...
```

- The installer updates the tunnel clients (secondary hubs) robot.cfg with the created certificate location. An example snippet is as follows:

```
<controller>
...
proxy_ca_location = robot/certs/robotclient1.pem
proxy_cert = robot/certs/robotclient1.pem
proxy_private_key = robot/certs/robotclient1.pem
proxy_private_key_password = +2U4jzflzhj01loXVWQ==
proxy_check_ip_first = 1
</controller>
```

- The installer deploys the hub\_adapter, secure hub, and secure robot to the tunnel server (primary hub). The following example screenshot shows that the required secure packages are successfully deployed to the primary hub (which is a tunnel server in this example):



Your primary hub is now secure.

### Upgrade Secondary Hubs

After the installer performs required tasks, you can now configure secondary hubs and make them secure.

#### Follow these steps:

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. From the primary hub archive, deploy the hub\_adapter probe to the secondary hubs (tunnel clients).  
The following example screenshot shows that the hub\_adapter probe is successfully deployed to the secondary hub:

The screenshot displays the 'Domains' tree on the left and a 'Probe' table on the right. In the 'Domains' tree, the 'uimhub1' node under 'uimserver1\_domain' is expanded, showing a sub-node 'uimhub1' with a green status icon. The 'Probe' table lists several probes with their versions.

| Probe       | Vers... |
|-------------|---------|
| hub_adapter | 9.20S   |
| controller  | 7.96    |
| hdb         | 7.96    |
| hub         | 7.96    |
| spooler     | 7.96    |
| distsrv     | 7.96    |

3. From the primary hub archive, deploy the latest non-secure robot (7.97 or later) to the secondary hubs (tunnel clients).  
The following example screenshot shows that the non-secure robot is successfully deployed to the secondary hub:

The screenshot displays the 'Domains' tree on the left and a 'Probe' table on the right. In the 'Domains' tree, the 'uimhub1' node under 'uimserver1\_domain' is expanded, showing a sub-node 'uimhub1' with a red status icon. The 'Probe' table lists several probes with their versions.

| Probe       | Vers... |
|-------------|---------|
| hub_adapter | 9.20S   |
| controller  | 9.20    |
| hdb         | 9.20    |
| spooler     | 9.20    |
| hub         | 7.96    |
| distsrv     | 7.96    |

4. From the primary hub archive, deploy the latest secure hub to the secondary hubs (tunnel clients).  
The following example screenshot shows the secure hub is successfully deployed to the secondary hub:

The screenshot displays the 'Domains' tree on the left and a 'Probe' table on the right. In the 'Domains' tree, the 'uimhub1' node under 'uimserver1\_domain' is expanded, showing a sub-node 'uimhub1' with a red status icon. The 'Probe' table lists several probes with their versions.

| Probe       | Vers... |
|-------------|---------|
| hub_adapter | 9.20S   |
| controller  | 9.20    |
| hdb         | 9.20    |
| spooler     | 9.20    |
| hub         | 9.20S   |
| distsrv     | 7.96    |

5. From the primary hub archive, deploy the latest secure robot to the secondary hubs (tunnel clients). The following example screenshot shows the secure robot is successfully deployed to the secondary hub:

| Probe       | Vers... |
|-------------|---------|
| controller  | 9.20S   |
| hub_adapter | 9.20S   |
| hdb         | 9.20S   |
| hub         | 9.20S   |
| spooler     | 9.20S   |
| distsrv     | 7.96    |

6. From the primary hub archive, deploy the latest distsrv (9.20 or later) probe to the secondary hubs. The following example screenshot shows that the distsrv 9.20 is successfully deployed to the secondary hub:

| Probe       | Vers... |
|-------------|---------|
| controller  | 9.20S   |
| hub_adapter | 9.20S   |
| hdb         | 9.20S   |
| hub         | 9.20S   |
| spooler     | 9.20S   |
| distsrv     | 9.20    |

Your secondary hubs are now secure.

### **Upgrade UMP/OC**

After upgrading your secondary hubs, you can convert your UMP/OC to a secure state.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the robots pointing to the hub.
3. (Prior to 20.3.3) Use the certificate generation callback on the secure tunnel server hub to create a certificate package (UIMRobotCert) in the local archive of the secure tunnel server. This certificate package contains the \* tunnel certificate .pem file and robot.cfx. When you deploy this package, it deploys the certificate .pem file and updates the robot.cfg file with the .pem file location. For more information about how to generate the certificate, see the certificate generation section in this article. From the primary hub archive, deploy the certificate package (UIMRobotCert) to the UMP/OC robot.
4. From the primary hub archive, upgrade the UMP/OC robot version to the secure version.

5. Run the OC installer to upgrade UMP to OC.

Your OC deployment is now secure and is upgraded.

### **Upgrade CABI**

You can now upgrade your CABI to the secure state.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the robots pointing to the hub.
3. (Prior to 20.3.3) In the primary hub archive, locate the UIMRobotCert package that you have already created and deploy it to the CABI robot.
4. Upgrade the CABI robot version to the secure version.
5. Deploy the latest CABI package to the CABI robot.

Your CABI deployment is now upgraded and is secure.

### **Upgrade Other Robots**

If there are other independent robots in your domain that you want to make secure, you can do so.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the robots pointing to the hub.
3. (Prior to 20.3.3) In the primary hub archive, locate the UIMRobotCert package that you have already created and deploy it to the independent robots.
4. From the primary hub archive, upgrade the independent robot version to the secure version.

Your independent robots are now secure.

### **Convert Existing Environment Configured with Primary Hub as Tunnel Server**

Your existing environment is configured with tunnels. In this setup, your primary hub is configured as a tunnel server and all other secondary hubs are configured as tunnel clients. The steps are as follows:

1. Upgrade UIM Server (Primary Hub)
2. Upgrade Secondary Hubs
3. Upgrade UMP/OC
4. Upgrade CABI
5. Upgrade Other Robots

#### **NOTE**

Verify that the cipher security setting on the tunnel server is set to High. Otherwise, no communication happens if any hub in the domain is made secure.

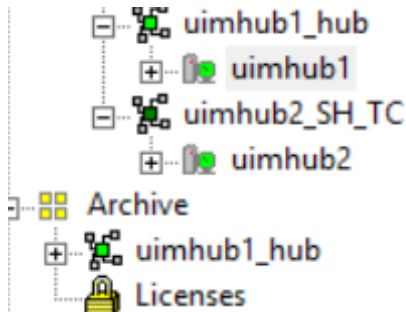
### **Upgrade UIM Server (Primary Hub)**

To run the UIM Server installer, follow the steps as explained in the previous section. As tunnels are already configured in the existing setup, the **Tunnel Server Configuration** section is not displayed.

In this scenario, when you enable the secure option, the behavior is as follows:

1. The installer does not change the existing tunnel setup.

2. The installer deploys the hub\_adapter, secure hub, and secure robot to the primary hub (tunnel server). The following example screenshot shows that the required secure packages are deployed to the primary hub (which is a tunnel server in this screenshot and scenario):



|                       |       |
|-----------------------|-------|
| ● controller          | 9.20S |
| ● hdb                 | 9.20S |
| ● hub                 | 9.20S |
| ● hub_adapter         | 9.20S |
| ● spooler             | 9.20S |
| ● alarm_enrichment    | 9.20  |
| ● automated_deploy... | 9.20  |

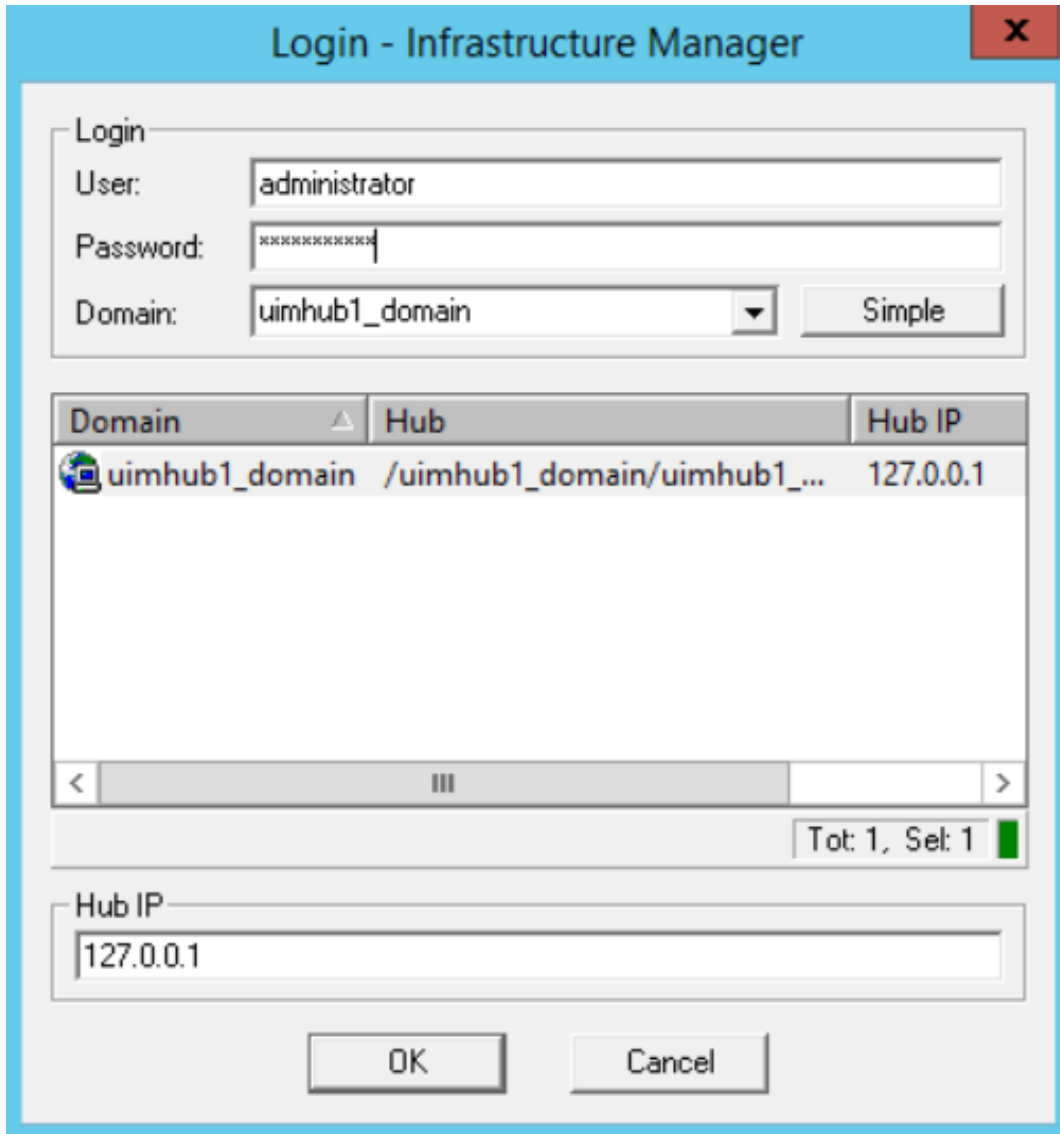
Your primary hub is now secure.

### **Upgrade Secondary Hubs**

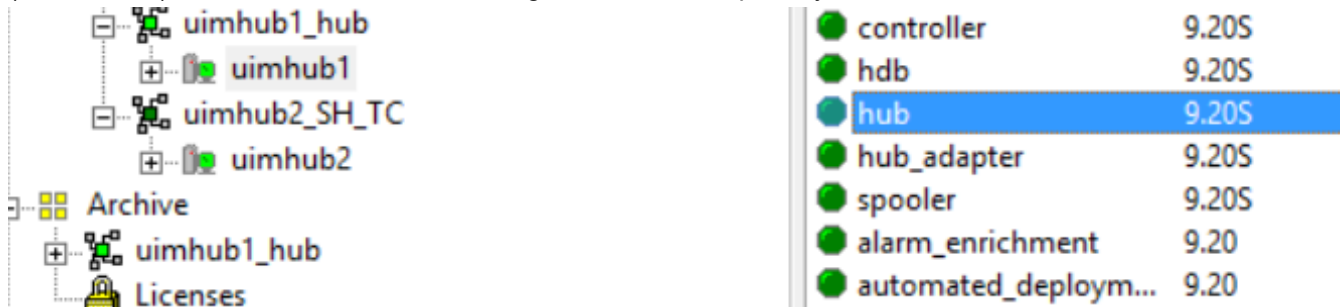
After the installer performs required tasks, you can now configure secondary hubs and make them secure.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).  
The following example screenshot shows the login to the IM on the secure primary hub using the loopback IP address:



You can see all your secondary hubs listed because tunnels are already configured. The following example screenshot shows that a secure primary hub (tunnel server) and non-secure secondary hub (tunnel client) are listed in the IM after the login on the secure primary hub:



- From the primary hub archive, deploy the latest hub\_adapter probe to the secondary hubs (tunnel clients). The following example screenshot shows that the hub\_adapter probe is successfully deployed to the secondary hub:



The screenshot shows a domain tree on the left with 'uimhub1\_domain' expanded to show 'uimhub1\_hub', 'uimhub1', 'uimhub2\_SH\_TC', and 'uimhub2'. Below it is an 'Archive' section with 'uimhub1\_hub'. On the right, a table lists probes and their versions:

| Probe       | Version |
|-------------|---------|
| hub_adapter | 9.20S   |
| controller  | 7.96    |
| distsrv     | 7.96    |
| hdb         | 7.96    |
| hub         | 7.96    |
| spooler     | 7.96    |

- From the primary hub archive, deploy the latest non-secure robot to the secondary hubs (tunnel clients). The following example screenshot shows that the non-secure robot is successfully deployed to the secondary hub:

The screenshot shows a domain tree on the left with 'uimhub1\_domain' expanded to show 'uimhub1\_hub', 'uimhub1', 'uimhub2\_SH\_TC', and 'uimhub2'. Below it is an 'Archive' section with 'uimhub1\_hub'. On the right, a table lists probes and their versions:

| Probe       | Version |
|-------------|---------|
| hub_adapter | 9.20S   |
| controller  | 9.20    |
| hdb         | 9.20    |
| spooler     | 9.20    |
| hub         | 7.96    |
| distsrv     |         |

- From the primary hub archive, deploy the latest secure hub package to the secondary hubs (tunnel clients). The following example screenshot shows that the secure hub is successfully deployed to the secondary hub:

The screenshot shows a domain tree on the left with 'uimhub1\_domain' expanded to show 'uimhub1\_hub', 'uimhub1', 'uimhub2\_SH\_TC', and 'uimhub2'. Below it is an 'Archive' section with 'uimhub1\_hub'. On the right, a table lists probes and their versions:

| Probe       | Version |
|-------------|---------|
| hub_adapter | 9.20S   |
| hub         | 9.20S   |
| controller  | 9.20    |
| hdb         | 9.20    |
| spooler     | 9.20    |
| distsrv     | 7.96    |

- From the primary hub archive, deploy the latest distsrv (9.20 or later) to the secondary hubs. The following example screenshot shows that distsrv 9.20 or later is successfully deployed to the secondary hub:

The screenshot shows a domain tree on the left with 'uimhub1\_domain' expanded to show 'uimhub1\_hub', 'uimhub1', 'uimhub2\_SH\_TC', and 'uimhub2'. Below it is an 'Archive' section with 'uimhub1\_hub'. On the right, a table lists probes and their versions:

| Probe       | Version |
|-------------|---------|
| hub_adapter | 9.20S   |
| hub         | 9.20S   |
| controller  | 9.20    |
| distsrv     | 9.20    |
| hdb         | 9.20    |
| spooler     | 9.20    |

- (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the robots pointing to the hub.

7. (Prior to 20.3.3) Use the robot certificate callback on the secure tunnel server hub to create a certificate package (UIMRobotCert). This certificate package contains the \* tunnel certificate .pem file and robot.cfx. When you deploy this package, it deploys the certificate .pem file and updates the robot.cfg file with the same .pem file location. From the primary hub archive, deploy the certificate package (UIMRobotCert) to the secondary hub robots, UMP/OC robot, CABI robot, and other independent robots
8. From the primary hub archive, deploy the latest secure robot package to secondary hub robots. The following example screenshot shows that the secure robot package is successfully deployed to the secondary hub:

The screenshot shows a domain tree on the left and a table of probe versions on the right. The domain tree includes 'Domains' with sub-items 'uimhub1\_domain', 'uimhub1\_hub', 'uimhub1', 'uimhub2\_SH\_TC', and 'uimhub2'. Below 'Domains' is an 'Archive' section with 'uimhub1\_hub'. The table on the right has two columns: 'Probe' and 'Version'. The 'controller' probe is highlighted in blue and has a version of 9.20S. Other probes include 'hub\_adapter', 'hdb', 'hub', 'spooler', and 'distsrv', all with versions 9.20S or 9.20.

| Probe       | Version |
|-------------|---------|
| controller  | 9.20S   |
| hub_adapter | 9.20S   |
| hdb         | 9.20S   |
| hub         | 9.20S   |
| spooler     | 9.20S   |
| distsrv     | 9.20    |

Your secondary hubs are now secure.

### **Upgrade UMP/OC**

After upgrading your secondary hubs, you can secure your UMP/OC deployment.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. From the primary hub archive, upgrade the UMP/OC robot version to the secure version.
3. Run the OC installer to upgrade UMP to OC.

Your OC deployment is now secure and is upgraded.

### **Upgrade CABI**

You can now upgrade your CABI to the secure state.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. From the primary hub archive, upgrade the CABI robot version to the secure version.
3. Deploy the CABI 4.30 package to the CABI robot.

Your CABI deployment is now upgraded and is secure.

### **Upgrade Other Robots**

If there are other independent robots in your domain that you want to make secure, you can do so.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. From the primary hub archive, upgrade the robot version to the secure version.

Your independent robots are now secure.

## **Convert Existing Environment Configured with Primary Hub as Tunnel Client**

Your existing environment is configured with tunnels. In this setup, your primary hub is configured as a tunnel client, one of the secondary hubs is configured as a tunnel server, and remaining secondary hubs are configured as other tunnel clients. The steps are as follows:

1. Upgrade UIM Server (Primary Hub)
2. Upgrade Secondary Hubs
3. Upgrade UMP/OC
4. Upgrade CABI
5. Upgrade Other Robots

### **NOTE**

Verify that the cipher security setting on the tunnel server is set to High. Otherwise, no communication happens if any hub in the domain is made secure.

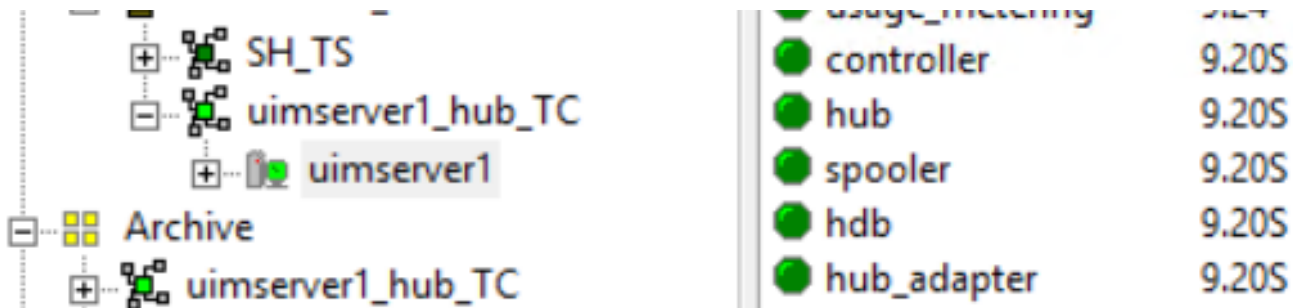
## **Upgrade UIM Server (Primary Hub)**

To run the UIM Server installer, follow the steps as explained in the previous section. As tunnels are already configured in the existing setup, the **Tunnel Server Configuration** section is not displayed.

In this scenario, when you enable the secure option, the behavior is as follows:

1. The installer does not change the existing tunnel setup. It duplicates the certificate used in the tunnel client configuration in the primary hub and places it in the `..\Nimsoft\robot\certs` folder. The robot is configured to use that certificate.
2. The installer deploys the `hub_adapter`, `secure hub`, and `secure robot` to the primary hub (tunnel client).

Your primary hub is now secure. The following example screenshot shows that the secure packages are deployed to the primary hub (which is a tunnel client in this screenshot):

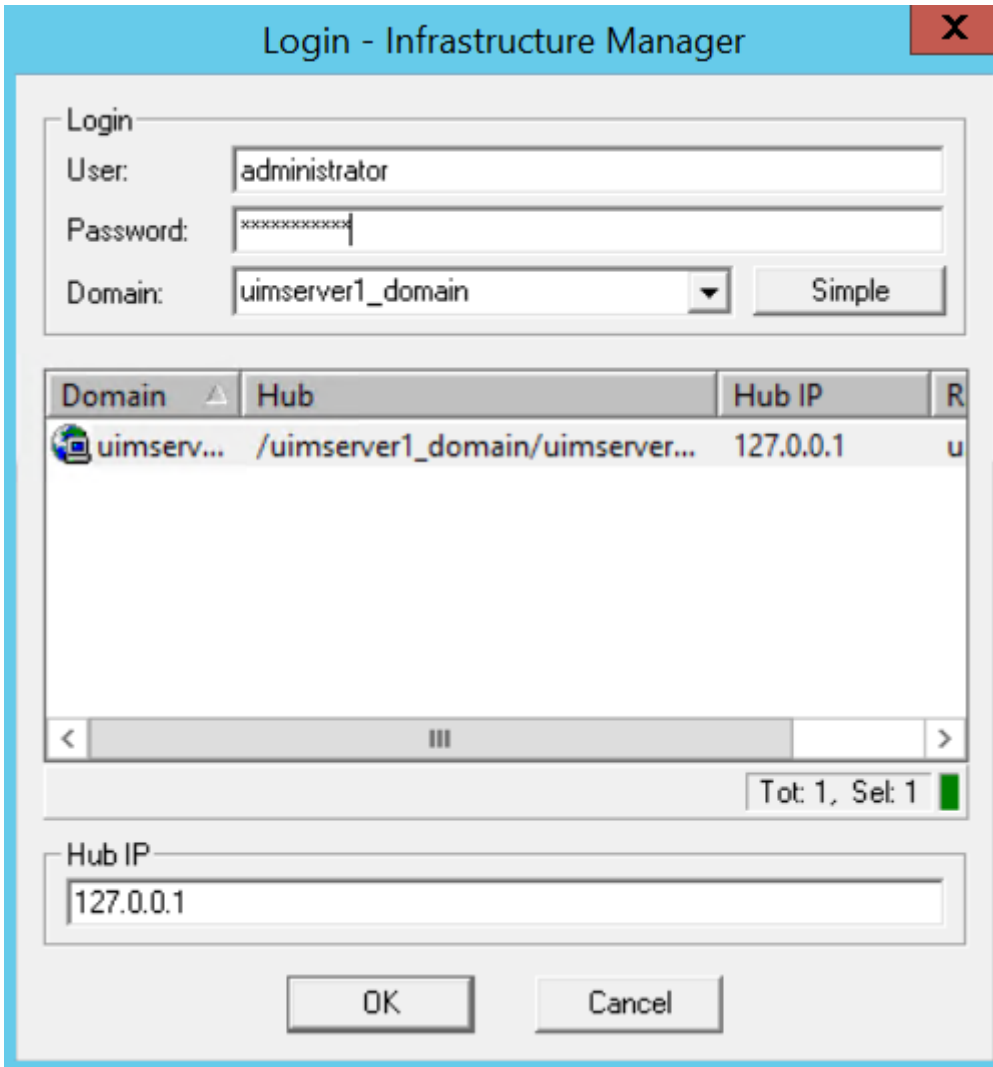


## **Upgrade Secondary Hubs**

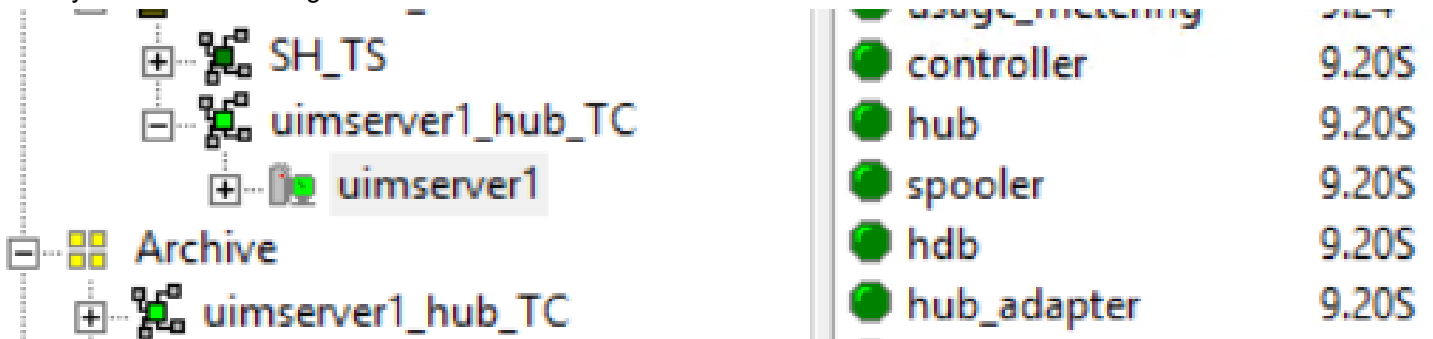
After the installer performs required tasks, you can now configure secondary hubs and make them secure. One of the secondary hubs is a tunnel server in this scenario.

### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP). The following example screenshot shows the primary hub IM login using the loopback IP:



You should be able to see all your secondary hubs listed because tunnels are already configured. The following example screenshot shows the non-secure secondary hub (which is a tunnel server in this screenshot) and the secure primary hub after the IM login:



- From the primary hub archive, deploy the latest hub\_adapter probe to the secondary hubs. The following example screenshot shows that the hub\_adapter probe is successfully deployed to the secondary hub:

| Probe       | Vers... |
|-------------|---------|
| hub_adapter | 9.20S   |
| hub         | 7.96    |
| hdb         | 7.96    |
| controller  | 7.96    |
| distsrv     | 7.96    |
| spooler     | 7.96    |

- From the primary hub archive, deploy the latest non-secure robot to the secondary hubs.  
The following example screenshot shows that the non-secure robot is successfully deployed to the secondary hub:

| Probe       | Vers... |
|-------------|---------|
| hub_adapter | 9.20S   |
| hdb         | 9.20    |
| controller  | 9.20    |
| spooler     | 9.20    |
| hub         | 7.96    |
| distsrv     | 7.96    |

- Deploy the secure hub to the secondary hubs.  
The following example screenshot shows that the secure hub is successfully deployed to the secondary hub:

| Probe       | Vers... |
|-------------|---------|
| hub         | 9.20S   |
| hub_adapter | 9.20S   |
| hdb         | 9.20    |
| controller  | 9.20    |
| spooler     | 9.20    |
| distsrv     | 7.96    |

- Deploy the latest distsrv to the secondary hubs.  
The following example screenshot shows that distsrv 9.20 or later is successfully deployed to the secondary hub:

| Probe       | Vers... |
|-------------|---------|
| hub         | 9.20S   |
| hub_adapter | 9.20S   |
| hdb         | 9.20    |
| controller  | 9.20    |
| distsrv     | 9.20    |
| spooler     | 9.20    |

6. (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the robots pointing to the hub.
  7. (Prior to 20.3.3) Connect to IM from any Windows computer by using the normal IP of the tunnel server. Use the robot certificate callback on the secure tunnel server hub to create a certificate package (UIMRobotCert). This certificate package contains the \* tunnel certificate .pem file and robot.cfx. When you deploy this package, it deploys the certificate .pem file and updates the robot.cfg file with the same .pem file location. From the tunnel server archive, deploy this certificate package to the secondary hub robots, UMP/OC robot, CABI robot, and independent robots.
  8. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
  9. From the primary hub archive, deploy the latest secure robot package to secondary hubs.
- The following example screenshot shows that the secure robot is successfully deployed to the secondary hub:

| Probe       | Vers... |
|-------------|---------|
| hub         | 9.20S   |
| hub_adapter | 9.20S   |
| hdb         | 9.20S   |
| controller  | 9.20S   |
| spooler     | 9.20S   |
| distsrv     | 9.20    |

Your secondary hubs are now secure.

### **Upgrade UMP/OC**

After upgrading your secondary hubs, you can convert your UMP/OC to a secure state.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. From the primary hub archive, upgrade the UMP/OC robot version to the secure robot version.
3. Run the OC installer to upgrade UMP to OC.

---

Your UMP/OC is now upgraded and is secure.

### **Upgrade CABI**

You can now upgrade your CABI to the secure state.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. From the primary hub archive, upgrade the CABI robot version to the secure version.
3. Deploy the CABI 4.30 package to the CABI robot.

Your CABI is now upgraded and is secure.

### **Upgrade Other Robots**

You can now upgrade other independent robots to the secure state.

#### **Follow these steps:**

1. Log in to the primary hub Admin Console or IM (only on Windows using the loopback IP).
2. From the primary hub archive, upgrade the independent robot version to the secure version.

Your independent robots are now secure.

### **Existing Environment Configured with Partial Tunnel Setup**

#### **NOTE**

It is not ideal to have a primary hub as a tunnel server, but it might be useful in very small environments or for demonstrating proof of concepts (PoCs). However, in production environments, it is recommended that you always make your primary hub as a tunnel client.

A partial tunnel setup implies all the hubs in your existing setup are not communicating through tunnels. Consider a scenario where tunnels are configured only on the secondary hubs and not on a primary hub. In this case, when you run the installer by using the secure option, your primary hub will be made a tunnel server and all other secondary hubs that point to the primary hub will become tunnel clients to the tunnel server (primary hub).

Therefore, to work in this type of scenario, you must manually configure tunnels in your environment so that one of the secondary hubs in the domain is configured as a tunnel server and all other hubs as tunnel clients to that hub (tunnel server). After that, you use the installer as you do in the case where tunnels are already configured in the setup and primary hub is a tunnel client.

### **(Applicable for Prior to 20.3.3) Generate Certificate Package**

Use the `create_robot_cert_package` hub callback on the *secure tunnel server* to generate a \* (wildcard) certificate package. The callback creates the certificate package (UIMRobotCert) and places it in the secure tunnel server archive. This package includes a \* certificate .pem file (client#.pem) and robot.cfx file.

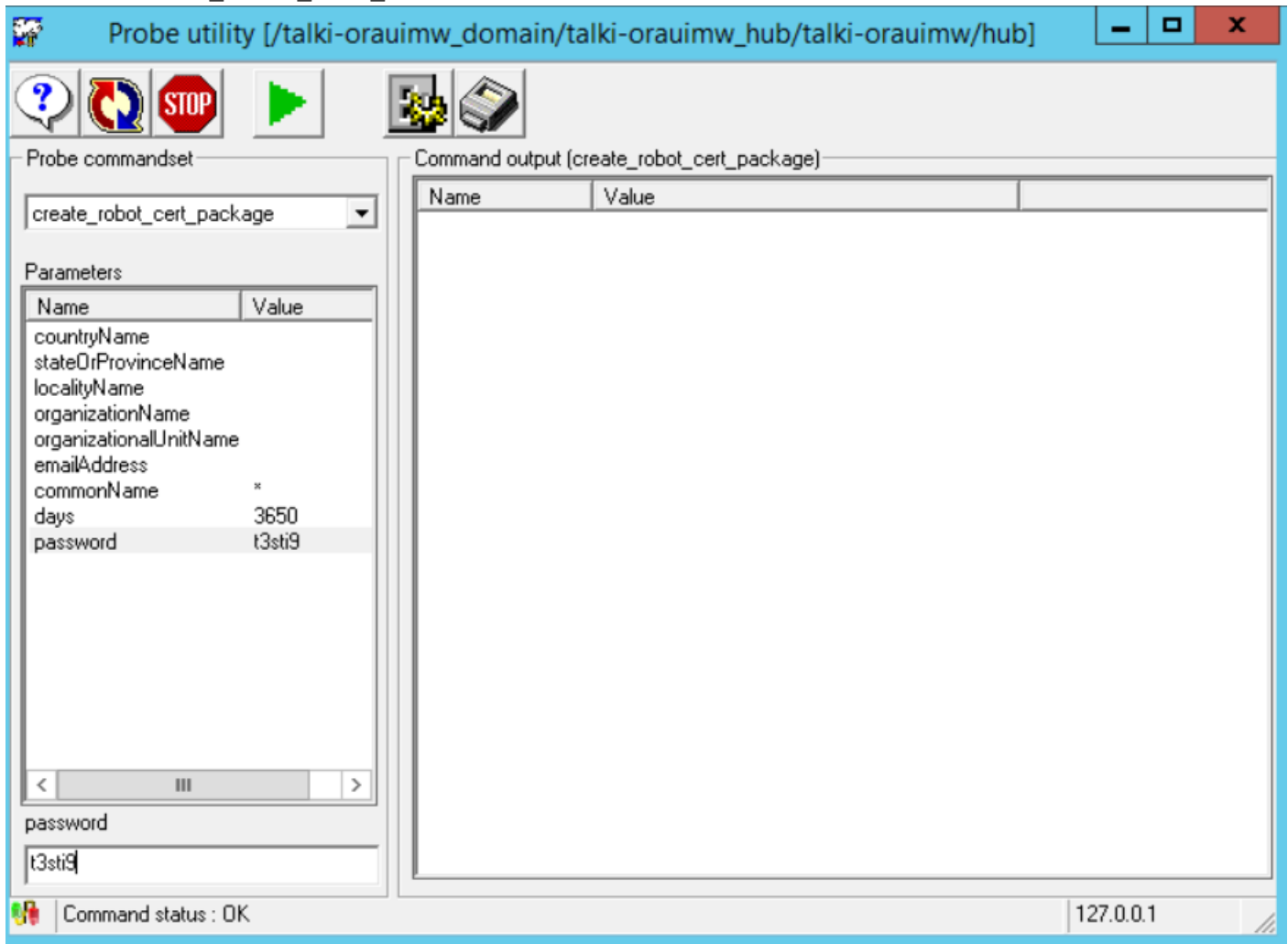
Deploy this package to the required non-secure robot (for example, tunnel client robot, independent robot, UMP/OC robot, CABI robot) that you want to secure. When you deploy this certificate package to a robot that you want to secure, the package deploys the \* certificate .pem file in the `<Nimsoft>\robot\certs` folder and updates the robot.cfg file with the .pem file location.

#### **NOTE**

Ensure that the latest version of the distsrv probe or ade probe (released with 20.3.0) is already deployed to the secure tunnel server for this callback to work properly. If the latest version of both the probes is available, the callback uses distsrv by default. If distsrv is not available, it uses the ade probe.

**Follow these steps:**

1. Open the probe utility (pu) for the secure tunnel server hub.
2. Select the `create_robot_cert_package` callback from the drop-down list as shown in the following screenshot:



3. Provide appropriate information for the following parameters:
  - a. **countryName** (Optional)
  - b. **stateOrProvince**(Optional)
  - c. **localityName**(Optional)
  - d. **organizationName**(Optional)
  - e. **emailAddress**(Optional)
  - f. **commonName** (Mandatory)  
Specify the common name as \* (wildcard) to generate a \* tunnel certificate.
  - g. **days** (Mandatory)  
Specify the validity of the certificate.
  - h. **password** (Mandatory)  
Specify the password for the certificate.

**NOTE**

If you try to run this callback without providing values for the mandatory parameters (**commonName**, **days**, and **password**), the callback displays the invalid argument error.



4. Run the command request.  
When the command is successfully completed, the robot client certificate package (UIMRobotCert) is created and is added to the secure tunnel server archive.
5. Deploy this certificate package to the robots that you want to secure.

### **Add a New Robot to a Secure Environment**

If you want to add a new robot to a secure environment, you can use the appropriate method depending on your requirements:

- Add a Robot Without Using a Non-Secure Secondary Hub
- Add a Robot Using a Non-Secure Secondary Hub
- Add a Robot Using UMP/OC
- Add a Robot Using an XML File

### **Add a Robot Without Using a Non-Secure Secondary Hub**

You can directly add a robot to the secure setup.

#### **NOTE**

This procedure is not applicable for Linux. For Linux, you must have a non-secure secondary hub in your secure setup. Therefore, for Linux, see the [Add a Robot Using a Non-Secure Secondary Hub](#) section.

#### **Follow these steps:**

1. Ensure that the secure hub to which you want to add a new robot already has hub\_adapter enabled on it.
2. Download the robot installer (NimBus Robot.exe) from the UIM home page.
3. Run the robot installer on the computer to install the robot. Provide information about the required secure hub to which you want to add the robot.
4. Deploy the latest robot (7.97 or later).
5. (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the robots pointing to the hub.
6. (Prior to 20.3.3) On the secure tunnel server, use the robot certificate callback and generate the robot certificate package, if not already done. Deploy the robot certificate package to the robot computer.
7. Deploy the latest secure robot to the robot computer.  
Non-secure robot is now converted to a secure robot.

### **Add a Robot Using a Non-Secure Secondary Hub**

You can use a non-secure secondary hub in your secure environment to add a new robot.

#### **NOTE**

For Linux, you must have a non-secure secondary hub in your secure setup. Also, ensure that the required package (install\_LINUX\_23\_64) is already available in the non-secure secondary hub archive.

#### **Follow these steps:**

1. Download the robot installer (nimldr or NimBus Robot.exe) from the UIM home page to the computer that you want to add as a robot.
2. Run the robot installer on the computer to install the robot. Provide information about the required non-secure secondary hub during the robot installation.  
The following example screenshot shows that the nimldr is executed successfully and deploys the new robot:

```

What is that Nimsoft Hub's IP address?
==>[10.17[REDACTED]]
nimbus.service is not a native service, redirecting to /sbin/chkconfig.
Executing /sbin/chkconfig nimbus on
Cleaning up temporary files
Finished Robot installation!
[root@talki-robo2 LINUX_23_64]# █

```

3. Deploy the latest robot.

The following example screenshot shows that the non-secure robot is successfully deployed to the new robot computer:

The screenshot shows a tree view of domains on the left and a table of probes on the right. The domain tree includes:

- talki-orauiw\_domain
  - talki-orahub1w
  - talki-orahub2l
  - talki-orauiw\_hub
  - talki-sql14
  - talki-robo2
  - talki-sql14

The probe table on the right is as follows:

| Probe      | Version |
|------------|---------|
| cdm        | 6.42-MC |
| controller | 9.20    |
| hdb        | 9.20    |
| spooler    | 9.20    |

4. Move the robot to the appropriate secure hub in your environment.

The secure hub must be able to communicate with the non-secure robot because of the presence of hub\_adapter on the secure hub.

The following example screenshot shows that the new robot is successfully moved to the secure hub:

The screenshot shows a tree view of domains on the left and a table of probes on the right. The domain tree includes:

- talki-orauiw\_domain
  - talki-orahub1w
  - talki-orahub2l
  - talki-orauiw\_hub
  - talki-oracabiw
  - talki-orauiw
  - talki-oraumpw
  - talki-robo1
  - talki-robo2
  - talki-sql14
  - talki-sql14

The probe table on the right is as follows:

| Probe      | Version |
|------------|---------|
| cdm        | 6.42-MC |
| controller | 9.20    |
| hdb        | 9.20    |
| spooler    | 9.20    |

5. On the secure tunnel server, use the robot certificate callback and generate the robot certificate package, if not already done.
6. (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the robots pointing to the hub.
7. (Prior to 20.3.3) Deploy the robot certificate package to the robot computer.
8. Deploy the latest secure robot to the robot computer.  
Non-secure robot is now converted to a secure robot.

### **Add a Robot Using UMP/OC**

In this scenario, you use UMP/OC in your secure environment to add a robot. Ensure that the hub\_adapter probe is active on the secure hub. This allows the secure hub to communicate with the non-secure robot.

#### **Follow these steps:**

1. In your secure environment, log in to OC.
2. Start the [Discovery Wizard](#) and locate the device that you want to convert to a secure robot.
3. Select the device and deploy the latest non-secure robot.  
The non-secure robot is deployed in the secure setup and is visible in IM and Admin Console.
4. (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the robots pointing to the hub.
5. (Prior to 20.3.3) On the secure tunnel server, use the robot certificate callback and generate the robot certificate package, if not already done. Deploy the robot certificate package to the robot computer.
6. Deploy the latest secure robot to the robot computer.  
Non-secure robot is now converted to a secure robot.

### **Add a Robot Using an XML File**

In this scenario, you use an [XML file](#) in your secure environment to add a robot. Ensure that the hub\_adapter probe is active on the secure hub. This allows the secure hub to communicate with the non-secure robot.

#### **Follow these steps:**

1. In your secure environment, ensure that the latest automated\_deployment\_engine (ade) probe is running on the secure primary hub.
2. Navigate to the <Nimsoft>\probes\service\automated\_deployment\_engine folder.
3. Create an XML file and provide all robot-related details (for example, user name, password, computer details, hub information).
4. Save the file with the name as host-profiles.xml in the <Nimsoft>\probes\service\automated\_deployment\_engine folder.  
The ade probe checks the XML file and deploys the non-secure robot. The non-secure robot becomes visible in IM and Admin Console.
5. (For 20.3.3 and later) Follow the instructions in the [Secure Transmission of Certificates](#) article to securely transfer the certificates from the hub to the robots pointing to the hub.
6. (Prior to 20.3.3) On the secure tunnel server, use the robot certificate callback and generate the robot certificate package, if not already done. Deploy the robot certificate package to the robot computer.
7. Deploy the latest secure robot to the robot computer.  
Non-secure robot is now converted to a secure robot.

An example of an XML file is as follows:

```
<hosts>
 <host>
 <profile>Windows</profile>
```

```
<arch>64</arch>
<hostname>10.xxx.xxx.xxx</hostname>
<username>Administrator</username>
<password>in#4572</password>
<domain>uimser01_domain</domain>
<hubip>10.xxx.xxx.xxx</hubip>
<hub>uimser01_hub</hub>
<hubrobotname>uimser01</hubrobotname>
<hubport>48002</hubport>
<robotname>talsec_robot</robotname>
<tempdir>c:\tmp</tempdir>
</host>
</hosts>
```

### **Add a New Hub to a Secure Environment**

If you want to add a new hub to a secure environment, you can use the appropriate method depending on your requirements:

- Add a New Hub Without Using a Non-Secure Secondary Hub
- Add a New Hub Using a Non-Secure Secondary Hub

### **Add a Hub Without Using a Non-Secure Secondary Hub**

You can directly add a hub to the secure setup.

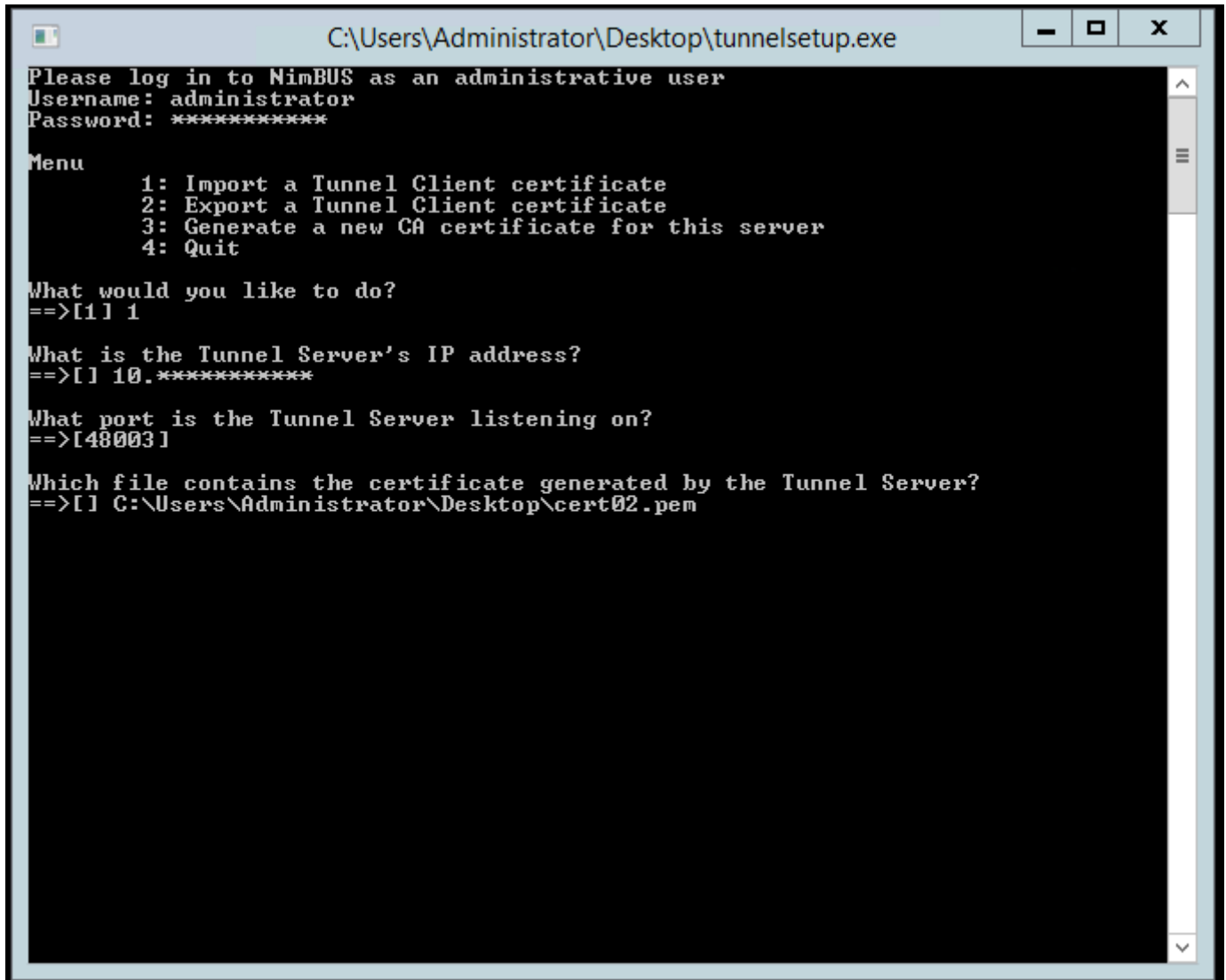
#### **NOTE**

This procedure is not applicable to Linux. For Linux, you must have a non-secure secondary hub in your secure setup. Therefore, for Linux, see the [Add a New Hub Using a Non-Secure Secondary Hub](#) section.

#### **Follow these steps:**

1. Download the secondary hub installer (NimBUS Infrastructure.exe) from the UIM home page to the system that you want to add as a hub.
2. Run the installer to install the secondary hub on the system. Provide the domain name to which you want to add this hub.
3. Copy the tunnelsetup.exe utility and the client certificate from the secure tunnel server. The tunnelsetup.exe utility is available in the `..\Nimsoft\hub` folder. The client certificate is available in the `..\Nimsoft\hub\certs` folder.
4. Run the tunnelsetup.exe on the new hub and provide all the details (for example, tunnel server IP, UIM administrator credentials, and certificate path).

An example screenshot is as follows:



```

C:\Users\Administrator\Desktop\tunnelsetup.exe
Please log in to NimBUS as an administrative user
Username: administrator
Password: *****

Menu
 1: Import a Tunnel Client certificate
 2: Export a Tunnel Client certificate
 3: Generate a new CA certificate for this server
 4: Quit

What would you like to do?
==>[1] 1

What is the Tunnel Server's IP address?
==>[1] 10.10.10.10

What port is the Tunnel Server listening on?
==>[48003]

Which file contains the certificate generated by the Tunnel Server?
==>[1] C:\Users\Administrator\Desktop\cert02.pem

```

**NOTE**

Alternatively, you can use IM on this new hub to make it a tunnel client of the secure tunnel server. To do so, you copy the certificate from the secure tunnel server and create a tunnel client certificate on the new hub.

5. Open the hub configuration, navigate to the **Status** tab (**Tunnel Status** section) and verify that the tunnel connection is up and running.  
The new non-secure hub is now listed in the domain.
6. Follow the usual steps (as explained earlier) to bring the new hub to a secure state depending on your scenario:
  - a. Deploy hub\_adapter to the new hub.
  - b. Deploy the latest robot to the new hub.
  - c. Deploy the latest secure hub to the new hub.
  - d. Deploy the robot certificate package to the robot.
  - e. Deploy the latest secure robot to make it a secure robot.
 You have successfully added a new hub and secured it.

## Add a Hub Using a Non-Secure Secondary Hub

You can add a new hub to a secure setup by using a non-secure secondary hub, which is already present in the secure setup.

### NOTE

For Linux, you must have a non-secure secondary hub in your secure setup. Also, ensure that the required package (install\_LINUX\_23\_64) is already available in the non-secure secondary hub archive.

### Follow these steps:

1. Download the secondary hub installer (nimldr or NimBUS Infrastructure.exe) from the UIM home page.
2. Run the installer to install the secondary hub on the new system. Provide the required non-secure secondary hub information during the robot installation. For Linux, ensure that you make the new hub a tunnel client during the hub installation.

The following example snippet shows that nimldr is being used to install the hub as a tunnel client:

```
Attempting to log in to NMS...
Enter Nimsoft username and password...
 Username: administrator
 Password:
 1 /talki-orauimw_domain/talki-sql14/talki-sql14/distsrv
Beginning download of install_LINUX_23_64
/
Done!

What are we installing? (1=Robot,2=Infrastructure)
==>[1] 2
A Nimsoft Robot and Hub will be installed.

Would you like to install the Distribution Server (distsrv)?
==>[yes]
Extracting files from archive /opt/nimsoft/tmp//install_LINUX_23_64.zip to temp directory /opt/nimsoft/tmp/

Where should NMS be installed?
==>[/opt/nimsoft]

Automatically unregister Robot from Hub on termination?
==>[no]

Should this Robot run in passive mode?
==>[no]
```

3. For Windows, perform the following steps to make the new hub as a tunnel client (already explained in the previous procedure):
  - a. Copy the tunnelsetup.exe utility and the client certificate from the secure tunnel server. The tunnelsetup.exe utility is available in the ..\hub folder. The client certificate is available in the ..\hub\certs folder.
  - b. Run the tunnelsetup.exe on the new hub and provide all the details (for example, tunnel server IP, UIM administrator credentials, and certificate path).

For Linux, the new hub is made the tunnel client during the hub installation.
4. Open the hub configuration, navigate to the **Status** tab (**Tunnel Status** section) and verify that the tunnel connection is up and running.

The following example screenshot shows the successful tunnel communication between the new hub (talki-robo2) and the secure primary hub:

| Peer Hub                      | Started             | Last     | Connection Stats(ms) | Connections | Traffic In/Out |
|-------------------------------|---------------------|----------|----------------------|-------------|----------------|
| talki-orauimw_hub [10.17.1... | 5/14/2019 3:46:5... | 15:47:50 | 6 / 33 / 139         | 8           | 85 KB/134 KB   |

5. Follow the usual steps (as explained earlier) to bring the new hub to a secure state depending on your scenario:
  - a. Deploy hub\_adapter to the new hub.
  - b. Deploy the latest robot to the new hub.
  - c. Deploy the latest secure hub to the new hub.
  - d. Deploy the robot certificate package to the robot.
  - e. Deploy the latest secure robot to make it a secure robot.
 You have successfully added a new hub and secured it.

### **Converting Back to a Non-Secure Mode**

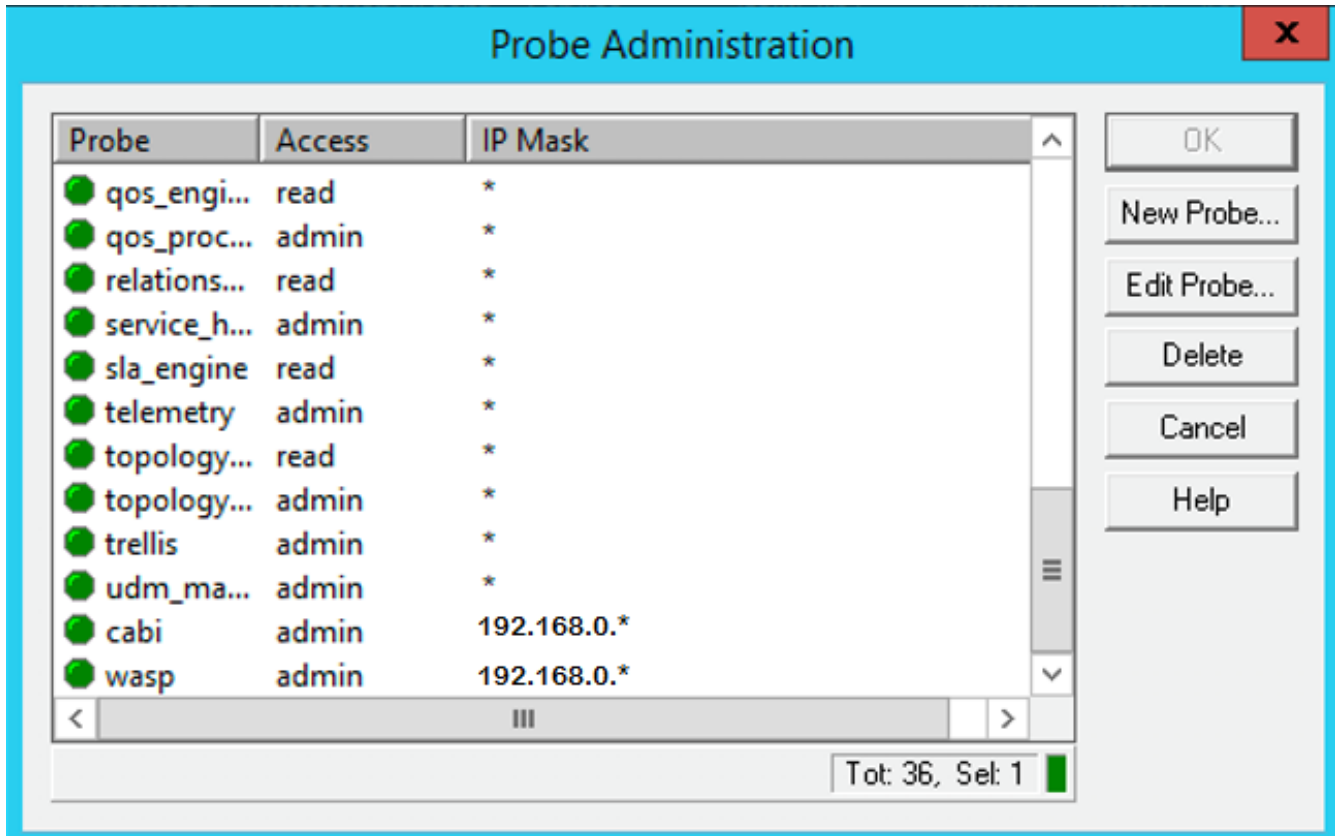
To revert your secure environment to the non-secure state, you must downgrade all the robots and hubs in your secure environment by downloading and installing an older version of the robot and hub from the archive. Based on your setup, you can downgrade robots and hubs as follows:

1. If your secure environment consists of standalone robots that are connected to a secure hub, then you must first downgrade all the standalone robots to an older version that you downloaded from the archive.
2. After you downgrade standalone robots, downgrade the robots running on the secure hub to an older version that you downloaded from the archive.
3. After you downgrade all the robots, downgrade the hubs to an older version that you downloaded from the archive.

### **Enable CABI and OC to Communicate Securely from Separate Secure Robots**

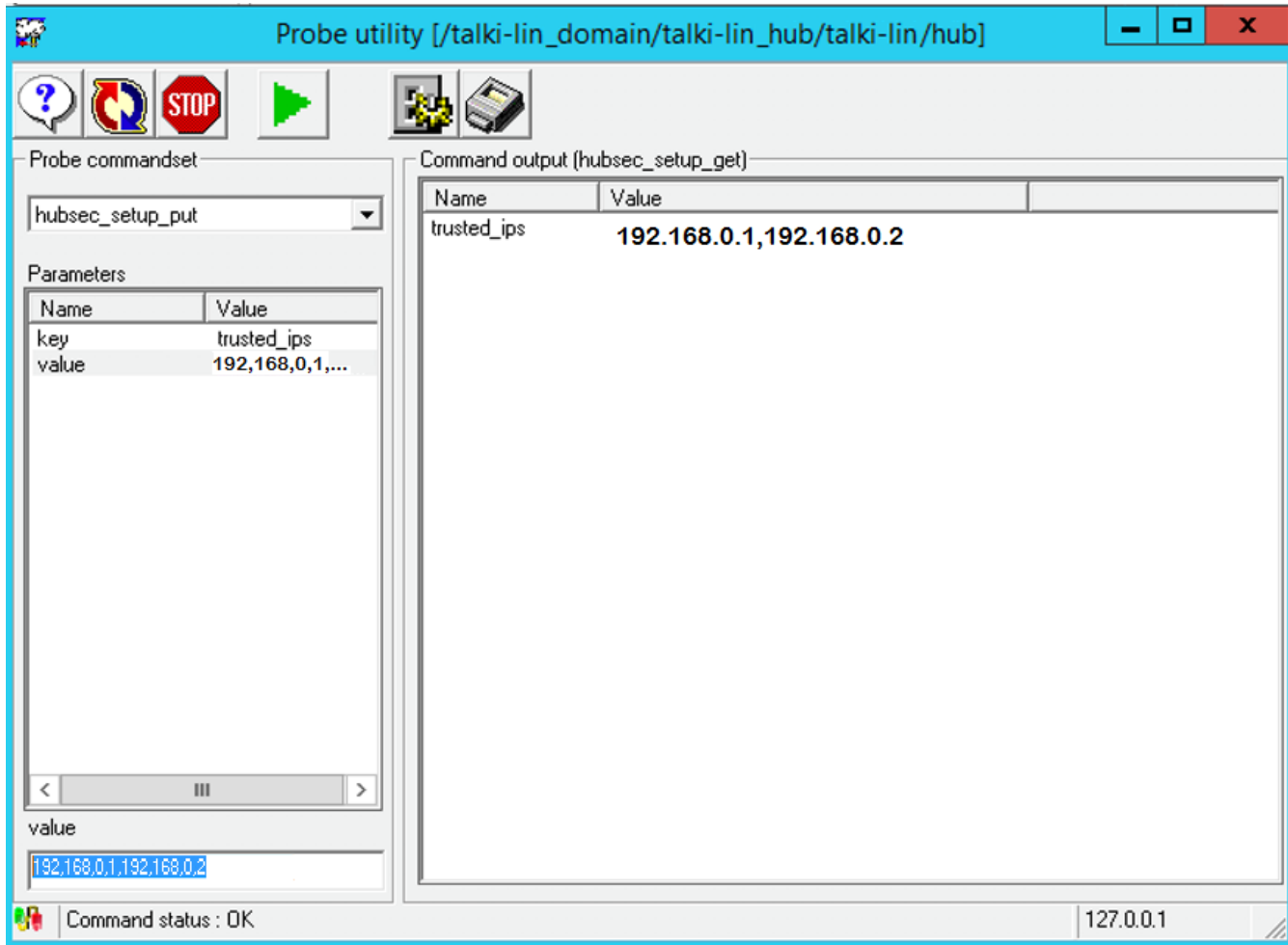
To enable CABI and OC to communicate securely from separate secure robots, follow these steps:

1. Whitelist the IP subnets where UMP and cabi are running by using the existing probe administration UI in IM. This configuration ensures that the secure bus understands that wasp and CABI on these subnets can be trusted by the bus.



- Using Probe Utility, use the `hubsec_setup_put` callback on the primary hub to add the IPs of the UMP/OC robot and CABI robot as "trusted\_ips" in the `security.cfg` file of the hub. Use a comma-separated list. This configuration ensures that the secure bus understands that these are special robots, and user logins from these robots must be allowed without downgrading access.





- Restart the primary hub, restart OC, wait until OC is fully up, and then restart CABI.

### Known Issues

The following are the secure hub- and robot-related known issues:

- The ppm probe provides functionality for the Admin Console probe configuration UIs. The ppm probe does not run on AIX hubs. To configure robots and probes on AIX hubs, use the Raw Configure utility in Admin Console, or use Infrastructure Manager.
- If the communication with a robot fails in Linux, review your network configuration:
  - Check for a valid entry for the local system in the `/etc/hosts` file for a robot, hub, server, or OC system
  - The entry for the local system must be a fully qualified hostname and IP address.
  - If only the loopback address is defined, for example, localhost 127.0.0.1, the controller is unaware of its own IP address.
  - IP address problems result in network communication failure.
- The `automated_deployment_engine` robot distribution to Windows targets sometimes fails to activate the hdb and spooler probes. To resolve the issue, do a validate security on the affected probes (hdb and spooler)
- If robots are added to the inventory by automated discovery, OC cannot auto-deploy the robots to AIX or z/Linux systems. Use one of the following alternative methods:
  - Run the native installer manually or with a third-party tool. See [Deploy Robots in Bulk with a Third-Party Tool and Native Installers](#).

- b. Use the `automated_deployment_engine` (ade) probe with an XML file. See [Deploy Robots with an XML File and the ADE Probe](#).
- c. Import an XML file in OC. See [Deploy Robots with an XML File in OC](#).
- In a secure environment, if any probe that is installed on an independent secure robot tries to subscribe to queues in the related secure hub, the probe fails to attach to the queues. As a workaround, if the probes require to read or publish to a hub queue, then deploy the probe to the primary hub robot.
- If you rename the package name in the archive and try to deploy the package to the hub after logging into the same hub, an unexpected error can appear. However, deployment is completed without any issue. For example, if you rename the `robot_update` package in the archive and try to deploy it to the hub after logging into that hub, you get the following error: `Aborted, retry limit exceeded, unknown status`, but the deployment completed successfully.
- In a *regular to secure* conversion, when you deploy the new `hub_secure` or `robot_update_secure` packages, an error message is shown that states that the deployment has been aborted. However, the deployment completes without any issue. If you receive this error, you can ignore it.
- `distsrv 9.20` has a dependency on `robot 9.20/9.20S`. During an upgrade, when you try to deploy `distsrv` before the robot deployment, an error message is displayed stating that the existing robot version is lower than `9.20/9.20S`. This error message does not display the suffix "S" in the robot version if the robot package is a secure one. It simply displays the version without "S", which is misleading. The following error is displayed: `Dependency check error: Robot version >=9.20 is required (7.97 found)`

### **Additional Information**

- **Manual Conversion Process**

If you do not convert to secure hub and robot using the installer (UIM Server) and want to do it at a later stage, you can follow the manual process. However, we recommend that you use the installer as it automatically performs various tasks and significantly eases the process. For more information about how to perform these manual steps, follow the information documented in [Manually Convert to Secure and Hub](#).

- **Troubleshooting**

To review various troubleshooting topics, see the [Troubleshooting Secure Hub and Robot](#) article.

## **Manually Upgrade to Secure Hub and Robot**

This article provides comprehensive information about how to manually convert to a secure hub and robot. This manual process is helpful when you do not use the secure hub and robot option while using the [UIM Server installer](#) and want to convert your setup to a secure setup at a later stage.

### **NOTE**

We recommend that you use the [UIM installer](#) instead of the manual process, as the installer automatically performs various tasks and significantly eases the secure conversion process.

The following topics cover the required information:

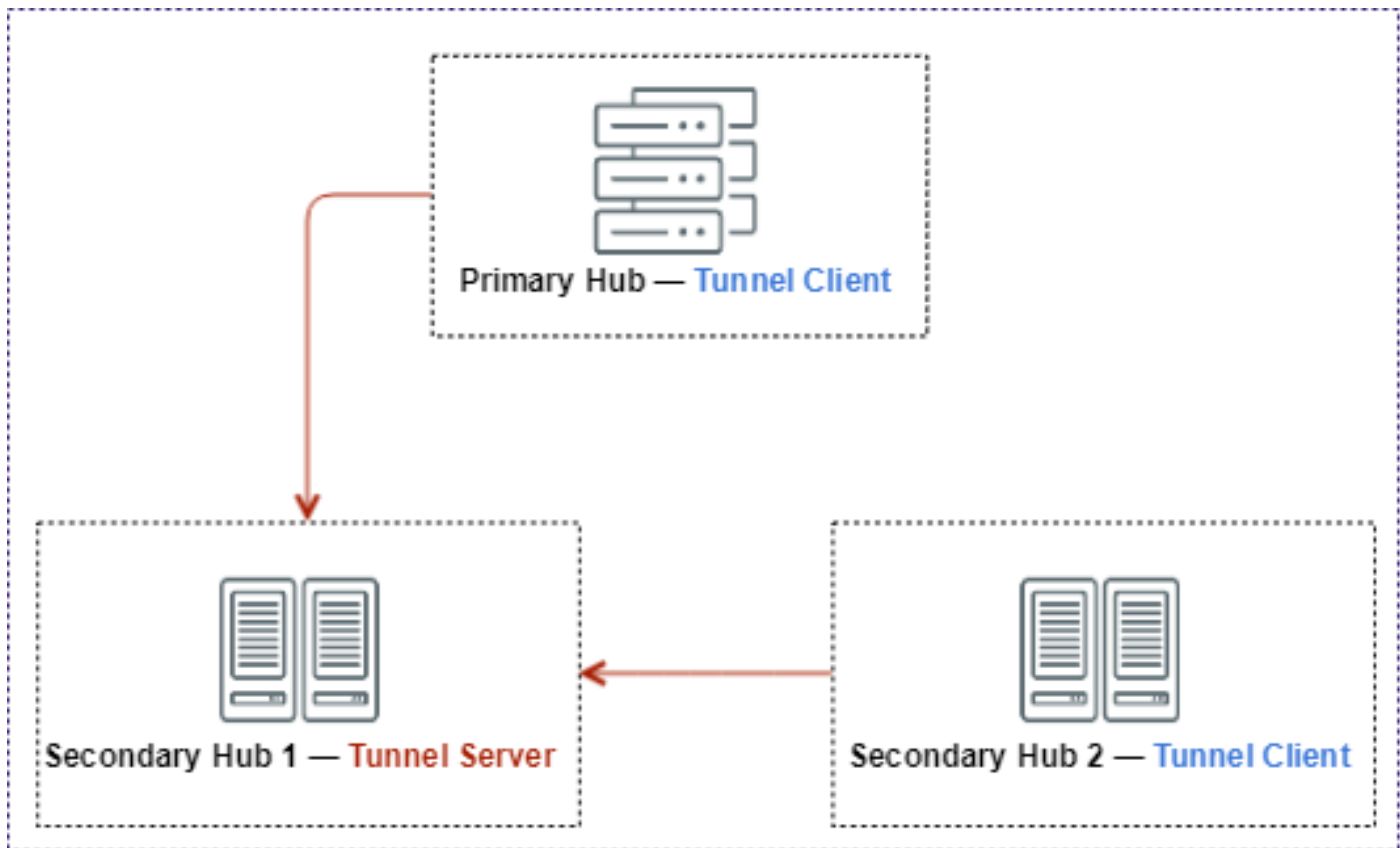
### **Manual Conversion Scenario**

The following are the assumptions for the secure hub and robot conversion process that is explained in this article:

- The example domain consists of three hubs:
  - Primary hub - Tunnel Client
  - First secondary hub - Tunnel Server
  - Second secondary hub - Tunnel Client
- You do not yet have tunnels connecting your hubs.

The following diagram shows the domain setup:

Figure 19: Tunnel\_Setup



### Considerations

We recommend that you review all the considerations that are outlined in the [Secure Hub and Robot](#) article.

### Prerequisites

Review the following prerequisites:

1. You have already executed the installer (UIM Server) in a non-secure mode on the existing UIM setup. This ensures that the latest packages, including secure packages, are available in the primary hub archive.
2. [Configure the first secondary hub as a tunnel server.](#)
3. [Configure the other two hubs as tunnel clients \(primary hub and second secondary hub\).](#)
4. [Verify the tunnel connectivity.](#)
5. [Get CA-approved certificates and place them on the tunnel server and tunnel client computers.](#)

### Configure the First Secondary Hub as Tunnel Server

A tunnel server consumes extra resources. To avoid the extra burden on the primary hub, choose a secondary hub in the domain to be the tunnel server. Upgrade this tunnel server hub first.

#### **Follow these steps:**

1. In IM, open the hub probe configuration for the first secondary hub; that is, the tunnel server hub.
2. In the **General** tab, select the **Enable Tunneling** option.

3. Select the **Tunnels** tab.
4. Select **Server Configuration**.
5. Select the **Active** option.
6. Create a local Certificate Authority (CA) for the tunnel server. Take the defaults for the certificate information here, and supply a password. Non-secure tunnel certificates require a password. This step creates a CA and server certificate (CN: IP address).

**NOTE**

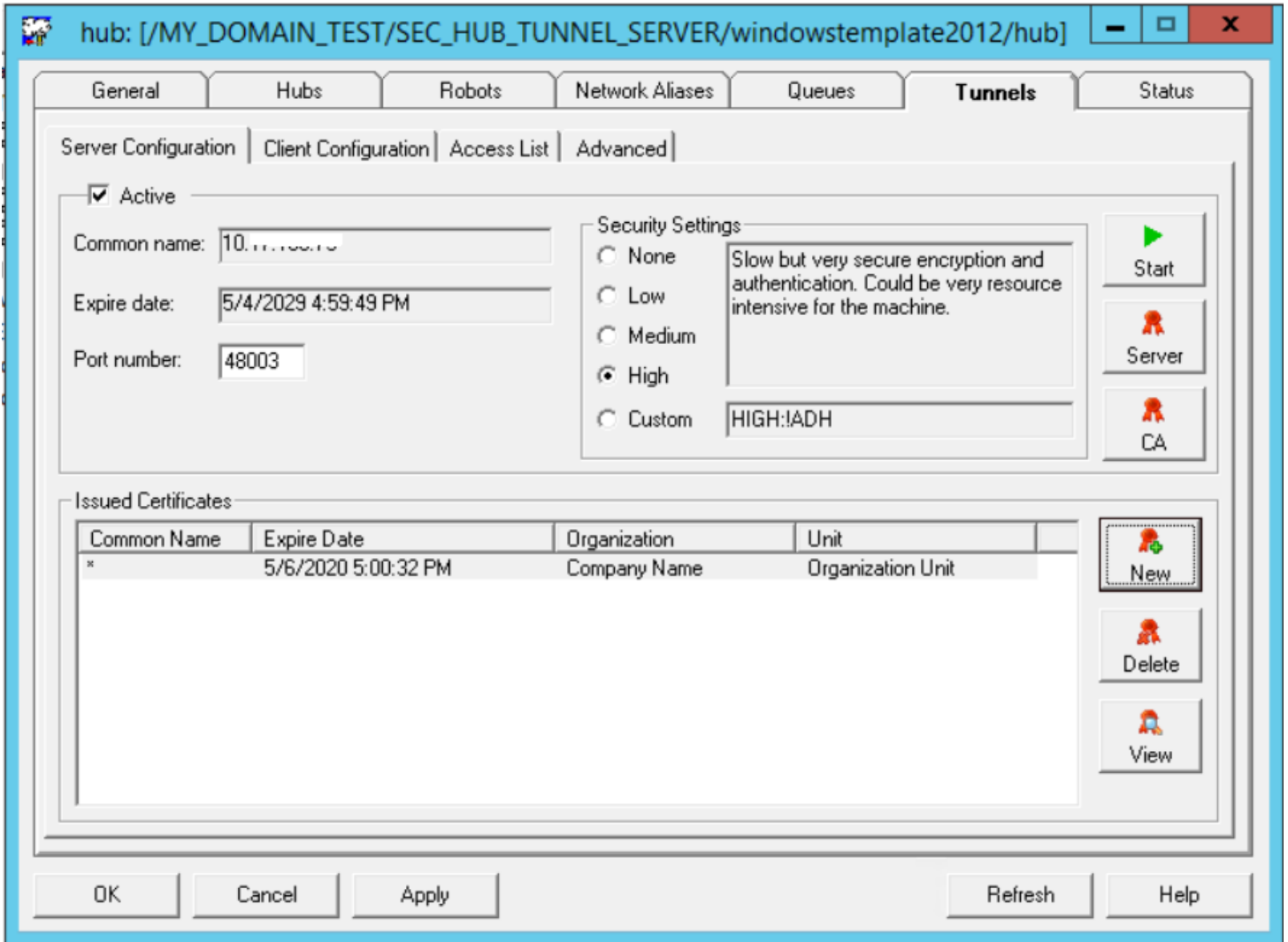
While configuring the secure hub and robot at a later stage, you can work with the same tunnel certificates that you have already configured here or you can replace them with the third-party certificate, as required. That is, you can use the same tunnel certificates or third-party certificates on the required robots. You can also use \* (wildcard) as the commonName to generate and use \* tunnel client certificates.

7. When you select **OK** on the **Certificate Authority Setup**, you are returned to the **Server Configuration** tab.
8. Select **New** to generate the new certificate that is signed by the same CA, which you can use for your tunnel clients. You can use \* as the common name to issue a \* tunnel certificate.
9. Provide the newly issued certificate when you create each tunnel client. Select **View**, and select the **Certificate** tab. You can copy the certificate to the Clipboard.
10. Select **OK** to return to the **Server Configuration** tab, select **Apply**, and select **OK**. Select **Yes** to restart the hub probe and activate the new tunnel server.

Appropriate files are created in the <Nimsoft>\hub\certs folder during the tunnel server configuration:

- The ca.pem is the local CA file, server.pem is the server certificate file, and cert#.pem (for example, cert02.pem) is the \* tunnel certificate file on the tunnel server.
- Note the timestamp of your cert#.pem file to identify your required \* tunnel certificate file, because it is possible that you have multiple client certificate files on the tunnel server. However, it is recommended to delete the existing unused \* certificates to avoid confusion. There is no need to have multiple \* certificates that are signed by the same CA. Furthermore, you need to copy this file (cert#.pem) to all the robots pointing to this server and update the robot.cfg with the certificate information as explained later in this article.

The following example screenshot shows the tunnel server certificate configuration:



### **Create Tunnel Clients on Primary Hub and Other Secondary Hub**

The primary and the other secondary hubs in the domain connect to the tunnel server as tunnel clients. Create tunnel clients on these hubs.

#### **Follow these steps:**

1. In IM, open the hub probe configuration for the primary hub.
2. In the **General** tab, select the **Enable Tunneling** option.
3. Select the **Tunnels** tab.
4. Select **Client Configuration** to create a new tunnel client.
5. Select **New**.
6. Select the **Active Tunnel** option.
7. Clear the **Check Server CommonName** option.
8. Enter the description.
9. In the **Server** field, enter the IP address of the tunnel server hub.
10. In the **Password** field, enter the password that you specified when you created the certificate that you wanted to use for tunnel clients.

11. In the **Certificate** field, paste in the body of the certificate you copied from the tunnel server certificate.
12. Select **OK**.  
The new tunnel client is added to the list of tunnel clients on the hub. On a given hub, you can have only one tunnel server, but you can have many tunnel clients.
13. Select **Apply**, and then select **OK**.  
The hub restarts to pick up the new tunnel client.
14. Repeat the steps to create a tunnel client on the remaining hubs in the domain.

Appropriate \* tunnel certificate .pem file (client#.pem) is created in the <Nimsoft>\hub\certs folder during the tunnel client configuration. You need to copy this file (client#.pem) on all the robots pointing to this computer and update the robot.cfg with the certificate information as explained later in this article.

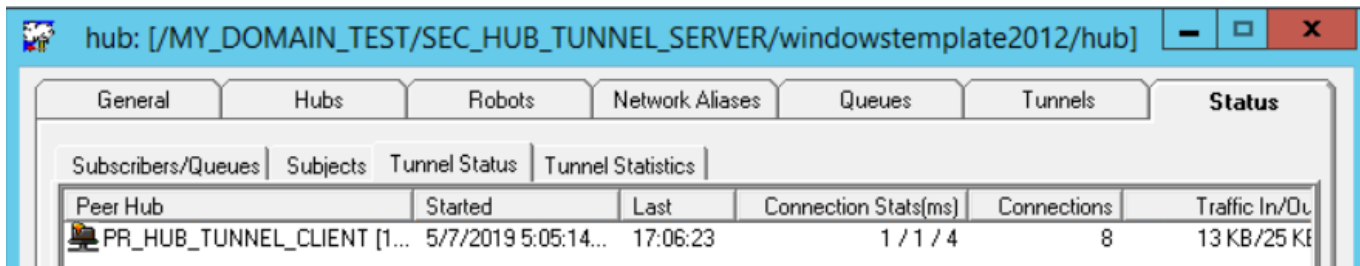
### **Verify Tunnel Connectivity**

Verify the status of each tunnel server and tunnel client to ensure that they are connected.

#### **Follow these steps:**

1. In IM, open the hub probe configuration for the first secondary hub—the tunnel server hub.
2. Select the **Status** tab.
3. Select **Tunnel Status**.  
The **Peer Hub** list contains an entry for each tunnel client that is connected to the tunnel server. Statistics are shown for each tunnel client. Each tunnel client hub also reports the tunnel server it is connected to, and includes statistics.

The following screenshot shows the tunnel connectivity between the secondary hub (which is a tunnel server in this example screenshot) and primary hub (which is a tunnel client in this example screenshot):



| Peer Hub                   | Started             | Last     | Connection Stats(ms) | Connections | Traffic In/Du |
|----------------------------|---------------------|----------|----------------------|-------------|---------------|
| PR_HUB_TUNNEL_CLIENT [1... | 5/7/2019 5:05:14... | 17:06:23 | 1 / 1 / 4            | 8           | 13 KB/25 KB   |

### **Get CA-Approved Certificates (For Third-Party Certificates)**

#### **NOTE**

If you are using tunnel certificates (for example, \* certificate), you do not need to perform the steps that are mentioned in this section. These steps are only for third-party certificates.

**(Only for third-party certificates)** You can use the same third-party certificates for hub-to-hub and robot-to-hub communications. Before you create and use third-party certificates, review the following third-party certificates-related requirements:

- Elliptic curve (EC) and RSA ciphers are supported.
  - Use PEM format for keys and certificates.
  - Certificate revocation lists are not checked.
  - Non-standard X.509 certificate extensions are not supported.
- Validation of certificate commonName or subjectAltName for hub-to-hub communication is enabled by default.
- The public key, private key, and certificate chain files are required on all hubs and robots.
- Copy your third-party certificate files to each hub, making a note of the location.

To get CA-approved certificates (for example, RSA with server `uim1.ca.com`), you can use OpenSSL and can follow these steps:

**NOTE**

For wildcard certificates, use `*` in the Common Name field when prompted; for example, `*.ca.com`.

1. Ensure that OpenSSL is already available on the computer where you want to create certificates.
2. Create a private key for the server `uim1.ca.com` as follows (example):  

```
openssl genrsa -out uim1.ca.com.key 2048
```
3. Create a certificate request (CSR) as follows (example):  

```
openssl req -new -key uim1.ca.com.key -out uim1.ca.com.key.csr
```
4. Send the certificate request to your certificate authority (CA) and request for the `.pem` file.  
 CA sends the required `.pem` files for your server and the applicable CA certificate chain.

If you receive the files in `.crt` format, you can use the following command to convert a `.crt` file to a `.pem` file (example):

```
openssl x509 -in uim1.crt -out uim1-crt.pem -outform pem
```

Additionally, you can use the following command to convert private keys to PEM (example):

```
openssl rsa -in uim1.ca.com.key -out uim1-pvt-crt.pem -outform pem
```

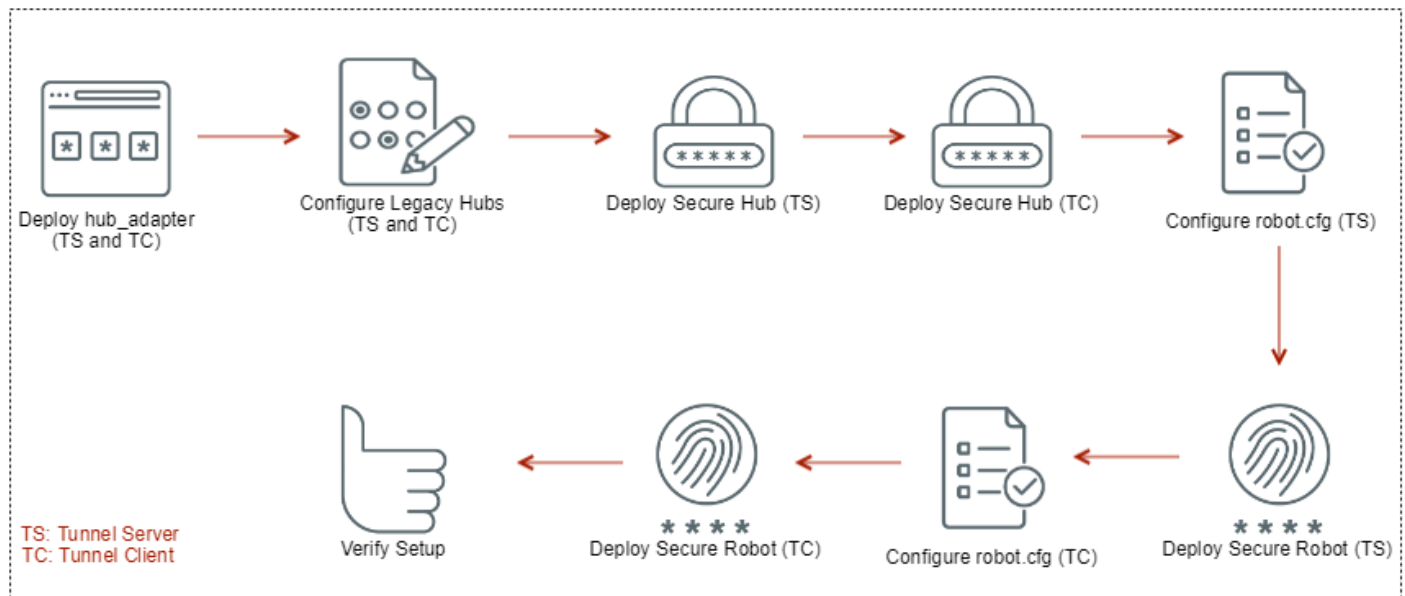
**NOTE**

Copy your third-party certificate files to each hub, making a note of the location. Also, you can use a single certificate for all robots.

**Conversion Process**

The following diagram shows the process steps to convert to a secure hub and robot:

**Figure 20: Manual\_Convert\_Secure\_Hub\_Draft**



The steps are as follows:

1. [Deploy hub\\_adapter on the tunnel server and the tunnel clients.](#)
2. [Configure non-secure hubs to use third-party certificates.](#)
3. [Deploy the secure hub on the tunnel server.](#)

4. [Deploy the secure hub on the tunnel clients.](#)
5. [Configure robot.cfg on the tunnel server.](#)
6. [Deploy the secure robot on the tunnel server.](#)
7. [Configure the robot.cfg file on the tunnel clients.](#)
8. [Deploy the secure robot on the tunnel clients.](#)
9. [Verify the setup.](#)

**NOTE**

For deploying a secure hub to a tunnel server and tunnel client, ensure that you have one non-secure hub (which can be one of the tunnel clients) in the setup for deploying the packages.

If the non-secure hub that you are using for deploying the packages is **not a primary hub**, copy the secure hub, secure robot, hub\_adapter, distsrv (required for running the certificate callback), and non-secure robot builds from the **non-secure primary hub** ..\Nimsoft\archive folder to the ..\Nimsoft\archive folder of the **non-secure hub**. Connect to the non-secure hub using IM. Use this IM connection to import the packages into the non-secure hub archive and then deploy the required packages to the tunnel server and tunnel clients.

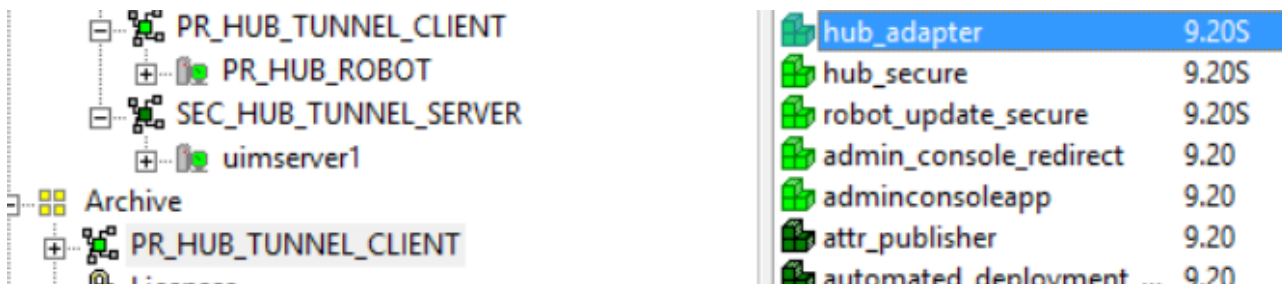
However, if the non-secure hub that you are using for deploying the packages is a **primary hub**, you do not need to copy the packages because they will be available in the non-secure primary hub archive. In this case, connect to the IM on the non-secure primary hub and deploy the required packages to the tunnel server and tunnel clients. The example screenshots that are included in this procedure use the primary hub (tunnel client) archive for deploying the packages.

**Deploy hub\_adapter on Tunnel Server and Tunnel Clients**

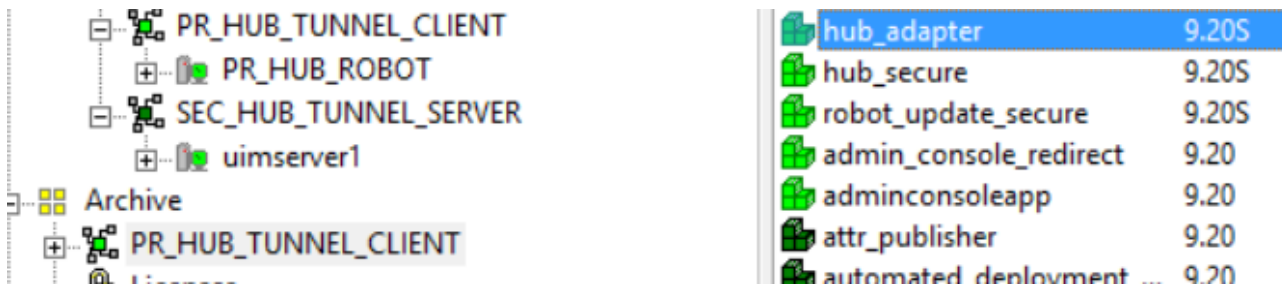
The hub\_adapter probe acts as a proxy for communication between a secure hub and non-secure robots. A secure hub cannot control non-secure robots unless a hub\_adapter is installed on it. Therefore, you must install the hub\_adapter probe on secure hubs that control non-secure robots.

Deploy the hub\_adapter probe from the archive to the tunnel server and the tunnel clients.

The following example screenshot shows that the hub\_adapter probe is already available in the primary hub archive. Also, note that hub and hub\_secure are also available in this archive:



The following example screenshot shows that the hub\_adapter probe is successfully deployed on the secondary hub (tunnel server) from the primary hub archive (which is a tunnel client in this example screenshot):





The following screenshot shows that the hub\_adapter probe is successfully deployed on the primary hub (tunnel client in this example screenshot). Note that all other probes have been updated because of the upgrade on the primary hub:



## Configure Non-Secure Hubs to Use Third-Party Certificates

### NOTE

This configuration is required only for third-party certificates. When you perform this configuration, the communication happens through the third-party certificates. However, if you are using tunnel certificates (for example, \* certificate), then you do not need to perform these steps; in this case, the communication happens through tunnel certificates.

**(Only for third-party certificates)** Copy your third-party certificate files to each hub, making a note of the location. Do not restart the hub after editing hub.cfg. The process restarts the hub and the changes you make to hub.cfg are evaluated at that time. If the hub configuration is updated to the secure configuration before the hub is upgraded, you lose the connectivity with that hub. Additionally, do not use raw config edit for hub.cfg.

- On non-secure tunnel clients hub, temporarily rename the following keys to unique key names in the <tunnel><clients> section of hub.cfg. Rename the keys to retain the values until the hub is upgraded to secure and the keys can be discarded. Rename:
    - cert
    - password
  - Set the following keys in the hub.cfg file on every hub.
    - For a tunnel server, locate the <tunnel><server> section of hub.cfg and add the following keys.
      - `ca_location`  
Specifies the location of a certificate chain file from a certificate authority (CA). The key can also refer to a directory where multiple root certificates are stored. If you provide a directory, use the hash format (for more information, see the [OpenSSL](#) documentation.)
      - `public_cert`  
Specifies the location of the public certificate file.
      - `private_key`  
Specifies the location of the private key file.
    - For each tunnel client, locate the <tunnel><clients><#> section of hub.cfg and add the following keys:
      - `ca_location`  
Specifies the location of a certificate chain file from a certificate authority (CA). The key can also refer to a directory where multiple root certificates are stored. If you provide a directory, use the hash format (for more information, see the [OpenSSL](#) documentation.)
      - `public_cert`  
Specifies the location of the public certificate file.
      - `private_key`  
Specifies the location of the private key file.
- Note:** For more information, see the [Linux](#) and [Windows](#) examples below.
- Save your changes.

Review the following points:

- Avoid using spaces in directory or file names.
- The maximum length of any key-value pair in a UIM configuration file is 2047 characters. This limit includes the entire line in the configuration file:
  - Indentation spaces
  - Key name, space, equal sign, and following space
  - The value of the key
- In Linux:
  - You can specify an absolute path, or a relative path from UIMHOME/hub.
  - Symbolic keys are supported for certificate keys.
  - The key-value pair specifying an absolute or relative path can be a maximum of 2047 characters.
- In Windows:
  - You can specify an absolute path, a relative path from UIMHOME/hub, or an absolute path in long UNC format.
  - The maximum length of a path in Windows is 259 characters. The operating system converts relative paths to absolute paths. Ensure that a relative path does not expand to exceed 259 characters.
  - Windows accepts the back slash ( \ ) or the forward slash ( / ) as the path separator in relative or absolute paths.
  - To use a path longer than 259 characters in Windows, use a long UNC path.
    - Long UNC paths begin with \\?\
    - A long UNC path must be an absolute path, and must use the back slash ( \ ).
    - The key-value pair specifying a long UNC path can be a maximum of 2047 characters.

#### Linux Example

In this case, UIMHOME=/opt/nimsoft and certificates files are stored in /opt/nimsoft/certs .

Add the following keys to the <tunnel><server> section of the hub.cfg file in Linux:

```
ca_location=/opt/nimsoft/certs/ChainFile.pem
public_cert=/opt/nimsoft/certs/PublicKey.pem
private_key=/opt/nimsoft/certs/PrivateKey.pem
```

#### Windows Example

Use an absolute local filesystem path:

```
ca_location=c:/certs/ChainFile.pem
ca_location=c:\certs\ChainFile.pem
```

Use a relative local filesystem path relative to C:\Program Files (x86)\nimsoft\hub:

```
ca_location=certs/ChainFile.pem
ca_location=certs\ChainFile.pem
```

Use a long UNC path:

```
ca_location=\\?\C:\<very_long_path>\certs\ChainFile.pem
```

#### **Deploy Secure Hub on Tunnel Server**

Secure hub requires the presence of the non-secure robot. Therefore, before you deploy the secure hub, ensure that the non-secure robot is already available on the hub.

The following example screenshot shows that the non-secure robot version has been updated by deploying the package from the primary hub (tunnel client in this screenshot) archive to the secondary hub (tunnel server in this screenshot):

| Probe       | Version |
|-------------|---------|
| hub_adapter | 9.20S   |
| controller  | 9.20    |
| spooler     | 9.20    |
| hdb         | 9.20    |
| hub         | 7.96    |
| distsrv     | 7.96    |

Now, the secure hub can be deployed to the secondary hub (tunnel server). The following example screenshot shows that the secure hub has been successfully deployed from the primary hub (tunnel client) archive to the secondary hub (tunnel server in this screenshot):

| Probe       | Version |
|-------------|---------|
| hub         | 9.20S   |
| hub_adapter | 9.20S   |
| controller  | 9.20    |
| spooler     | 9.20    |
| hdb         | 9.20    |
| distsrv     | 7.96    |

### **Deploy Secure Hub on Tunnel Client**

Upgrade the tunnel client hubs by following the same process that is explained for the tunnel server.

The following example screenshot shows that the secure hub has been successfully deployed on the primary hub (tunnel client in this example screenshot)

| Probe            | Version |
|------------------|---------|
| usage_metering   | 9.24    |
| hub_adapter      | 9.20S   |
| hub              | 9.20S   |
| udm_manager      | 9.20    |
| data_engine      | 9.20    |
| discovery_server | 9.20    |

Hubs restart after an upgrade. Allow a few minutes for tunnel communication to stabilize.

### **Configure robot.cfg on Tunnel Server**

You can use the same certificates for hub-to-hub and robot-to-hub communications. For example, if you have generated the \* tunnel certificates at the tunnel server, the same can be used on the robot pointing to that tunnel server.

#### **Follow these steps:**

1. Validation of certificate commonName or subjectAltName for robot-to-hub communication is enabled by default.

- Fully Qualified Domain Names (FQDN) are required for validation. If short host names are provided, validation fails.
  - Validation is platform-specific, but typically is first attempted through `/etc/hosts`. If validation fails, DNS validation is used:
    - The hosts file on Linux is `/etc/hosts`.
    - The hosts file on Windows is `C:\Windows\System32\drivers\etc\hosts`.
2. (For third-party certificates) Copy public key, private key, and certificate chain files to all hubs and robots.
  3. Set the following keys in `robot.cfg`:

**NOTE**

For third-party certificates, you must use only the first three parameters (`proxy_ca_location`, `proxy_cert`, and `proxy_private_key`). If you are using the tunnel certificate (for example, \* tunnel certificate), you must use all the five parameters.

- `proxy_ca_location`  
(For third-party certificates) Specifies the location of a chain file from a certificate authority (CA). The key can also refer to a directory where multiple root certificates are stored. If you provide a directory, use the hash format (for more information, see the [OpenSSL](#) documentation). For example,  
`proxy_ca_location = C:\certs\ca-chain.ec.cert.pem`  
(For tunnel certificates) Specifies the location of the \* tunnel certificate on the computer. For example,  
`proxy_ca_location = C:\Program Files (x86)\Nimsoft\hub\certs\cert02.pem`
- `proxy_cert`  
(For third-party certificates) Specifies the location of the public certificate file. For example,  
`proxy_cert = C:\certs\gk01-j05.ca.com.ec.cert.pem`  
(For tunnel certificates) Specifies the location of the \* tunnel certificate on the computer. For example,  
`proxy_cert = C:\Program Files (x86)\Nimsoft\hub\certs\cert02.pem`
- `proxy_private_key`  
(For third-party certificates) Specifies the location of the private key file. For example,  
`proxy_private_key = C:\certs\gk01-j05.ca.com.ec.key.pem`  
(For tunnel certificates) Specifies the location of the \* tunnel certificate on the computer. For example,  
`proxy_private_key = C:\Program Files (x86)\Nimsoft\hub\certs\cert02.pem`
- `proxy_private_key_password`  
(For tunnel certificates) Specifies the password that you used while creating the tunnel certificate.
- `proxy_check_ip_first`  
(For tunnel certificates) If enabled (that is, set to 1), it checks the common name in the hub certificate to find whether the IP address is used. If it matches the IP address, it proceeds. If not, it looks for the host name. If it matches with the host name, it proceeds without any issue. Otherwise, it throws an error. The default value is 1 (enabled).  
If not enabled, it looks only for the host name match.

**NOTE**

For more information, see [Linux](#) and [Windows](#) examples below.

4. Save your changes.

Review the following points:

- Avoid using spaces in directory or file names.
- The maximum length of any key-value pair in a UIM configuration file is 2047 characters. This limit includes the entire line in the configuration file:
  - Indentation spaces
  - Key name, space, equal sign, and following space
  - The value of the key
- In Linux:

- You can specify an absolute path, or a relative path from UIMHOME/robot.
- Symbolic links are supported for proxy keys.
- The key-value pair specifying an absolute or relative path can be a maximum of 2047 characters.
- In Windows:
  - You can specify an absolute path, a relative path from UIMHOME/robot, or an absolute path in long UNC format.
  - The maximum length of a path in Windows is 259 characters. The operating system converts relative paths to absolute paths. Ensure that a relative path does not expand to exceed 259 characters.
  - Windows accepts the back slash ( \ ) or the forward slash ( / ) as the path separator in relative or absolute paths.
  - To use a path longer than 259 characters in Windows, use a long UNC path.
    - Long UNC paths begin with \\?\
    - A long UNC path must be an absolute path, and must use the back slash ( \ ).
    - The key-value pair specifying a long UNC path can be a maximum of 2047 characters.

### Linux Example

In this case, UIMHOME=/opt/nimsoft and proxy certificate files are stored in /opt/nimsoft/certs .

Add the following keys to the robot.cfg file to specify relative paths:

```
proxy_ca_location=../certs/ChainFile.pem
proxy_cert=../certs/PublicKey.pem
proxy_private_key=../certs/PrivateKey.pem
```

### Windows Examples

Use an absolute local filesystem path:

```
proxy_ca_location=c:/certs/ChainFile.pem
proxy_ca_location=c:\certs\ChainFile.pem
```

Use a relative local filesystem path where certificate files are stored in C:\Program Files (X86)\Nimsoft\certs

```
proxy_ca_location=../certs/ChainFile.pem
proxy_ca_location=../certs/ChainFile.pem
```

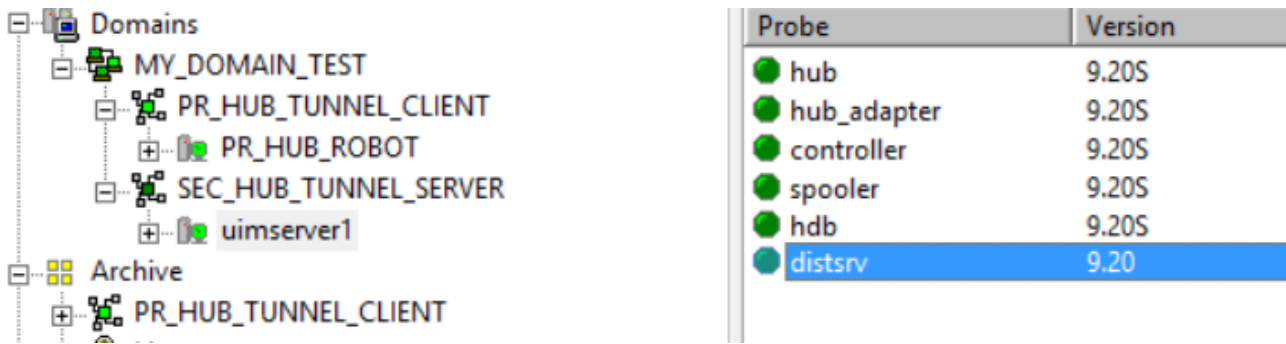
Use a long UNC path:

```
proxy_ca_location=\\?\c:\<very_long_path>\certs\ChainFile.pem
```

### **Deploy Secure Robot on Tunnel Server**

Apply the latest secure robot to the tunnel server robot. Select the required package and deploy it.

The following example screenshot shows that the secure robot has been successfully deployed from the primary hub (tunnel client) archive to the secondary hub (tunnel server in this screenshot):



**Configure robot.cfg on Tunnel Clients**

Follow the process that is explained in the [Configure robot.cfg on Tunnel Server](#) section to configure robot.cfg file on the required tunnel clients.

An example of entries for the third-party certificates is as follows:

- proxy\_ca\_location = C:\certs\ca-chain.ec.cert.pem
- proxy\_cert = C:\certs\gk01-j05.ca.com.ec.cert.pem
- proxy\_private\_key = C:\certs\gk01-j05.ca.com.ec.key.pem

An example of entries for the \* tunnel certificate on a tunnel client is as follows:

- proxy\_ca\_location = C:\Program Files (x86)\Nimsoft\hub\certs\client1.pem
- proxy\_cert = C:\Program Files (x86)\Nimsoft\hub\certs\client1.pem
- proxy\_private\_key = C:\Program Files (x86)\Nimsoft\hub\certs\client1.pem
- proxy\_private\_key\_password = +2I4kxfkvjh0loWVXAkzWx==
- proxy\_check\_ip\_first = 1

**NOTE**

In addition to securing tunnel client robots, you must also secure other independent robots pointing to the secure hub to ensure that the environment is completely secure.

**Deploy Secure Robot on Tunnel Clients**

Apply the secure robot to the tunnel client robots. Select the required package and deploy it.

The following screenshot shows that the secure robot has been successfully deployed to the tunnel client (primary hub in this screenshot):



**NOTE**

Follow the same steps to upgrade all other child robots (if any) that are connected to secure hubs.

## Verify the Setup

After you complete all the previously mentioned steps, log in to the tunnel server and tunnel client computers, using IM with the IP 127.0.0.1. Both the tunnel server and tunnel client hubs must be listed in IM in both the computers. This implies that the tunnel communication between server and client is working properly.

### For Windows

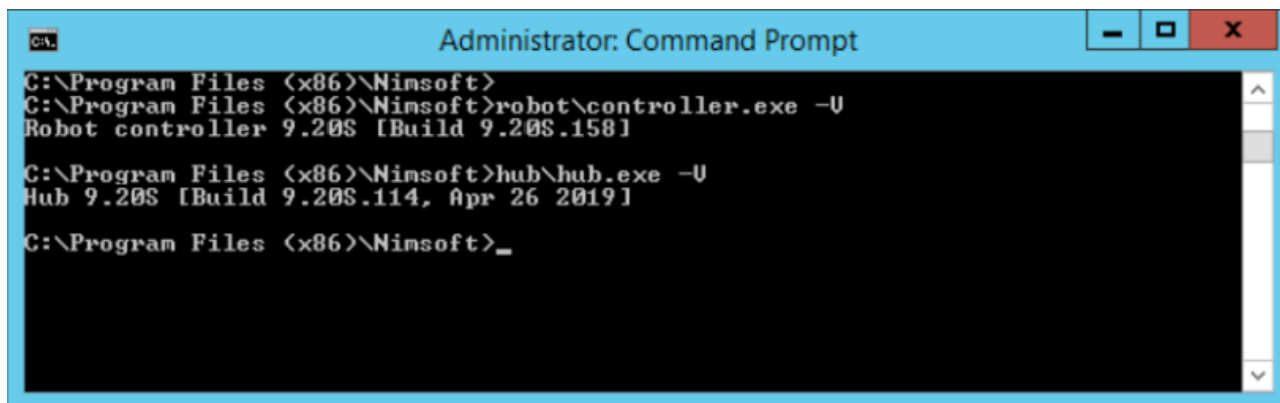
To verify that the hub upgrade is successful:

1. Log in to the Windows server hosting the hub.
2. Open a Windows command prompt, and execute  
`Drive:\YOUR_UIM_HOME_FOLDER\hub\hub.exe -V`
3. Verify the hub version that is returned.

To verify that the robot upgrade is successful:

1. Log in to the Windows server hosting the hub.
2. Open a Windows command prompt, and execute  
`Drive:\YOUR_UIM_HOME_FOLDER\robot\controller.exe -V`
3. Verify the controller version that is returned.

The following example screenshot shows the secure hub version and robot version:



```

Administrator: Command Prompt
C:\Program Files (x86)\Ninsoft>
C:\Program Files (x86)\Ninsoft>robot\controller.exe -U
Robot controller 9.20S [Build 9.20S.158]

C:\Program Files (x86)\Ninsoft>hub\hub.exe -U
Hub 9.20S [Build 9.20S.114, Apr 26 2019]

C:\Program Files (x86)\Ninsoft>_

```

### For Unix

To verify that the hub upgrade is successful:

1. Log in to the server hosting the hub.
2. At a command prompt, execute `UIMHOME/hub/hub -V`
3. Verify the hub version that is returned.

To verify that the robot upgrade is successful:

1. Log in to the server hosting the hub.
2. At a command prompt, execute `UIMHOME/robot/controller -V`
3. Verify the controller version that is returned.

## Multi-Tiered All-Linux Environment

To update a multi-tiered all-Linux environment, follow these steps:

1. You need to have at least one Windows secure hub (which is a tunnel client) in the setup.
2. Once the entire setup is secured, connect to this Windows computer.
3. Open IM in Windows computer and log in with 127.0.0.1.

4. All secure hubs are listed (all Windows and Linux).

### **Uninstall or Remove Secure Bus**

To revert your secure environment to the non-secure state, you must downgrade all the robots and hubs in your secure environment by downloading and installing an older version of the robot and hub from the archive. Based on your setup, you can downgrade robots and hubs as follows:

1. If your secure environment consists of standalone robots that are connected to a secure hub, then you must first downgrade all the standalone robots to an older version that you downloaded from the archive.
2. After you downgrade standalone robots, downgrade the robots running on secure hub to an older version that you downloaded from the archive.
3. After you downgrade all the robots, downgrade the hubs to an older version that you downloaded from the archive.

### **Additional Information**

- If your requirement is to use the UIM Server installer to convert to a secure hub and robot, follow the information in [Secure hub and robot](#).
- To review the troubleshooting information, see the [Troubleshooting Secure Hub and Robot](#) article.

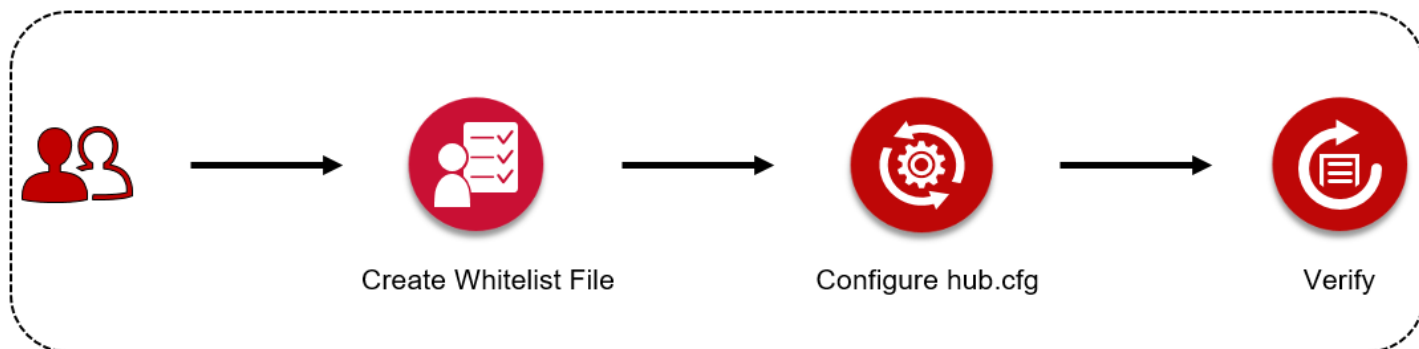
### **Secure Transmission of Certificates**

With newer security issues coming up every single day, organizations understand the importance of products having robust security mechanism. UIM 20.3.3 has further enhanced its security by enabling the seamless transfer of the certificates *from a hub to a robot* over a secure channel. Now, you no longer need to manually drag-and-drop the certificates from a hub to a robot when using the secure bus. The complete process is automatically done without any manual intervention, which ensures that the communication is secure and the data is not tampered with.

#### **NOTE**

Review the [Secure Hub and Robot](#) article that contains the complete flow of securing the environment. Secure transmission of certificates is one of the steps involved in the overall process.

The following illustration outlines the certificate transfer process:



The following topics provide the detailed information:

At a high level, you create a whitelist file that contains the target robots pointing to a specific hub. You then configure the hub.cfg file. Based on the whitelist file and hub configuration, certificates are transferred to the target robots over a secure channel. The hub reads the whitelist file after every 1 minute.



## Considerations

Review the following considerations:

- Tunnels must be configured in your environment.
- The latest version of the distsrv or ADE probe (available with UIM 20.3.3) must be deployed.
- This functionality is applicable for the robot and hub packages that are released with UIM 20.3.3.
- If a specific robot is not online, the certificate transfer does not happen on that robot.
- The certificate transfer does not work in the case of passive robots.
- Tunnel server acts as a certificate authority (CA).
- You can create a whitelist file manually or can use a callback.

## Create the Whitelist Configuration File

Create the whitelist configuration file, robots\_certs\_details.cfg, in the ..\Nimsoft\hub\changes location. In this file, you add the list of robots to which you want to transfer the certificates. The robots must point to the hub from where you want to transfer the certificates. The corresponding hub reads this file to determine the robots where it will transfer the certificates. You must add this file to all the required hubs. The hub reads the file after every 1 minute.

### NOTE

You can also use a callback to create the whitelist file. The callback creates the file, adds the robot information to it, and places it in the "changes" folder. The callback performs these tasks automatically. However, you can add only one robot entry at a time if you are using the callback. For more information, see [Use a Callback to Create Whitelist File](#).

### Follow these steps:

1. Navigate to the ..\Nimsoft\hub\ location. This is the hub from where you want to transfer the certificates to the target robots that are pointing to it.
2. Create a new folder named "changes" under the ..\Nimsoft\hub\ folder.
3. Navigate to the "changes" folder.
4. Create the robots\_certs\_details.cfg file with the following information under the "changes" folder:

```
<certs>
 <robotname>
 name=robot_name_ABC
 commonName=10.xx.xxx.xx
 expiry_in_days=6
 location=<keep_blank>
 deployed=no
 </robotname>
</certs>
```

Add the information for all the target robots.

5. Review the parameters:
  - name: Specifies the name of the robot where you want to transfer the certificates. This robot points to the same hub.
  - commonName: Specifies the IP of the target robot.
  - expiry\_in\_days: Specifies the certificate expiry. If you leave it blank, the default expiry (one year) is considered.
  - location: Specifies the location where the generated certificate file (<robot\_name>.pem) is stored. At this stage, this parameter is empty because the certificate transfer process has not started yet.
  - deployed: Specifies the status of the certificate deployment on the target robot. The default value is *no*, which implies that the deployment has not been done. Once the certificate is deployed successfully, the value is automatically changed to *yes*.
6. Save the changes.

You have successfully created the whitelist file. Follow the same process to create the files for other hubs.

### **Use a Callback to Create the Whitelist File**

If you do not want to manually create the whitelist file, you can use a callback to create it. However, you can add only one robot at a time using the callback.

#### **Follow these steps:**

1. Open the probe utility (pu) for the hub (tunnel client or tunnel server). Ensure that the robots to which you want to transfer the certificates are pointing to this hub.
2. Select the `secure_transmission_add_robot_to_certs_whitelist` callback from the drop-down list.
3. Enter the following information:
  - a. `robotName`: Specify the name of the target robot to which you want to transfer the certificate. This robot must point to the hub where you are running this callback.
  - b. `commonName`: Specify the IP address of the target robot.
  - c. `expiry_in_days`: Specify the number of days after which you want the certificate to expire. If you do not provide any value, the default expiry (1 year) is used.
4. Run the command request.

The whitelist file `robots_certs_details.cfg` is created in the `..\Nimsoft\hub\changes` folder. The following snippet shows an example of the generated file:

```
<certs>
 <robotname>
 name=robotname_ANC
 commonName=10.xx.xxx.xx
 expiry_in_days=10
 location=
 deployed=no
 </robotname>
</certs>
```

You have successfully created the whitelist file. Follow the same process to create the whitelist files for the other hubs. Note that the `deployed` value is still `no` because the transfer has not been completed. Similarly, note that the `location` field is blank because the certificate has not been transferred yet.

### **Configure the hub.cfg file**

After you create the whitelist file, you configure the `hub.cfg` file to enable the secure transmission of the certificates. You must perform this configuration for all the hubs in the domain that you want to use for transferring the certificates. Only after this configuration is done, the process to securely transfer the certificates starts.

#### **Follow these steps:**

1. Navigate to the `..\Nimsoft\hub\hub.cfg` file.
2. Open the file and add the following parameters:
  - `enable_secure_cert_transmission`: Specifies whether you want to enable the process of transferring the certificates from a hub to its robot over a secure channel. To do so, add the value as `yes`.
  - `get_all_robots_certs`: Specifies whether you want to transfer the certificates to all the robots that are pointing to the hub or only to those that are already listed in the whitelist file. The default value is `no`, which implies that the whitelist file is used for identifying the target robots. If you change the value to `yes`, then the certificate is transferred to all the robots pointing to that hub, overriding the whitelist file.
3. Save your changes.

You have successfully configured the `hub.cfg` file.

After the `hub.cfg` file is configured, the transfer process starts and performs the following tasks:

- The following files are added to the `..\Nimsoft\hub\robots_certs` folder on the hub:
  - `<robot_name>.pem`
  - `robots_certs_details.cfg`
- NOTE**

This file is created based on the whitelist file that is placed in the `..\Nimsoft\hub\changes\` folder. After the creation of this file, the whitelist file is removed from the `..\Nimsoft\hub\changes\` folder. Any modifications that are made to the `..\Nimsoft\hub\changes\robots_certs_details.cfg` file are appended to the already created `..\Nimsoft\hub\robots_certs\robots_certs_details.cfg` file.

  - `robots_certs_details.cfx`
- The following parameters are added/updated in the `..\Nimsoft\hub\robots_certs\robots_certs_details.cfg` file:
  - `password`: Specifies a randomly generated and encrypted password.
  - `location`: Specifies the location where the generated certificate file (`<robot_name>.pem`) is stored. For example, `location = robots_certs/<robot_name>.pem`.
  - `deployed`: Updates the value to `yes`.
- The certificates are transferred to the listed robots. The certificates `.pem` file is copied to the target `..\Nimsoft\robot\certs` folder:
  - `<robot_name>.pem`
- The `robot.cfg` file is updated with the location of the certificates:
  - `proxy_private_key=robot/certs/<robot_name>.pem`
  - `proxy_ca_location= robot/certs/<robot_name>.pem`
  - `proxy_cert=robot/certs/<robot_name>.pem`
  - `proxy_private_key_password=/123456ZO7/0134QVSRf4`
- The `hub.cfg` file adds a parameter `robot_certs_issuing_hub`. This parameter shows the hub that is issuing the certificates to the target robots. For example, `robot_certs_issuing_hub=/<domain_name>/<hub_name>/<robot_name>`

### **Verify the Secure Transmission of Certificates**

When the `hub.cfg` file is configured appropriately, it starts the transfer process and places the certificates in the required locations. You can verify whether the transfer happened successfully.

#### **Follow these steps:**

1. Open the `..\Nimsoft\hub\robots_certs_details.cfg` file.
2. Locate the value of the `deployed` parameter.
  - If the value is `yes`, it means that the certificates have been successfully transferred to the target robots.
  - If the value is `no`, it means that the certificates have not been deployed successfully.

You have successfully verified the status.

### **Retrieve Information from Whitelist File**

You can retrieve the information from the whitelist file. For example, you can get all the robots that are part of the whitelist file.

#### **Follow these steps:**

1. Open the probe utility (`pu`) for the hub (tunnel client or tunnel server).
2. Select the `secure_transmission_get_robot_certs_whitelist` callback from the drop-down list.
3. Run the command.

**NOTE**

If you want to get the information for a specific robot, you can enter the robot name in the field.

All the information that is included in the whitelist file is retrieved.

#### 4. Review the information.

### **Use the uimapi APIs**

You can also use the latest uimapi package that is released with UIM 20.3.3 to perform these tasks:

- Retrieve robot certificate information from the whitelist file.
- Add robot certificate information to the whitelist file.

### **Retrieve Robot Certificate Information from the Whitelist File**

You can use this procedure to get the robot certificate information from the whitelist file of a specific hub.

#### **Follow these steps:**

1. Access the uimapi.
2. Expand the hubs section.
3. Locate and expand the following endpoint:  
GET /hubs/{domain}/{hub}/{robot}/robotcertswhitelist
4. Enter the following information:
  - a. domain: Specifies the domain name.
  - b. hub: Specifies the hub that is related to the whitelist file.
  - c. robot: Specifies the name of the hub robot.
  - d. (Optional) robotname: Specifies the name of the specific robot for which you want to get the certificate information from the whitelist file.
5. Execute the API.  
The response is generated and includes the information about the robot certificates.

### **Add Robot Certificate Information to the Whitelist File**

You can use this procedure to add the robot certificate information to the whitelist file of a specific hub.

#### **Follow these steps:**

1. Access the uimapi.
2. Expand the hubs section.
3. Locate and expand the following endpoint:  
POST /hubs/{domain}/{hub}/{robot}/robotcertswhitelist
4. Enter the following information:
  - a. domain: Specifies the domain name.
  - b. hub: Specifies the hub that is related to the whitelist file.
  - c. robot: Specifies the name of the hub robot.
  - d. robotCert: Specifies the payload that contains the robotname, commonName, and expiry of certificate in days.
 

```
<RobotCert>
 <commonName>10.xx.xxx.xxx</commonName>
 <expiry_in_days>3</expiry_in_days>
 <robotName>ANC</robotName>
</RobotCert>
```
5. Execute the API.  
The response is generated and the robot certificate is added to the whitelist file. All the other remaining steps in the process are followed in the same way.

---

## Troubleshooting Secure Hub and Robot

This article includes troubleshooting topics for secure hub and robot.

### Unable to Deploy Secure Hub

#### **Symptom:**

In my environment, I have a primary hub, secondary hubs, and configured tunnels. Now, when I try to deploy a secure hub, I am unable to do so.

#### **Solution:**

You must ensure that you first upgrade your robot to 7.97 or later (non-secure) and then deploy the secure hub.

### Infrastructure Manager Not Working After Upgrading to Secure State

#### **Symptom:**

After upgrading from to the secure state, Infrastructure Manager (IM) stops working. In this case, when I try to log in to the primary hub using 127.0.0.1, no hubs or domains are listed.

#### **Solution:**

If you have a saved user profile, delete it from the `.. \Nimsoft\hub\profiles` location.

### No UI to Validate Probes in All Linux Environment

#### **Symptom:**

In an all Linux implementation, once I am on a secure hub, I do not have any GUI method to validate probes.

#### **Solution:**

To validate probes in an all Linux environment, you can use the `probe_verify` callback to validate probes. Specify the name of the probe that you want to validate and run the callback.

### Unable to Secure a Hub Due to Communication Issues Between Tunnel Server and Tunnel Client

**Symptom:** After running the UIM Server upgrade installer in the secure mode, when I try to convert my hub into a secure hub, I am facing a communication issue between the tunnel server and tunnel client. I am unable to make my hub a secure one.

**Solution:** If you face any communication issue between a tunnel server and tunnel client and unable to make your hub a secure hub, you can follow these steps:

1. Explicitly log in to the hub.
2. Download the `vs2017-vcredist_x64 1.01` (or later) and `vs2017-vcredist_x86 1.01` (or later) packages into the hub archive.
3. Download robot 7.97 (or later) into the hub archive.
4. Deploy robot 7.97 (or later) on the hub archive.
5. Manually copy `hub_adapter` and `hub_secure` into the hub.
6. Deploy `hub_adapter` and then `hub_secure` on the hub.  
When the hub becomes secure, it should be able to communicate with the other secure hubs in the domain. You can then proceed with remaining steps to deploy the certificate package and `robot_update_secure` to this hub.

### Non-Secure Robots Not Getting Disconnected After Disabling `hub_adapter`

#### **Symptom:**

After I deactivate `hub_adapter` on a secure hub, the non-secure robot pointing to that hub is not getting disconnected immediately.

**Solution:**

When you deactivate `hub_adapter` on a secure hub, the non-secure robots pointing to that hub do not get disconnected immediately. It takes more than 30 minutes for the non-secure robots to show as disconnected in the hub IM. During this time, the non-secure robots cannot process any alarms or QoS messages. The non-secure robot configuration is possible during this time.

**Discovery Wizard Not Displaying in OC After Upgrading**

**Symptom:** After upgrading to 20.3.0 (or later), when I log in to OC, the Discovery wizard is not displaying by default.

**Solution:** The display of the Discovery wizard depends on the key `needDiscovery`, which is available in the `umpsettings` table. If the value of the key is `true`, the Discovery wizard is displayed; otherwise, it is not displayed. By default, the value is set to `true`. Therefore, when you log in for the first time in OC, you see the Discovery wizard. However, if you click the close button and select the 'do not show again' option, the value of the `needDiscovery` key is set to `false`, which disables the automatic display of the wizard.

**CABI Dashboards Not Appearing in OC After Upgrade**

**Symptom:** I used the secure robot option in the 20.3.0 upgrade installer while upgrading the UIM server. After the upgrade, I upgraded CABI to 4.20. Now, I do not see the CABI dashboard in OC. How can I resolve this issue?

**Solution:** Sometimes, it is possible that you do not see the CABI dashboard (by default) in OC after upgrading CABI. If you encounter this issue, we recommend that you add the `cabi` key to the OC raw configuration for the CABI dashboard to appear in OC. The key is `cabi` and the value is `/domainname/hub/cabirobot/cabi`. Use this key-value pair only when you do not see the CABI dashboard in OC after the upgrade.

**Admin Console Inaccessible After Primary Hub Upgrade**

**Symptom:**

After I upgrade the primary hub, the UIM Server Home Page and Admin Console (AC) are inaccessible.

**Solution:**

To gain access, add the primary hub IP address to the `service_host` configuration file, `UIMHOME/probe/service/service_host/service_host.cfg`.

- Add the following entry to the `<http_connector>` section:  
`address = primary_hub_IP_address`
- If Admin Console is configured for `https`, add the entry to the `<https_connector>` section instead of the `<http_connector>` section.
- Restart the `service_host` probe for the changes to take effect.

**Communication with Infrastructure Manager and Admin Console Disrupting After Upgrade in Mixed Mode**

**Symptom:**

After I upgrade a non-secure hub to a secure hub, communication with Infrastructure Manager (IM) and Admin Console (AC) is disrupting.

**Solution:**

The `hubs.sds` file contains static route information that is used by non-secure hubs. Secure hubs do not use static routes. When a non-secure hub, which is connected to other non-secure hubs, is upgraded to secure, the static routes are

invalidated. All hub-to-hub communication occurs over tunnels that you create. If you have a domain with non-secure and secure hubs, take the following actions on each non-secure hub:

- Edit `UIMHOME/hubs/hub.cfg`. In the `<hubs>` section, add the key `broadcast_on = no`.
- Delete the `UIMHOME/hub/hubs.sds` file from non-secure hubs to remove the old static routes.
- Restart the hub.

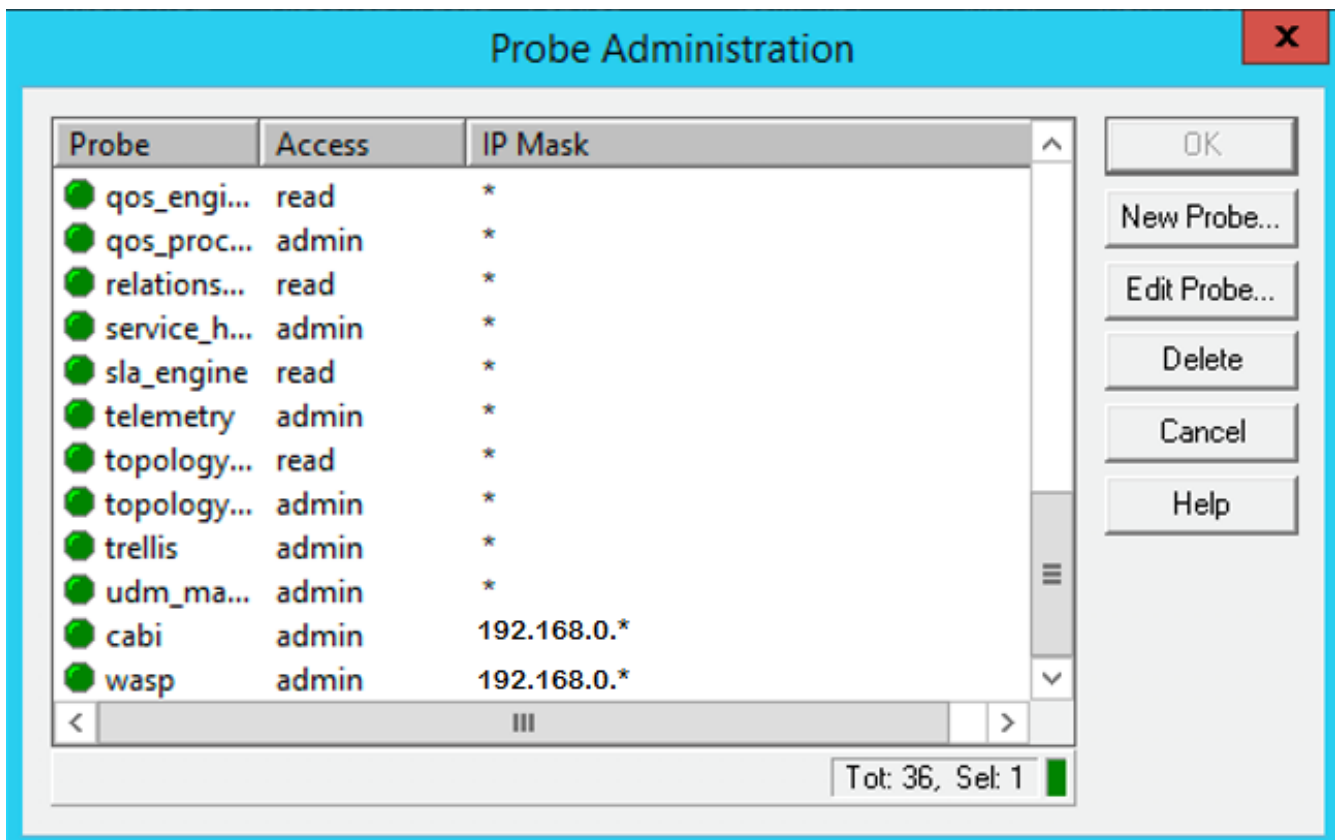
If the `hubs.sds` file is not deleted from non-secure hubs, you can experience the following problems:

- A non-secure hub can appear to be disconnected in IM or AC.
- Robots that are controlled by a non-secure hub can disappear from IM or AC.
- Robots that are controlled by a non-secure hub are listed, but AC displays the message, *No probes to display*.

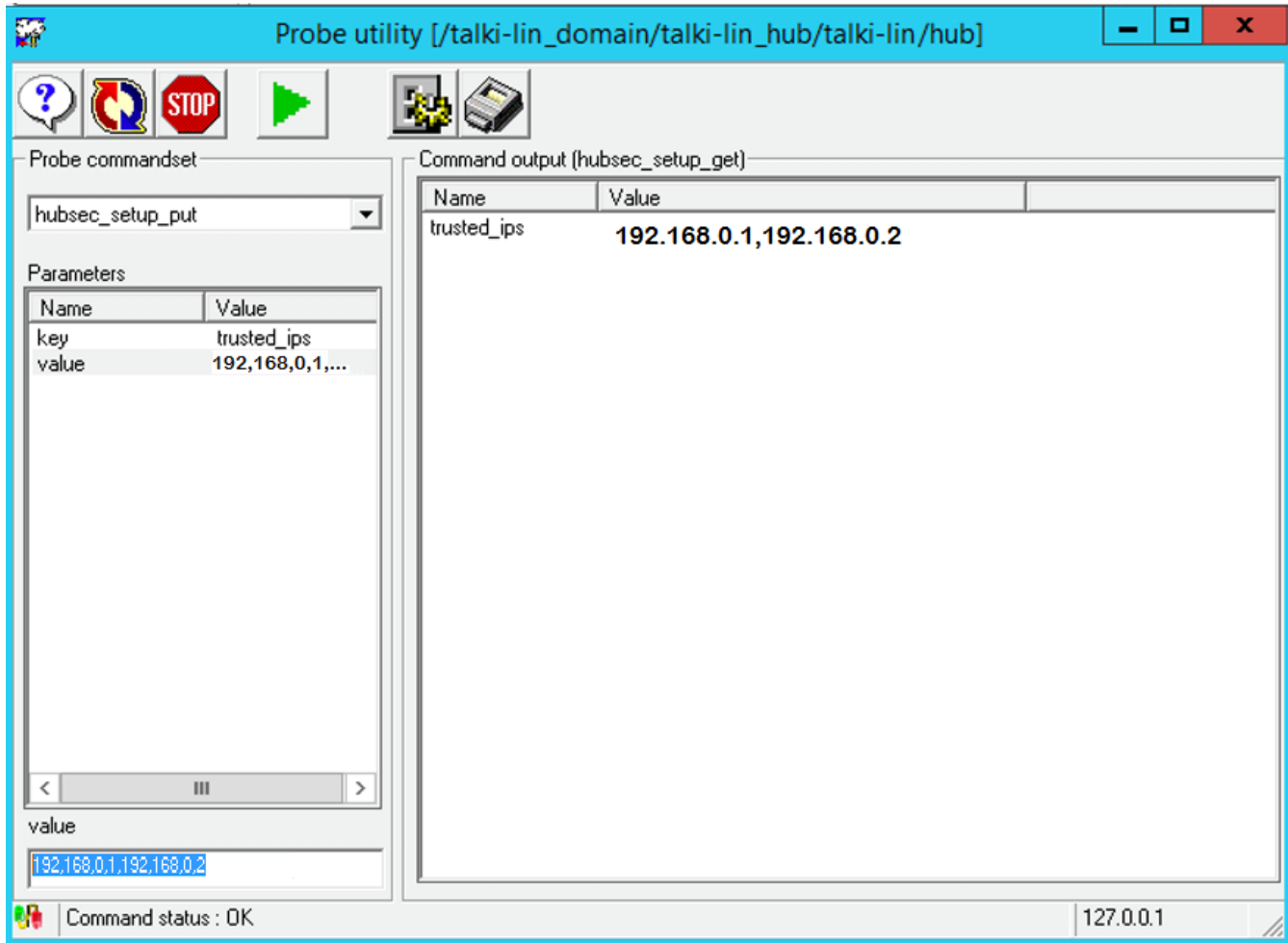
### **Enable CABI and OC to Communicate Securely from Separate Secure Robots**

To enable CABI and OC to communicate securely from separate secure robots, follow these steps:

1. Whitelist the IP subnets where OC and `cabi` are running by using the existing probe administration UI in IM. This configuration ensures that the secure bus understands that `wasp` and CABI on these subnets can be trusted by the bus.



2. Using Probe Utility, use the `hubsec_setup_put` callback on the primary hub to add the IPs of the OC robot and CABI robot as "trusted\_ips" in the `security.cfg` file of the hub. Use a comma-separated list. This configuration ensures that the secure bus understands that these are special robots, and user logins from these robots must be allowed without downgrading access.



- Restart the primary hub, restart OC, wait until OC is fully up, and then restart cabi.

### **Tunnel Communication Not Occurring Correctly**

When secure hub and robot are configured and tunnel communication is not happening properly, go to the tunnel client hub and check the tunnel status. If it is showing following errors, follow the related steps to correct the problem:

- **Invalid or missing certificate password. Reason: Failed to decrypt the certificate.**  
Verify and correct the certificate paths in `hub.cfg` and restart the tunnel client robot.
- **An application specific error.**  
Add the tunnel server and the tunnel client computer details in the `/etc/hosts` file in all the secure hubs and then restart the tunnel client robots.
- **Could not connect to hub. Please check that the server is running.**  
Follow these steps:
  - Verify whether certificate details are provided in the `hub.cfg` file.
  - Change the names for the `cert` and `password` keys.
  - Provide the valid certificate path in `hub.cfg`, save the file, and restart the robot.

### **Unable to Access a Robot Connected to a Secondary Hub**

**Symptom:**



---

After I remove hub\_adapter from the secondary hub, I cannot access the robot that is connected to the secondary hub.

**Solution:**

Secure hub does not accept communication from non-secure robots without the hub\_adapter. The hub\_adapter should not be removed until all of the robots under a secure hub have been upgraded. Otherwise, communication with the robots is lost unless the hub\_adapter is restored.

**Robot Upgrade Failing****Symptom:**

My robot upgrade installation failed. What happened?

**Solution:**

The secure bus robot installer runs a pre-installation check for safety before the installation is allowed to proceed. This checks your robot configuration and runs some communication checks to ensure that if the new robot were to be installed that it would come up successfully. If this check fails, more information can be found in robot/proxy\_check.log on the robot. Typos or incorrect formatting of the new configuration parameters is the most common cause.

**Tunnel Server Not Starting Up****Symptom:**

After you set up the secure hub tunnel, the tunnel server does not start up as it reports an inconsistency with the host name (short host name) and the host name extracted from the certificate (FQDN).

**Solution:**

Change the order of the entries in the host file to IP FQDN host name (instead of IP host name FQDN).

**Receiving SID Expired Errors****Symptom:**

The IM message window shows "SID expired" errors.

I have the following architecture: Primary hub is tunnel client to tunnel server; third-tier hub is tunnel client to the same tunnel server. From the primary hub, I am unable to expand the hub on the third-tier/client hub. If I restart that hub, it seems to start working again after a few minutes, then stops again. If I open an IM client on the tunnel server, I can successfully communicate with both its clients. Also, from the primary hub, a "transfer check" and "response check" are successful. It is only IM that is failing.

**Solution:**

To address this issue, verify that no time difference exists between the clocks on the primary and remote client.

**ACLs Not Working Correctly****Symptom:**

On a Linux primary hub, ACLs are behaving strangely, downgraded to the Operator from Administrator when the hub is being replaced with secure hub.

**Solution:**

In a secure UIM Linux environment, IM does not work. While accessing the Linux primary hub from the IM running on a Windows computer, the ACLs are downgraded from Administrator to Operator and probe deployment from Archive also fails. To resolve this issue, add the IP address of the Windows computer where IM is installed to the list of trusted IPs on the Linux primary hub.

Follow these steps:

1. Run the command: `/opt/nimsoft/bin ./pu hub -u <username> -p<password> hubsec_setup_put`
2. Create a key **trusted\_ips** and specify IP address of the Windows computer as the **value**.
3. Restart the IM.

### **OC AccountAdmin view Not Listing ACLs**

#### **Symptom:**

OC AccountAdmin view cannot list ACLs with secure bus in place. When accessing OC after applying all the patches, in the AccountAdmin view, I cannot load the ACLs. I get a "500 internal server error."

#### **Solution:**

If the OC is installed on a secure secondary robot and you are accessing the OC using browser from a different computer, you might see the "500 internal serve error" while accessing the AccountAdmin view. To resolve this issue, add the IP address of the computer that you are using to access OC to the list of trusted IPs in the primary hub.

Follow these steps:

1. Run the command from a primary hub computer:

(Windows)

```
C:/Program Files (x86)/Nimsoft/bin pu -u <username> -p <password> hubsec_setup_put
```

(Linux) `/opt/nimsoft/bin ./pu hub -u <username> -p<password> hubsec_setup_put`

2. Create a key **trusted\_ips** and specify IP address of the computer that you are using to access OC as the **value**.
3. Restart OC.

### **wasp Not Working**

#### **Symptom:**

The wasp probe does not work when the OC is installed on a robot (non-secure) pointing to a secure hub.

#### **Solution:**

For the wasp probe to work, the non-secure robot on which OC is installed must be converted to secure robot because secure hub can communicate with non-secure robots only if `hub_adapter` is deployed on the secure hub.

### **Removing hub\_adapter**

#### **Symptom:**

When should I remove the `hub_adapter` probe and what things should I verify before removing?

#### **Solution:**

You should remove the `hub_adapter` probe only when your complete environment is converted to a secure environment. However, if you have a mixed environment where you have a combination of secure and non-secure robots communicating with secure hub, then the `hub_adapter` probe should not be removed because secure hub communicates with the non-secure robots using `hub_adapter`.

## Firewall and Port Reference for Secure Setup

This article provides information on the firewall and port reference for a secure setup.

| UIM Component     | Ports               | Direction         | Firewall Rules                                          | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|---------------------|-------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Controller</b> | 48000; configurable | Inbound, outbound | Allow inbound on 48000+ for probe access on all robots. | <p>The controller listening port. In a Secure Setup it accepts only SSL traffic.</p> <p>For an enterprise, enable communication both ways on port 48000 through a firewall. Communication both ways allows UIM to contact and control hubs, robots, and probes. This port also receives status from BUS components.</p> <p>The hub spooler and the spooler for robots transmit alarm and QoS data. A port must be set in the controller configuration for Infrastructure Manager (IM) and Admin Console to connect to remote tunnels through the tunnel server and client IPs: for example, 192.168.1.10:50003.</p> <p>For tunnel hubs, set the <b>First Probe port number</b> in Setup &gt; Advanced for the controller to 50000 or higher. If necessary, open the same port and higher in the firewall.</p> <p><b>Note:</b> You only need ports 48000 for the controller and 48002 for the hub open between the primary hub and the OC hub. You don't need these ports open between every hub in the domain and the OC server as the hub controllers will talk to the primary hub controller.</p> |

|                           |                                                                                    |                          |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------|--------------------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Hub_adapter</b></p> | <p>48001, 48002, opens the highest port available within the 48000-49000 range</p> | <p>Inbound, outbound</p> |  | <p>In case of non-secure robots, this component needs to be available for communication with a secure hub.</p> <ul style="list-style-type: none"> <li>• Hub_adapter creates a listening port for each connected hub.</li> <li>• You might need to relax the firewall rules to support the communication.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p><b>Tunnels</b></p>     | <p>48003 or 443; configurable</p>                                                  |                          |  | <p>Tunnel clients do not need any port.</p> <p>Tunnels using tunnel-server-to-tunnel-clients model or tunnel-client-to-tunnel-servers need port 48003, 443, or another configured port for incoming traffic. For example, a port must be open for the enterprise data center and MSP firewall.</p> <p><b>Note:</b> Port 443 is the default port for <b>https</b> but can be used for other purposes.</p> <p>Multi-hub infrastructures can use a tunnel with or without SSL. For tunnels that are NOT SSL tunnels, ports use the same assignment as for single-hub installations.</p> <p><b>Note:</b> You only need ports 48000 for the controller and 48002 for the hub open between the primary hub and the OC hub. You don't need these ports open between every hub in the domain and the OC server as the hub controllers will talk to the primary hub controller.</p> |

|                        |                                                                                                                    |                      |                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secure hub</b>      | 48003; configurable                                                                                                | Inbound,<br>Outbound | Allow inbound, outbound through a firewall. | <p>Secure bus needs SSL tunnels between the hubs so that it matches the earlier SSL tunnel communication.</p> <ul style="list-style-type: none"> <li>• The controller port must be set to 48000.</li> <li>• If applicable, the hub_adapter port must be set to 48002.</li> <li>• The wasp probe must be set to port 80 to access Admin Console and the UIM web page.</li> </ul> <p>All other UIM ports, other than the configured SSL tunnel port, must be blocked.</p> |
| <b>Discovery_agent</b> | DNS - port 53<br>NetBIOS - port 137<br>SSH - port 22<br>SNMP - port 161; configurable<br>WMI - port 135 and others | Outbound             | Allow outbound on ports for the protocol    | Discovery_agent makes calls, as a client, to the services hosted on target machines.                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Probes</b>          |                                                                                                                    |                      |                                             | Probes in a Secure Setup are listening only on local address. No port needs to be specifically opened for the external traffic. All the data proxies through controller.                                                                                                                                                                                                                                                                                                |

|                            |                                                                                                                                   |                |                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>UIM database</b></p> | <p>1433 (Microsoft SQL Server); configurable<br/>         1521 (Oracle); configurable<br/>         3306 (MySQL); configurable</p> | <p>Inbound</p> | <p>Allow inbound for database.</p> | <p>The primary hub (data_engine) to UIM database is preferably local/on the same subnet as UIM. If the database for the primary hub is behind an internal firewall, then the appropriate port has to be open from the UIM server to the UIM database, outbound from hub server, and inbound on the UIM database server. Responses from the database server to the primary hub come back over the same connection/port.</p> <p><b>Tip:</b> Port information for your UIM database is located in the <b>Database Configuration</b> section of the data_engine probe GUI.</p> |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                           |                           |                 |                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|---------------------------|-----------------|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>ADE</b></p>         | <p>22</p>                 | <p>Outbound</p> |                                               | <p>The automated_deployment engine probe uses port <b>22</b> to deploy robots using SSH file transfer to the target system. If you cannot open port 22 on the primary hub:</p> <ul style="list-style-type: none"> <li>• a. Deploy the automated_deployment_eng a secondary hub where port 22 is not blocked.</li> <li>b. Log in to Infrastructure Manager directly from the secondary hub.</li> <li>c. Drag and drop the robot packages that you want to deploy into the archive on the secondary hub.</li> <li>d. Deploy the robots to the secondary hub through an XML file. For more information, see the topic <a href="#">Bulk Robot Deployment with an XML File</a>.</li> </ul> |
| <p><b>udm_manager</b></p> | <p>4334; configurable</p> | <p>Inbound</p>  | <p>Allow inbound on 4334 for UDM Manager.</p> | <p>UDM clients (Datomic peer), including OC, Trellis, and the Discovery Server, must connect to the SQL database and also to UDM Manager on this port.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                              |                                                                |                   |                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|----------------------------------------------------------------|-------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OC server</b>             | 8080, 80, or 443;<br>configurable range: 1–65535               | Inbound, outbound | Allow inbound on 8080, 80, or 443 on OC server.      | The port assignment for the OC server can vary by client/browser to OC and depends on your choice during the OC installation.<br>If you are using a configuration with multiple OC servers, the servers communicate through multicasting on the following IP address and ports: <ul style="list-style-type: none"> <li>IP addresses <b>239.255.0.1</b> through <b>239.255.0.5</b></li> <li>Ports <b>23301</b> through <b>23305</b></li> </ul> |
| <b>OC (Tomcat connector)</b> | 8009                                                           | Inbound, outbound | Allow inbound on 8009 on OC server.                  | The OC portal engine. Allow inbound on port 8009 from the UIM server to the OC instance (wasp probe).                                                                                                                                                                                                                                                                                                                                         |
| <b>OC database</b>           | 1433 (Microsoft SQL Server);<br>1521 (Oracle);<br>3306 (MySQL) | Inbound           | Allow inbound on respective port to Database server. | Inbound from OC to the chosen database.<br>The wasp probe requires a connection to the UIM database. Ensure that the database ports between the OC and database servers are open.                                                                                                                                                                                                                                                             |
| <b>UIM Server home page</b>  | 80; configurable                                               | Inbound           | Allow inbound to port 80 (internal enterprise).      | The UIM Server home page is typically internal-access only. Open the port in the firewall for any systems that must be able to contact the primary hub to run applications or download and install the client software.                                                                                                                                                                                                                       |
| <b>SMTP</b>                  | 25; configurable                                               | Outbound          | Allow outbound                                       | Report Scheduler creates output in PDF and CSV that is transmitted via email to users. Email transmission requires a designated server with this SMTP port open.                                                                                                                                                                                                                                                                              |
| <b>SNMP</b>                  | 161; configurable                                              |                   |                                                      | SNMP is an internet-standard protocol for managing devices on IP networks. The snmpcollector probe uses port <b>161</b> by default to communicate with the SNMP port on a device.                                                                                                                                                                                                                                                             |



|                                                |                                     |                   |                                                      |                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------|-------------------------------------|-------------------|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hub to LDAP/AD server</b>                   | 389, 686; configurable              | Outbound          | Allow outbound to LDAP/AD server.                    | Allow outbound to any custom port set in wasp probe configuration.                                                                                                                                                                                                                                                                                                        |
| <b>Web clients, browsers to OC, OC clients</b> | 80, 443; configurable               | N/A               | Allow inbound on port 80 or 443.                     | Portal access over the Internet.                                                                                                                                                                                                                                                                                                                                          |
| <b>Admin Console</b>                           | 80, 443; configurable<br>wasp probe | Inbound           | Allow inbound on port 80 or 443 on primary hub.      | Admin Console is hosted on the primary hub with <code>service_host</code> . <ul style="list-style-type: none"> <li>80 is the default port to access Admin Console and UIM web page through HTTP.</li> <li>443 is the default port to access Admin Console and UIM web page through HTTPS.</li> </ul>                                                                      |
| <b>CABI Server, UIM database</b>               | 1433, 1521 or 3306                  | Inbound           | Allow inbound on respective port to database server. | Inbound from CABI to the chosen database.                                                                                                                                                                                                                                                                                                                                 |
| <b>CABI Server, OC</b>                         | 80 or 443; configurable             | Inbound, outbound | Allow inbound on 80 or 443 to OC and CABI Server.    | This connection provides browser and customer client connectivity to CABI and OC. Port 80 by default, or port 443 or another configured port for HTTPS. The port can vary from client/browser to CABI and OC. The value depends on your choice during the CABI and OC installation. For example, port 80 or port 443. The configurable range of ports is 1 through 65535. |

## Convert Files to PEM Format

While using third-party certificate files, ensure that the files are of .pem format. If not, follow the information in this section to convert them.

### Convert RSA Key File to PEM Format

Use the following command to convert an RSA key file to a .pem format file:

- **Syntax:** `openssl rsa -in <path-to-key-file> -text <path-to-PEM-file>`
- **Example:** `openssl rsa -in C:\Certificates\serverKeyFile.key -text > serverKeyFileInPemFormat.pem`

### Convert CER File to PEM Format

Use the following command to view the .cer file:

- **Syntax:** `openssl x509 -in <path-to-cer-file> -text -noout`
- **Example:** `openssl x509 -in C:\Certificates\AnyCert.cer -text -noout`

If you receive the following error, it implies that it is a DER-encoded .cer file. Then, follow the Convert DER-Encoded .cer File section to convert a DER-encoded .cer file:

```
unable to load certificate 12626:error:0906D06C:PEM routines:PEM_read_bio:no start
line:pem_lib.c:647:Expecting: TRUSTED CERTIFICATE
```

### **Convert DER-Encoded CER File**

Use the following commands to convert a DER-encoded .cer file to a .pem format:

- **Syntax:** `openssl x509 -inform DER -in <path-to-cer-file> -out <path-to-crt-file> openssl x509 -in <path-to-crt-file> -out <path-to-pem-file> -outform PEM`
- **Example:** `openssl x509 -inform DER -in C:\Certificates\AnyCert.cer -out C:\Certificates\AnyCertCrt.crt openssl x509 -in C:\Certificates\AnyCertCrt.crt -out C:\Certificates\AnyCertInPem.pem -outform PEM`

### **Convert a base64-Encoded CER File**

Use the following command to convert a base64-encoded .cer file to a .pem format file:

- **Syntax:** `openssl x509 -in <path-to-cer-file> -outform pem -out <path-to-pem-file>`
- **Example:** `openssl x509 -in C:\Certificates\AnyCert.cer -outform pem -out C:\Certificates\AnyCertInPem.pem`

## **(Optional) Upgrade the Infrastructure Manager**

In this article, learn how to upgrade the Infrastructure Manager by downloading and running the latest version of the Infrastructure Manager installer.

For upgrade scenarios, you need to reinstall Infrastructure Manager post the UIM Server upgrade. If your primary hub server is a Windows system, CA recommends you install it there. It also can be installed on another Windows system in your environment, and from there you can use it to manage your domain.

### **WARNING**

Infrastructure Manager requires the vs2017\_vcrist\_x64 Package.

### **Follow these steps**

1. From the system where you want to install Infrastructure Manager, browse to your UIM Server web page ([http://<servername\\_or\\_IP\\_address>:80](http://<servername_or_IP_address>:80)).
2. Click the **Installers** tab. Under **UIM Server Administration**, click **Infrastructure Manager** to download the installer file.
3. Run the installer, following the prompts to complete the installation.

### **NOTE**

If you have installed UMP, port 80 has been assigned to wasp by default. To access the UIM Server page, browse to [http://<servername\\_or\\_IP\\_address>/uimhome/](http://<servername_or_IP_address>/uimhome/) to begin the installation.

[Next Step: Upgrade the Hubs >](#)

## Upgrade the Hubs

In this article, learn how to upgrade the hubs. We recommend that you upgrade your secondary hubs to the version that is installed on your primary hub.

### Considerations


Review the following considerations:

- The contents of the hub configuration file (hub.cfg) are retained during the upgrade. When a hub is upgraded, other packages are not affected.
- From UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with the latest UIM to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required). We recommend taking a backup of the existing licenses before upgrading to UIM 20.3.0.
- The robot version must always be higher than or equal to the hub version. Also, ensure that the required versions of java\_jre, robot\_update, and attr\_publisher are already deployed on the secondary hub robots.
- UIM uses OpenJDK instead of Oracle JDK. For more information about the OpenJDK usage in UIM, see [Adopting OpenJDK](#).
- For more information about upgrading to secure hubs (hub\_secure), see [Secure Hub and Robot](#).

### Upgrade a Hub Using the Admin Console

You can deploy a package from the local archive of any hub that has the automated\_deployment\_engine probe to any robot in your infrastructure.

#### Follow these steps:

1. Log in to Admin Console.
2. Select a hub, and then select the **Archive** tab.  
Columns in the archive will display the local archive version of the hub currently installed and the version available from the web, if a newer one exists. You can have more than one version of a probe in the archive, and deploy any of the versions to the hub or to another robot.
3. If a newer version of a probe in the local archive exists in the web archive, an update link will appear in the local archive column. Click on this link and enter valid credentials to download the newer package. A verification dialog box appears to verify the update.
4. Select the check box next to the hub name and then select the vertical dots icon  

  
or the **Actions** menu and the **Deploy** option.
5. In the dialog box, select a hub for deployment.
6. Click the **Deploy** button.

The page redirects to the **Deployment Activity** tab where you can monitor the deployment progress.

### Verify a Hub Package is Deployed in Admin Console

After a package has been deployed to a robot, if the package is a probe, it is displayed in both the **Installed Packages** tab and the **Probes** tab. If the package is not a probe, it is only displayed in the **Installed Packages** tab.

#### Follow these steps:

1. Select the hub.
2. Select the **Installed Packages** tab.

You can also select the robot for the hub, click on the Installed Packages tab, and view all installed packages, including the new hub.

### **Upgrade the Hubs Using the Infrastructure Manager**

You can deploy a package from the local archive of any hub that has the `automated_deployment_engine` probe to any robot in your infrastructure.

#### **Follow these steps:**

1. Launch Infrastructure Manger on your upgraded primary hub (or another hub with an updated archive).
2. Locate the **hub** probe in the **Archive**.
3. Drag-and-drop the probe onto the icon of the hub that you want to update.

[Next Step: Upgrade the Robots >](#)

## **Upgrade the Robots**

In this article, learn how to upgrade the robots in your domain, including the robots on secondary hubs.

### **WARNING**

UIM does not support the use of native installers to perform robot upgrades. To upgrade your robots, you must use the **robot\_update** package that is available in either the Admin Console or Infrastructure Manager Archive.

For first-time robot installations, the native robot installers are still supported.

### **NOTE**

- For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.
- For more information about upgrading to secure robots, see [Secure Hub and Robot](#).
- Do not include the source robot (where `distsrv/ade` is running) in the list while applying the bulk `robot_update`.
- From UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and `distsrv` versions released with the latest UIM to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required). We recommend taking a backup of the existing licenses before upgrading to the latest UIM version.
- `distsrv 9.31` has a dependency on `robot 9.31/9.31S`.
- UIM uses OpenJDK instead of Oracle JDK. For more information about the OpenJDK usage in UIM, see [Adopting OpenJDK](#).

### **Upgrade the Robots Using the Admin Console**

Deploy the **robot\_update** package to the robot you want to update.

### **Upgrade the Robots Using the Infrastructure Manager**

#### **Follow these steps:**

1. Launch Infrastructure Manger on your upgraded primary hub (or another hub with an updated archive).
2. Locate the **robot\_update** package in the **Archive**.
3. Drag-and-drop the package onto the icon of the robot you want to update.

[Next Step: Configure robot.cfg >](#)

## Configure robot.cfg

The UIM Server installer creates a .pem file (certificate.pem) in the <Nimsoft>\security folder. The .pem file is a symmetric key that is shared with the required robots, which is then used for communication with the data\_engine probe. You copy this .pem file to the remote OC, UR, and CABI robots and provide the location of the file in the robot.cfg file (cryptkey = <.pem file location>). Furthermore, if any impacted probe is not on the same computer where data\_engine is present, copy the generated .pem file to the robot computer (where data\_engine is not available) and update the robot.cfg file with the .pem file location on that computer.

To configure the robot.cfg file, follow these steps:

1. Navigate to the <Nimsoft>\robot folder.
2. Open the robot.cfg file in a text editor.
3. Add the following parameter to the file:  

```
cryptkey = <location of the .pem file>
```

 For example, cryptkey = c:\Certificate\certificate.pem
4. Save your changes.  
**Note:** You do not need to restart the robot.

You have successfully configured the robot.cfg file.

### Create a .pem File

Though the UIM Server installer automatically generates a .pem file (certificate.pem) in the <Nimsoft>\security folder, you can generate your own .pem file, if you want. You then need to copy the same .pem file to all the required places (UMP robot, UR robot, CABI robot) and configure the robot.cfg file as explained. You can use [OpenSSL](#) to create a .pem file.

**Note:** data\_engine does not consider the .pem file expiry though the automatically generated .pem file has a validity of 365 days. However, as a best practice, we recommend that you keep regenerating your .pem file based on your security requirements.

### Follow these steps:

1. For Windows, you can download OpenSSL from <http://gnuwin32.sourceforge.net/packages/openssl.htm>. Then, create a new system environment variable OPENSSL\_CONF with the value C:\Program Files (x86)\GnuWin32\share\openssl.cnf. For Linux, use appropriate package manager to install OpenSSL.
2. Open the command prompt and navigate to the location where the OpenSSL executable file is available.
3. Run the following command:  

```
openssl req -nodes -new -x509 -days <number of days the certificate is valid for> -out <certificate_filename>.pem
```

**Note:** Ensure that your certificate filename does not include spaces.
4. Enter the following information when prompted:
  - Country Name (2 letter code) [AU]:
  - State or Province Name (full name) [Some-State]:
  - Locality Name (eg, city) []:
  - Organization Name (eg, company) [Internet Widgits Pty Ltd]:
  - Organizational Unit Name (eg, section) []:
  - Common Name (e.g. server FQDN or YOUR name) []:
  - Email Address []:
 The .pem file is generated in the same location where the OpenSSL executable is available.
5. Copy the .pem file to the location that is accessible only to the appropriate users in your environment. You provide this location while configuring the robot.cfg file.

[Next Step: Upgrade UMP >](#)

## Upgrade Operator Console

In this article, learn how to upgrade UMP/OC to Operator Console. You prepare for the upgrade, run the upgrade, and complete post-upgrade tasks.

### NOTE

- To upgrade from a previous version of OC to OC 20.3.3, use the OC 20.3.3 upgrade installer that is available as part of the UIM 20.3.3 release. For more information about the UIM 20.3.3 release, see the [UIM 20.3.3](#) article.
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.
- To upgrade from a previous version of OC to OC 20.3.2, use the OC 20.3.2 upgrade installer that is available as part of the OC 20.3.2 patch release. For more information about the OC 20.3.2 patch, see the [OC 20.3.2 Patch](#) article.
- To upgrade from OC 20.3.0 to OC 20.3.1, use the upgrade installer for Operator Console that the UIM 20.3.1 patch contains. Note that UIM 20.3.1 is a patch release over UIM 20.3.0. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes the OC upgrade installer along with the separate standalone artifacts that you can use to upgrade the respective components to 20.3.1. For more information about the artifacts that are available as part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.
- In UIM 20.3.0, use the OC installer to upgrade UMP, as UMP is no longer available in UIM 20.3.0. The OC installer uninstalls the deprecated components and upgrades the valid components.
- Note that the "Upgrade Operator Console" and "[Upgrade a Multiple OC Configuration](#)" are two separate procedures. Based on your setup, you can follow the appropriate procedure.
- The wasp probe is installed as a core probe with OC to manage network communications. Do not attempt UMP/OC upgrades or downgrades by redeploying the wasp probe without running the OC installer.
- While upgrading to 20.3.0, if the OC installer is trying to install OC on the primary hub instead of the UMP server, follow the information in the [Troubleshooting Operator Console](#) article.

### Prepare for the Upgrade

Verify that you are prepared to upgrade UMP/OC to OC by completing all tasks in the following table. Do not continue with the upgrade until all these tasks are complete.

| Task                      | Description and Steps                                                                                                                                                                                                                                                     |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verify your upgrade path. | Ensure that you follow a supported upgrade path.<br>View the <a href="#">Compatibility Matrix</a> and review the Supported Upgrade Paths section.                                                                                                                         |
| Back up the system.       | After the upgrade, the only way to revert to your previous system is to restore a backup.<br><br>If you cancel the installation during the upgrade due to errors, your current system can no longer be operational. In this case, the only option is to restore a backup. |

|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Back up any customized files in the ROOT Webapp directory</p>     | <p>During the upgrade, the directory <code>&lt;UMP/OC_installation&gt;/Nimsoft/probes/service/wasp/webapps/ROOT/</code> is overwritten. If you have customized any of the files in this directory, back them up before upgrading. The following list includes some commonly customized files:</p> <ul style="list-style-type: none"> <li>• portal-ext.properties</li> <li>• web.xml</li> </ul> <p>Both of these files are modified as part of multi-UMP or HTTPs configuration.</p> <p>In UIM 20.3.0, portal-ext.properties file is replaced with config.properties. You can replace the content of config.properties with content of portal-ext.properties in the <code>&lt;UMP/OC_installation&gt;/Nimsoft/probes/service/wasp/config/</code> folder when the upgrade is complete.</p> <p>You can add the changes in your web.xml file to web.xml in the <code>&lt;UMP/OC_installation&gt;/Nimsoft/probes/service/wasp/webapps/ROOT/</code> folder when the upgrade is complete.</p> |
| <p>(Oracle only) Disable the Oracle recycle bin</p>                  | <p>If you are installing UIM for the first time, or upgrading from a previous version, the recycle bin must be disabled before you install or upgrade UIM and OC.</p> <p><b>Follow these steps:</b></p> <ol style="list-style-type: none"> <li>1. Use a tool such as SQL Developer to connect to the Oracle database.</li> <li>2. Enter the following commands: <pre>ALTER SYSTEM SET recyclebin = OFF DEFERRED; ALTER SESSION SET recyclebin = off;</pre> </li> <li>3. Verify that the recycle bin is disabled using the following command: <pre>show parameter recyclebin;</pre> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                         |
| <p>(SAML SSO configurations only) Back up the SAML configuration</p> | <p>If you are using SAML single sign-on, follow the instructions for backing up your SAML Configuration in the article <a href="#">Configure UMP to Use SAML Single Sign-On</a>. Upgrading UMP/OC to OC does not preserve the SAML configuration files.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <p>Configure robot.cfg</p>                                           | <p>The UIM Server installer creates a .pem file (certificate.pem) in the <code>&lt;Nimsoft&gt;\security</code> folder. The .pem file is a symmetric key that is shared with the required robots, which is then used for communication with the data_engine probe. You copy this .pem file to the remote UMP/OC and CABI robots and provide the location of the file in the robot.cfg file (<code>cryptkey = &lt;.pem file location&gt;</code>). Furthermore, if any <a href="#">impacted probe</a> is not on the same computer where data_engine is present, copy the generated .pem file to the robot computer (where data_engine is not available) and update the robot.cfg file with the .pem file location on that computer. For more information about the robot.cfg file configuration, see <a href="#">Configure the robot.cfg File</a>.</p>                                                                                                                                    |

|                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upgrading in Secure Setup                                                     | In an upgrade scenario, if you are upgrading UMP/OC to OC in a secure setup, ensure that you bring your UMP/OC robot to the secure state by deploying the appropriate certificates and then updating the robot version to the secure one. After that, you upgrade UMP/OC. For more information about the secure setup and how to deploy certificates, see <a href="#">Secure Hub and Robot</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Consideration if mon_config_service_ws on UIM Server and UMP on another robot | <p>If the mon_config_service_ws package is installed on the UIM Server and UMP is installed on another robot, review the following points while performing the upgrade:</p> <p><b>Scenario 1:</b> Before you upgrade the existing UIM Server to 20.3.0:</p> <ol style="list-style-type: none"> <li>1. Take a backup of the wasp folder available on the existing UIM Server.</li> <li>2. Delete the wasp probe from the existing UIM Server.</li> <li>3. Start the process to upgrade the existing UIM Server to 20.3.0 (UIM Server).</li> </ol> <p>After you complete the UIM Server upgrade, you can now upgrade 9.0.2/9.2.0 UMP to 20.3.0 OC. Without performing these steps, if you try to upgrade UMP to 20.3.0 OC, you will face issues.</p> <p><b>Scenario 2:</b> If you do not delete the wasp probe before upgrading the UIM Server to 20.3.0:</p> <ol style="list-style-type: none"> <li>1. Take a backup of the wasp folder available on the upgraded UIM Server.</li> <li>2. Delete the wasp probe from the upgraded UIM Server.</li> <li>3. Upgrade existing UMP to 20.3.0 OC.</li> <li>4. Deploy wasp that is available with 20.3.0 on the upgraded UIM Server.</li> <li>5. Deploy the adminconsole, mps, and telemetry packages that are available with 20.3.0.</li> </ol> <p>Without performing these steps, if you try to upgrade UMP to 20.3.0 OC, you will face issues.</p> |
| OpenJDK in UIM                                                                | UIM 9.2.0 has adopted Open JDK (JRE), replacing Oracle JDK. Therefore, when you upgrade UMP to OC, the upgrade process places OpenJDK onto the OC computer. However, unless you restart the OC robot, the new OpenJDK will not be picked up. This is an additional step that you need to perform after you upgrade UMP to OC. For more information about the OpenJDK usage in UIM, see <a href="#">Adopting OpenJDK</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Run the Upgrade

You upgrade UMP/OC to OC by following the same process as the installation of a new instance of OC. Follow the supported upgrade path that is described in the [Supported Upgrade Paths](#). The **Select Robot** panel of the installer provides the option to Upgrade to OC <x.x.x.x.>. The installer retains any settings, such as port numbers, that you changed from the default.

For 20.3.3, a new option **Specify IP** is also available in the **Select Robot** dialog. This option is in addition to the already existing **Choose** option. You can select the **Specify IP** option and directly enter the IP address of the robot where you want to upgrade the OC. The installer identifies that an older version of the OC is already available on the robot and prompts a message stating that you are going to upgrade the OC instance. You can then proceed with the remaining steps to upgrade the instance. For more information about the steps, see [Install Operator Console \(OC\)](#).



## **Operator Console Installer - Webapps Considerations**

After the upgrade, the webapps that are deployed/upgraded with the OC installer need to be verified and few webapps need to be manually upgraded.

The following gives more details about the webapps being installed as part of the OC installation, obsolete webapps in UIM, and the webapps that need to be manually upgraded after running the upgrade.

### **Deployed/Upgraded Webapps**

The following webapps are deployed/upgraded with the OC 20.3.0 (or later) installer:

- accountadmin
- policy\_management\_ws
- dashboard
- operatorconsole\_portlet
- mcs-ui-app
- cabi
- alarmviewer\_api
- reportscheduler (uim\_reportscheduler 20.3.3)
- slm
- samlssso
- nisapi

### **Obsolete Webapps from UIM OC WASP**

The following webapps are obsolete from UIM 20.3.0 (or later) OC WASP.

- cloudmonitor
- listdesigner
- listviewer
- mobile
- mytickets
- policyeditor
- qoschart
- relationshipviewer
- reports
- reportscheduler (UMP reportscheduler)
- servicedesk
- slareports
- unifiedreports
- usm
- saml-portlet
- ump-theme
- portal-compat-hook
- ump-read-only-theme

#### **NOTE**

If there are any undeleted folders of these webapps after the upgrade due to remote OC installation from Primary hub, users can manually delete post installation of OC.

### **Webapps to be manually upgraded**

The following webapps are required to be manually upgraded post installation of OC 20.3.0 (or later). Users are notified during OC installation if any earlier versions of these webapps exist.

- self\_cert/ump\_selfcert
- uimapi
- webservices\_rest
- ecometer\_admin (dcimadmin)
- ecometer\_admin

### **Complete Post-Upgrade Tasks**

Complete the following tasks after the upgrade is complete:

#### **Clear Your Web Browser**

If you upgraded from a previous UMP/OC version to OC, clear your browser completely to remove older versions of components that might be cached.

#### **NOTE**

For OC 20.3.2 or later, you do not need to perform this procedure if you are upgrading from an older version of OC to OC 20.3.2 or later.

#### **Follow these steps:**

1. Log out from OC.
2. Clear the browser cookies and cache.
3. Exit all browser windows.
4. Log in to OC.

#### **NOTE**

Custom ACLs with any new permissions added to the default administrator, would not be auto-selected for the custom ACLs after the upgrade. Those permissions must be selected manually for the custom ACLs after the upgrade.

### **(SAML SSO Configurations Only) Move xercesImpl.jar**

If you have configured UMP to use SAML Single Sign On in a release before 8.31, move or delete the **xercesImpl.jar** file from the directory `<UMP_installation>\probes\service\wasp\webapps\ROOT\WEB-INF\lib`. If you do not move xercesImpl.jar, you will receive the error "Unable to process SAML request" when you attempt to log in to OC after your upgrade.

### **Troubleshooting**

The wasp does not start after upgrading the Operator Console

**Symptom:** After upgrading the Operator Console using the OC Installer in UIM 20.3.0, wasp does not start.

**Solution:** After upgrading the Operator Console using the OC Installer in UIM 20.3.0, wasp does not start. This issue might be due to some obsolete webapps not removed from the OC wasp while installation. The leftover webapps must be manually removed to resolve the issue.

#### **Follow the below steps to clean up the obsolete webapps:**

Check for the obsolete webapps in the OC wasp webapps folder.

- Remove the obsolete webapps sections from wasp.cfg of the OC server. This removal can be done in two ways:
  - a. Open the wasp.cfg in Raw Configure and delete the listed webapps sections under the webapps folder using the Delete Section option.
  - b. Open the wasp.cfg in Edit mode and remove the sections under the webapps.
- Deactivate the wasp.
- Delete these webapps folders from \Nimsoft\probes\service\wasp\webapps.
- Delete the .war files of these webapps from \Nimsoft\probes\service\wasp\webapps.
- Restart the wasp.

**TIP**

We recommend moving the xercesImpl.jar into your root UIM install directory (Nimsoft).

[Next Step: Upgrade CA Business Intelligence with UIM >](#)

## Upgrade a Multiple OC Configuration

In this article, learn how to upgrade a multiple OC configuration. You run the upgrade and complete post-upgrade tasks.

**NOTE**

- Note that the "[Upgrade Operator Console](#)" and "Upgrade a Multiple OC Configuration" are two separate procedures. Based on your setup, you can follow the appropriate procedure.
- To upgrade from a previous version of OC to OC 20.3.3, use the OC 20.3.3 upgrade installer available with the UIM 20.3.3 upgrade release. For more information about UIM 20.3.3, see the [UIM 20.3.3](#) article.
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.
- To upgrade from a previous version of OC to OC 20.3.2, use the OC 20.3.2 upgrade installer available with the OC 20.3.2 patch release. For more information about the OC 20.3.2 patch, see the [OC 20.3.2 Patch](#) article.
- To upgrade from OC 20.3.0 to OC 20.3.1, use the upgrade installer for Operator Console that the UIM 20.3.1 patch contains. Note that UIM 20.3.1 is a patch release over UIM 20.3.0. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes the OC upgrade installer along with the separate standalone artifacts that you can use to upgrade the respective components to 20.3.1. For more information about the artifacts that are available as part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article.

### Run the Upgrade

To upgrade a multi-OC environment, follow the information in this section.

#### **For 20.3.3**

Run the OC installer on the primary hub and navigate to the **Select Robot** dialog. Select the robot where you want to upgrade the existing OC instance. In 20.3.3, a new option **Specify IP** is also available in the **Select Robot** dialog. This option is in addition to the already existing **Choose** option. You can select the **Specify IP** option and directly enter the IP address of the robot where you want to upgrade the OC instance. The installer identifies that an older version of the OC is already available on the robot and prompts a message stating that you are going to upgrade the OC instance. You can then proceed with the remaining steps to upgrade the instance.

For more information about the steps, see [Install Operator Console \(OC\)](#).

---

**Prior to 20.3.3**

1. Deactivate the wasp probe on the secondary OC server.
2. Deactivate the robot running the secondary OC server.
3. Execute the OC installer from the primary hub, and select the primary OC server as the target.

**NOTE**

Verify that your first OC is working correctly. Also, take a backup of your database.

4. Deactivate the wasp probe on the primary OC server.
5. Restart the robot running the secondary OC server.
6. Clean up the existing UMP webapps before upgrading to OC on the secondary OC server. Below are the UMP webapps that need to be deleted:
  - cloudmonitor
  - listdesigner
  - listviewer
  - mobile
  - mytickets
  - policyeditor
  - qoschart
  - relationshipviewer
  - reports
  - reportscheduler (UMP reportscheduler)
  - servicedesk
  - slareports
  - unifiedreports
  - usm
  - saml-portlet
  - ump-theme
  - portal-compat-hook
  - ump-read-only-theme

**Follow the below steps to clean up UMP webapps:**

- a. Remove these webapps sections from wasp.cfg of the secondary OC server. This can be done in two ways:
    - a. Open the wasp.cfg in Raw Configure and delete the listed webapps sections under the webapps folder using the Delete Section option.
    - b. Open the wasp.cfg in Edit mode and remove the sections under the webapps.
  - b. Deactivate the wasp.
  - c. Delete these webapps folders from \Nimsoft\probes\service\wasp\webapps.
  - d. Delete the .war files of these webapps from \Nimsoft\probes\service\wasp\webapps.
  - e. Restart the wasp.
7. Drag the following packages from the Archive in the below order to the secondary OC server:

- java\_jre
- wasp
- wasp\_service\_wrapper
- nisapi\_wasp
- ump
- ump\_operatorconsole
- wasp\_alarmviewer\_api
- policy\_management\_ws
- mcsuiapp\_portlet
- ump\_cabi
- ump\_accountadmin (Optional)
- ump\_dashboard (Optional)

**NOTE**

Ensure that you drag each of the ump\_<portlet\_name> packages that are required for your environment from the Archive.

8. If the following keys and addresses are not already present, add them to wasp through the Raw Configure option, ump\_common section:
  - maintenance\_mode = /<domain>/<hub>/<UIM\_server>/maintenance\_mode
  - udm\_manager = /<domain>/<hub>/<UIM\_server>/udm\_manager
  - mpse = /<domain>/<hub>/<UIM\_server>/mpse
9. Activate, and then deactivate, the wasp probe.
10. Activate the wasp probe on the primary OC server.
11. When the wasp is running on the primary OC server, activate the wasp on the secondary OC server.

**NOTE**

These manual steps (Prior to 20.3.3) will work for 20.3.3 also. However, it is recommended that you use the OC 20.3.3 installer as explained in the "For 20.3.3" section while upgrading from an earlier version of OC to OC 20.3.3.

You have successfully upgraded the multiple OC server configuration.

**Complete Post-Upgrade Tasks**

Complete the following tasks after the upgrade is complete:

**Clear Browser After Upgrading**

If you upgraded from a previous OC version, clear your browser completely to remove older versions of components that might be cached.

**NOTE**

You do not need to perform this step if you are upgrading from an earlier version of OC to OC 20.3.2 or later.

**Follow these steps:**

1. Log out from OC.
2. Clear the browser cookies and cache.
3. Exit all browser windows.
4. Log in to OC.

[Next Step: Upgrade CA Business Intelligence with UIM >](#)

## Upgrade CA Business Intelligence with UIM

See the topic [CA Business Intelligence with UIM](#) for upgrade instructions.

### NOTE

- In an upgrade scenario, if you are upgrading CABI in a secure setup, ensure that you bring your CABI robot to the secure state by deploying the appropriate certificates and then updating the robot version to the secure version (robot\_update\_secure 9.31S). After that, you upgrade CABI. For more information about the secure setup and how to deploy certificates, see [Secure Hub and Robot](#).
- The cabi 4.10 probe supports TLS v1.2 when communicating with the UIM database: Microsoft SQL Server - 2012, 2014, 2016, and Oracle - 11.2 and 12.1. However, CABI is not supported if Microsoft SQL Server 2012, 2014, or 2016 is installed on Windows Server 2016 and TLS v1.2 is enabled. Note that UIM 20.1 (and later) do not support Oracle 11.2.
- The cabi 3.40 probe, available with UMP 9.0.2 HF2, supports TLS v1.2 when communicating with the UIM database: Microsoft SQL Server- 2012, 2014, and Oracle - 11.2 and 12.1. However, CABI is not supported if Microsoft SQL Server 2012 or 2014 is installed on Windows Server 2016 and TLS v1.2 is enabled. For more information about how to apply the UMP 9.0.2 HF2 for CABI TLS functionality, see [UMP 9.0.2 HF2](#). Note that UIM 20.1 (and later) do not support Oracle 11.2
- The cabi 3.32 probe does not support TLS v1.2 when communicating with the UIM database: Microsoft SQL Server or Oracle. As a result, you cannot view the Operator Console home page, OOTB CABI dashboards, and OOTB CABI reports.
- TLS v1.2 support is not enabled by default when you install CA UIM 9.0.2.
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

For more information, see [CA Business Intelligence with UIM](#)

[Next Step: Upgrade Monitoring Configuration Service Templates >](#)

## Upgrade Monitoring Configuration Service Templates

For complete instructions to upgrade the Monitoring Configuration Service (MCS) templates, see the [mon\\_config\\_service Release Notes](#) in Probes Documentation.

Additionally, review the following information to know more about specific scenarios related to enhanced templates.

- **Upgrading from a previous version to the current version.**
  - If MCS profiles are already available for older MCS templates before the upgrade:
    - Enhanced templates will not be visible in OC by default.
    - If you migrate these existing legacy profiles to the latest legacy template, enhanced templates will be visible in OC.
  - If no MCS profiles are available for older MCS templates before the upgrade, then the new legacy and enhanced templates will be visible in OC.
- **For new installation.**
  - Both legacy and enhanced templates are visible in OC.

[Next Step: Perform Post-Upgrade Verification and Configuration>](#)

## Upgrade Step 4: Perform Post-Upgrade Verification and Configuration

In this fourth and final step of the upgrade process, you verify that the upgrade was successful. You ensure that any new product functionality or existing functionality that was upgraded works as expected. You also verify that your customizations work as expected.

### Verify That the System Is Working as Expected

Use the following steps to verify that the system is working as expected after the upgrade.

1. Verify that all existing product functionality is working as expected with no loss of functionality.
2. Verify that all new product functionality is working as expected.
3. Test and prove that the new functionality is working as expected by running tests, either automated scripts or manual tasks.
4. Perform final configuration on your integrations and customizations that might require post-upgrade configuration to operate correctly.

Congratulations! You have successfully upgraded CA Unified Infrastructure Management.



**Next Step:** Communicate and let your end-users know that the upgrade is successful and that they can begin using the new version.

## Roll Back to a Previous Version of UIM Server

If necessary, you can use your saved **nimsoft** directory folders to roll back your UIM Server upgrade.

### **Follow these steps:**

1. Stop the robot on the system you are restoring to the required version.
2. Replace the current **nimsoft** directory with the backed-up version.
3. Start the robot.

Repeat these steps for each system where the upgrade was deployed.

### **NOTE**

Ensure that you also restore the backup of the CA UIM database.

## Administering

---

CA UIM includes user interfaces that let you manage and configure your deployment:

- **Admin Console** is a browser-based GUI for configuration and management of your CA UIM system.
- **Infrastructure Manager** is a legacy Windows-based interface for configuration and management of your CA UIM system.

### NOTE

Infrastructure Manager is not installed with CA UIM by default. You must download it separately from the CA UIM server web page.

- **Account Admin** is a view in OC that lets you manage accounts and account contact users. In addition, you can use Account Admin to restrict certain views in OC.

### NOTE

When using Admin Console to configure probes on a secondary hub, the following probes must be deployed to the secondary hub:

- ppm
- baseline\_engine
- prediction\_engine

The baseline\_engine and prediction\_engine probes are dependencies of the ppm probe, and will automatically be deployed when you deploy the ppm probe.

## Working with Admin Console

This article introduces you to the Admin Console interface.

### Contents

#### Admin Console Features

Admin Console provides the following infrastructure management capabilities:

- View hubs and associated robots and archives.
- Import and download packages.
- Deploy packages to robots on one or more hubs.
- Manage probes:
  - View the probes deployed to each robot.
  - Activate, deactivate, restart, or delete probes.
  - Access the probe configuration GUIs and Raw Configure.
  - Access the Probe Utility.
  - View probe log files.
- Manage probe security settings.
- Manage bus users.
- Export any list in the main pane as a CSV file.



## Logging in to Admin Console

You can access Admin Console in a standalone webpage.

### Follow these steps:

1. Enter the following URL in a browser:

```
http://<target_hub_IP_address>:<wasp_port>/adminconsoleapp
```

#### NOTE

By default, the wasp probe uses port 80. Cookies must be enabled in your browser for Admin Console to function correctly.

2. Enter a valid CA UIM username and password.


## Navigating Admin Console

You can navigate your infrastructure using the breadcrumbs at the top of the Admin Console window, or by drilling into a hub or a robot listed in the left or right panes.

Information is displayed in Admin Console based on the hub or robot you select; tabs and menu options vary depending on whether a hub or a robot is selected.

## Viewing Hub Information

When you log in to Admin Console, the default landing page is the **Info** tab for the primary hub in your CA UIM installation. The **Info** tab displays the status of the selected hub's robots and licenses and summarizes properties

about the hub. The left pane lists the hubs in the domain, starting with the primary hub (  ). Select a different hub from the list to view the **Info** tab for the hub you select.

In addition to the **Info** tab, the following tabs are available when a hub is selected: **Robots**, **Archive**, **Deployment Activity**, and **Licenses**.

#### NOTE

The above-mentioned licensing functionality is no longer available in CA UIM 20.3.0. From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distrv versions released with CA UIM 20.3.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).

## Robots

The **Robots** tab displays a list of the robots deployed to the selected hub. The hub robot (  ) is shown at the top of the list. You can use the **Actions** menu or the inline menu button



(  ) to restart or remove the robots listed.

## Archive

Each hub that has the `automated_deployment_engine` probe has archive functionality in Admin Console. You can download and deploy packages from any hub that has archive functionality.

If a hub has archive functionality, its **Archive** tab displays the local versions and the web versions of packages. The **Local Version** column of the **Archive** tab displays packages that are present on the file system of the selected hub.

This is also sometimes called the *local archive*. Admin Console communicates with a central server, or *web archive*, to obtain the list of packages displayed in the **Web Version** column. The web version of a package must be downloaded to the local archive prior to being deployed. However, you can deploy a package from a local archive to any robot in your infrastructure.

### **Deployment Activity**

When you deploy a package, you are automatically redirected to the **Deployment Activity** tab, where you can view the progress of deployments. If necessary, you can cancel queued deployments. Filters are available to help you locate queued deployments or failed deployments that you want to re-attempt.

### **Licenses**

The **Licenses** tab is where you can view, add, or delete probe licenses. You can also configure the license of the selected hub on the **Licenses** tab, or on the **Info** tab.

#### **NOTE**

The above-mentioned licensing functionality is no longer available in CA UIM 20.3.0. From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 20.3.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).

### **Viewing Robot Information**

When you select a robot in your environment, the **Info** tab displays the status of the probes deployed to the selected robot. The **Info** tab also summarizes properties about the selected robot.

In addition to the **Info** tab, the following tabs are available when a robot is selected: **Probes**, **Installed Packages**, and **Environment Variables**.

### **Probes**

The **Probes** tab displays the probes deployed to the selected robot. CA UIM uses probes to monitor your system, send alarms, and generate dashboards.

Probes must be configured for your specific monitoring requirements.

### **Installed Packages**

After a package has been deployed to a robot, if the package is a probe, it is displayed in both the **Installed Packages** tab and the **Probes** tab. If the package is not a probe, it is only displayed in the **Installed Packages** tab.

### **Environment Variables**

The **Environment Variables** tab displays the environment variables applicable to the selected robot, based on the operating system and probes installed.

## **Admin Console Archive Concepts**

Any hub that has the `automated_deployment_engine` probe has archive functionality in Admin Console. You can download and deploy packages from any hub that has archive functionality.

If a hub has archive functionality, its **Archive** tab displays the local versions and the web versions of packages. The **Local Version** column of the **Archive** tab displays packages that are present on the file system of the selected hub, or the *local archive*. Admin Console communicates with a central server, or *web archive*, to obtain the list of packages displayed in

the **Web Version** column. The web version of a package must be downloaded to the local archive prior to being deployed. However, you can deploy a package from a local archive to any robot in your infrastructure.

Certain packages, such as some of the packages in the UIM Server installation package, only appear in the **Local Version** column; web versions of these packages cannot be downloaded from the web archive.

### **Probes vs. Packages**

All probes are packages, but not all packages are probes. Some packages are simply bundles of software.

From the perspective of the **Archive** tab, everything is a package. The **Archive** tab lists packages that are either on the file system of the selected hub (shown in the **Local Version** column), or downloadable from a central server (shown in the **Web Version** column).

After a package has been deployed to a robot, if the package is a probe, it is displayed in both the **Probes** tab and the **Installed Packages** tab. If the package is not a probe, it is only displayed in the **Installed Packages** tab.

After deployment, probes must be configured for your specific monitoring requirements.

## **Deploy Admin Console to a Secondary Hub**

### **Requirements**

The following items are requirements for deploying Admin Console:

- Admin Console must be installed on a robot running hub 7.80 or later.
- You can install Admin Console on a primary hub, but the primary hub must be running UIM 8.4 or later.
- To be able to log in to Admin Console, wasp must be able to access the database for user authentication. This means that the port that is used by the UIM database must be unblocked on the secondary hub system.

#### **NOTE**

Deploying Admin Console to a hub where OC is deployed is not supported.

### **Deploy Admin Console**

Use Infrastructure Manager or Admin Console to deploy Admin Console. Ensure that you perform the steps in the order shown.

#### **Follow these steps:**

1. Update all instances of the `automated_deployment_engine` probe in your environment to version 8.45 or later.
2. Verify that the following probes are present in the local archive:
  - wasp 8.40 or later
  - mps 8.41 or later
  - mpse 1.71 or later

Download the above probes to the local archive if they are not already in the local archive.

3. Deploy the AdminConsole package to the target hub.
4. Edit the `wasp.cfg` and update the probe address of the `data_engine` key as follows: `{domain}/{hub}/{robot}/data_engine`

#### **NOTE**

The wasp probe defaults to HTTP port 80. To use a different port, edit the `wasp.cfg` and change the `http_port` key.

5. Manually activate mpse on the target hub robot.
6. Manually activate wasp on the target hub robot.

7. (Optional) Deploy the ppm probe version 3.30 or later to all hubs where you want to be able to launch probe configuration GUIs.
8. Launch Admin Console. Enter the following URL in a browser (this assumes that wasp is using the default HTTP port 80): `http://<target_hub_IP_address>:80/adminconsoleapp`.

**NOTE**

Before you open Admin Console, close any browser windows where the original Admin Console is running.

## Log in to Admin Console

### Contents

The Admin Console application allows you to manage and maintain the hubs, robots, and probes in your installation. You can access Admin Console using the following method:

- In a standalone web page

CA UIM bus users and account contact users with elevated permissions can access Admin Console.

### Access Admin Console Using a Standalone Web Page

#### Follow these steps:

1. Enter `http://<hub_IP_address>:<wasp_port>/adminconsoleapp` in your web browser window.

**NOTE**

By default, the wasp probe uses port 80. Cookies must be enabled in your browser for Admin Console to function correctly.

2. Enter a valid CA UIM username and password.

## Manage Hub and Probe Licenses

**NOTE**

The licensing functionality explained in this article is no longer applicable for CA UIM 9.2.0. From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).


This article describes the procedures to view, add, or delete hub and probe licenses in Admin Console.

### Contents

### View or Configure a Hub License

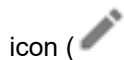
#### Follow these steps:

1. Log in to Admin Console.

By default, the primary hub (  ) is selected in the left pane, and the **Info** tab for the primary hub is displayed.

2. Select a different hub in the left pane, or continue with the primary hub selected.

3. Select the pencil



to the **License** summary, or select **Actions > Configure Hub License**.

4. To update the hub license, copy and paste a valid license into the **License** field.
5. Click **Save**.

### **Manage Probe Licenses**

You can select any hub in the left pane that has the distsrv probe deployed, and select the **Licenses** tab to view or configure probe licenses. The **Code** column displays the license string for each product listed.

### **Change the License Property Fields**

You can customize the license property columns that are displayed on the **Licenses** tab. Select the **Display**



**columns** icon ( ), and select or deselect the following properties:

- **Info** - License description.
- **Expiration** - Date the license expires.
- **IP** - IP address that is used to limit the systems that the probe is licensed to run on. An asterisk (\*) indicates that the probe is licensed to run on any system on your selected hub.
- **Number** - Number of licenses for the probe package.
- **Code** - Valid license code for the probe.

### **Add a Probe License**

#### **Follow these steps:**

1. Log in to Admin Console.
2. Select a hub, and select the **Licenses** tab.
3. Select **Actions > Add licenses**.

#### **NOTE**

You do not need to select any probes before adding licenses; the license strings you enter in the **Add licenses** dialog are applied to the appropriate probes regardless of the probes you select.

4. Paste one or more license keys into the **Add Licenses** window.

### **Delete a Probe License**

#### **Follow these steps:**

1. Log in to Admin Console.
2. Select a hub, and select the **Licenses** tab.
3. Check the box to the left of the probe you want to delete.
4. Select **Actions > Delete licenses**.  
You are prompted to confirm the deletion.


## Restart or Remove a Robot

When you remove a robot, the association between the robot and the hub is removed. To uninstall a robot, manually delete the robot directory from the server where it is deployed.

**Note:** You cannot remove a hub robot.

### Follow these steps:

1. Select the hub where the target robot is deployed, and select the **Robots** tab.
2. Take one of the following actions:
  - Select the inline menu button
 


)

 next to the target robot, and select **Restart | Remove**?.
  - Select the check box next to one or more robots, and select **Actions, Restart | Remove**.
3. Confirm to restart or remove the robot. Allow a few minutes for the console to update.

If the robot remains in the console tree after it is removed, you can manually delete it from the parent hub.

1. Log in to the parent hub server, and locate the `UIMHOME/hub` directory.
2. Delete the file `robot.sds`.
3. Restart the parent hub.

A new, empty `robot.sds` file is created during startup. As robots reconnect to the parent hub, they are added to the new `robot.sds` file, and the console tree is refreshed.

## Download, Update, or Import Packages

When there is a web version of a package that you do not have in the local archive, you use the download action to move the package to the local archive. When you have a local version of a package, but there is a more recent version in the web archive, you use the update action to obtain the more recent version from the web archive. You use the import action to move a package into the local archive that cannot be obtained from the web archive.


**Note:** The first time you download a package from the web archive, you will be prompted to enter your web archive credentials.

### Download a Package

If you want to deploy a package that is in the web archive, but not in the local archive, you must first download the package. Downloading the package moves it to the local archive.

### Follow these steps:

1. Select a hub, and select the **Archive** tab.
2. Do one of the following:
  - Select the inline menu button
 


)

 next to the package you want to download, and select **Download**.
  - Select multiple packages and then select **Actions > Download**.
3. Confirm that you want to download the package.

The **Local Version** column is updated to display the web version you downloaded.

## **Update Packages**

Use the steps in this section to update the local version of one or more packages to more recent web versions.

### **Follow these steps:**

1. Select a hub, and select the **Archive** tab.
2. Do one of the following:
  - Update individual items - Select the **Update** hotlink next to the local version of a package.
  - Bulk update - Select **Actions > Update All**.

**Note:** Enter text into the filter to narrow the scope to specific packages to update. Or, select the **Available Updates** filter from the drop-down menu to see only the packages with an available update.

After you confirm the update, the packages are updated to the web versions shown.

## **Import a Package**

If a package is not available from the web archive, such as a custom package, you must first import the package before you can deploy it.

### **Follow these steps:**

1. Select a hub, and select the **Archive** tab.
2. Select **Actions > Import Packages**.
3. Drag files to the **Import Packages** dialog, or click the **Browse** button and navigate to the files you want to import.

The **Local Version** column is updated to display the package you imported.

## **Deploy Packages**

You can deploy a package from the local archive of any hub that has the `automated_deployment_engine` probe to any robot in your infrastructure.

### **Follow these steps:**

1. Log in to Admin Console.
2. Select a hub, and then select the **Archive** tab.
3. Do one of the following:
  - Single package – select the inline menu button next to a package, and then select **Deploy**.
  - Multiple packages – select the check boxes next to multiple packages, and then select **Actions > Deploy**.
4. In the **Hubs** pane, select the check box next to a hub to select all the robots under the hub. Or, drill-down into the hub and select individual robots. To return to the list of hubs, click the back arrow in the middle pane. The **Target Robots** pane updates to show the selected robots.
5. Select **Deploy**.

The page redirects to the **Deployment Activity** tab where you can monitor the deployment.

## **Verify a Package Deployed**

After a package has been deployed to a robot, if the package is a probe, it is displayed in both the **Installed Packages** tab and the **Probes** tab. If the package is not a probe, it is only displayed in the **Installed Packages** tab.

### **Follow these steps:**

1. Select the hub, and then select the robot where the probe was deployed.

2. Select the **Installed Packages** tab. Or, if the package you deployed was a probe, you can also select the **Probes** tab to verify it is listed.

If the package you deployed was a probe, the probe is now ready for you to configure.

## Configure a Probe

Two different probe configuration tools are available in Admin Console: probe configuration GUIs and Raw Configure. Many probes, but not all, have a probe configuration GUI. All probe configurations can be modified using Raw Configure.

Each probe configuration GUI is designed to handle the specific workflows of the probe it was built for. Probes with more involved configurations typically provide a probe configuration GUI. Raw Configure is a generalized configuration file editor that does not provide any custom workflows. Raw Configure is typically used to make simple configuration edits, such as adjusting the log level of a probe.

Probe configuration GUIs often provide functionality that Raw Configure does not. For example, password encryption is handled for you if you modify the webgtw probe in its configuration GUI. If you add a password to the webgtw probe in Raw Configure, you have to encrypt the password yourself, and then enter the encrypted password. In addition, probe configuration GUIs often validate the entries you make, whereas Raw Configure does not.

### NOTE

For the specific configuration procedures for individual probes, see the [Probes Documentation](#).

### Contents

#### Open a Probe Configuration GUI or Raw Configure

##### Follow these steps:

1. Log in to Admin Console.
2. Select the hub, and select the robot where the target probe is deployed.
3. Select the **Probes** tab.
4. Select the inline menu button

)

next to the probe > **Configure** or **Raw Configure**.

If you selected **Configure**, the configuration GUI for the probe opens in a new tab. If you selected **Raw Configure**, the Raw Configure utility for the probe opens in Admin Console.

### TIP

You can search the configuration file for a probe using the search icon


)

in the Raw Configure utility.

#### About the Probe Configuration GUI

The probe configuration GUI contains a left and right navigation pane. The right navigation pane usually contains configuration information based on your selection in the left navigation pane. For more information about specific elements and configuration options for individual probes, see the Probe Documentation.



The left navigation pane contains a hierarchical representation of the monitoring targets and any configurable elements associated with the probe. The left navigation pane also contains a filter to help locate items within the probe hierarchy. This filter is especially useful if you must manage multiple probe configuration elements.

Make note of the following information when using the filter:

- The names of items that match your filter criteria appear as highlighted bold text.
- Collapsed items that contain child items that match your filter criteria appear as bold text.
- Items that do not match your filter criteria appear as gray text.
- Collapsed items that contain unloaded child items contain a white plus icon.



#### NOTE

The filter only locates items loaded in the current view. It might be necessary to expand a collapsed item to load any child items.



### Use Raw Configure to Edit a Probe Configuration

#### Follow these steps:

1. Log in to Admin Console.
2. Select the hub, and then select the robot where the target probe is deployed.
3. Select the **Probes** tab.
4. Select the inline menu button
 


  
 (  )

 next to the probe > **Raw Configure**.
5. Use the following options as needed:
  - To add a section, select the **Create new section** icon (+) in the left pane. Enter a name for the new section.
  - To add a new key, select the **Create new key** icon (+) in the right pane. Populate the **Key** and **Value** fields.
  - To edit an existing key, select the inline menu button
 


  
 (  )

 next to the key > **Edit value**. Update the **Value** field as needed.
6. Select **Update** to commit your changes.

### **Activate, Deactivate, or Restart a Probe**

From the Admin Console interface, you can activate, deactivate, or restart a probe on a target device.

#### Follow these steps:

1. Log in to Admin Console.
2. Select the hub, and select the robot where the target probe is deployed.
3. Select the **Probes** tab.
4. Select the inline menu button next to the probe > **Activate, Deactivate, or Restart**.

## View a Probe Log File

Each probe has a log file. This file contains information about the probe and is used for debugging purposes. A default of 500 lines displays in the log viewer window.

### Follow these steps:

1. Log in to Admin Console.
2. Select the hub, and select the robot where the target probe is deployed.
3. Select the **Probes** tab.
4. Select the inline menu button next to the probe > **View Log** or **View Log in New Window**.

### Download or Clear a Log File

#### Follow these steps:

1. Select the hub, and select the robot where the target probe is deployed.
2. Select the **Probes** tab.
3. Select **Actions** > **Download Log** or **Clear** in the log viewer window.

## Manage Probe Security Settings

Probe security settings determine an individual probe's access to other probes or computer systems in the domain. Probes have default security settings that do not usually need to be edited. In general, you only need to add probe security to custom probes.

### NOTE

Only bus users with the *Probe Security* permission can manage probe security settings.

### Contents

#### Manage Probe Security in Admin Console

You can modify the following probe security settings:

- **Access** - The level of bus access that the probe has--**open**, **read**, **write**, **admin**, or **super**.
- **IP mask** - The IP addresses where the probe security setting applies. The IP mask field allows for the use of Perl regular expressions. A wildcard (\*) in this field allows access to all systems in the domain.

### WARNING

If a probe is running on an IP address that does not match the IP mask that you enter, the probe is not allowed to start up and log in to the bus.

#### Add Probe Security

#### Follow these steps:

1. Log in to the Admin Console.

2. Select the menu button



(  )  
> **Probe Security**.

3. Select **Actions** > **Add**.
4. Enter the name of the probe you want to restrict access to.
5. Select the **Access** level that you want, and optionally, specify an **IP Mask**.
6. Select the **Save** button to commit your changes.

### **Edit Probe Security**

#### **Follow these steps:**


1. Log in to the Admin Console.
2. Select the menu button



(  ) > **Pro**

3. Select the inline menu button



(  ) next  
to the appropriate probe, and select **Edit**.

4. Update the **Access** level or **IP Mask** as needed.
5. Select the **Save** button to commit your changes.

### **Delete Probe Security**

#### **Follow these steps:**

1. Log in to the Admin Console.
2. Select the menu button



(  ) > **Pro**

3. Do one of the following:

- Select the inline menu button



(  ) next  
to a probe > **Delete**.

- Select the check box next to one or more probes, and then select **Actions** > **Delete Probe Access**.

4. Confirm that you want to delete the probe security access level.

## **Use the Probe Utility**

CA UIM components communicate with each other via commands, or *callbacks*, on the bus. The Probe Utility lets you issue ad hoc callbacks for debugging a probe, scripting automated tasks, or developing custom probes.

#### **Follow these steps:**

1. Log in to Admin Console
2. Select the hub, and select the robot running the target probe.

3. Select the inline menu button



next to the target probe > **View Probe Utility in New Window**.

4. Select a callback from the **Command** column, and provide additional parameters if required.
5. Select the play button to run the callback.

## Manage Bus Users

You can add, edit, or delete bus users in Admin Console. Only bus users with the ACL permission *User Administration* can manage bus users.

### NOTE

Account contact users are managed in the Account Admin view in OC.

### Contents

#### Add a Bus User

##### Follow these steps:

1. Log in to Admin Console.
2. Select the menu button (☰) > **Manage Users**.
3. Select the plus icon (+) to add a user.
4. Enter the following information about the user:

### NOTE

Avoid creating bus users and LDAP users with identical user names.

- **User name** (required) – must be 1 to 254 characters long; cannot contain control characters, right or left arrows (< or >), or forward slashes ( / )
  - **Description**
  - **Password** (required) – must be 5 to 254 characters long; cannot be the user name
  - **ACL** (required) – select the access control list assigned to the user
  - **Mobile Phone Number**
  - **Email Address**
5. Select **Create** to commit your changes. The user information is saved in the security file, **<UIM\_installation>/hub/security.cfg**.

#### Edit a User

##### Follow these steps:

1. Log in to Admin Console.
2. Select the menu button (☰) > **Manage Users**.
3. Select the user to edit.

### NOTE

You cannot edit the **User Name** of an existing user.

4. In the **Edit User** pane, update fields as needed.
5. Select **Update** to commit your changes.

## Delete a User

### Follow these steps:

1. Log in to Admin Console.
2. Select the menu button (☰) > **Manage Users**.
3. Select the trash icon next to the user you want to delete.

#### NOTE

You cannot delete the user *administrator* or the user you are currently logged in as.

4. Confirm that you want to delete the user.

## Admin Console ACL Permissions Reference

Bus users and account contact users can access Admin Console. However, the majority of what users can see and do in Admin Console is controlled by the individual permissions selected in their ACL.

The following table summarizes the ACL permissions that are required for various features in Admin Console.

#### NOTE

Certain features in Admin Console are only available to bus users. For example, only bus users can manage other bus users.

| ACL Permission            | Actions and UI Locations                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Archive Management</b> | Delete (Archive)                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Basic Management</b>   | Download (Archive)<br>Update (Archive)<br>Update All (Archive)<br>Delete (Robots)<br>Restart (Robots)<br>Enter Web Credentials (Archive)<br>Import Package (Archive)<br>Probe Security (Menu)<br>Active (Probe)<br>Deactivate (Probe)<br>Restart (Probe)<br>Delete (Probe)<br>Configure (Probe)<br>Raw Configure (Probe)<br>View Config (Probe)<br>View Log (Probe)                                                                                                         |
| <b>Distribution</b>       | Deploy (Archive)                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>License Management</b> | Edit the hub license (Hub Details and Licenses)<br><br><b>Note:</b> From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required). |

|                            |                                                                   |
|----------------------------|-------------------------------------------------------------------|
| <b>Probe Basic</b>         | Probe Security (Menu)<br>View Config (Probe)<br>View Log (Probe)  |
| <b>Probe Configuration</b> | Configure (Probe)<br>Raw Configure (Probe)<br>View Config (Probe) |
| <b>Probe Security</b>      | Add (Security)<br>Edit (Security)<br>Delete (Security)            |
| <b>User Administration</b> | Manage Users (Menu)                                               |

## Working with Infrastructure Manager

Infrastructure Manager is a legacy management interface that is required for some CA UIM tasks.

### General Probe Management in Infrastructure Manager

This article covers all the probe management tasks that you can perform in Infrastructure Manager.

#### NOTE

For the specific configuration procedures for individual probes, see the [Probes Documentation](#).

#### Deploy Individual Probes

As a CA UIM administrator, you can deploy probes with Infrastructure Manager. CA UIM uses probes to monitor your system, send alarms, and provide dashboards that display the status of your system. Configure the probe for your specific monitoring requirements after deployment.

#### NOTE

Probe packages that are added to the archive with Admin Console, are not visible in the Infrastructure Manager archive list until distsrv is restarted.

Before you begin, review the prerequisites for your monitoring probes. See the [Probes Documentation](#).

#### Distribute Probes from the Local Archive

#### NOTE

Some updated versions of probes have dependencies on newer UIM components. Check the [Probe Support Matrix](#) to confirm compatibility and support before distributing updated probes on top of older robots and hubs.

#### Follow these steps:

1. Select a hub under the **Archive** node to display the probes.
2. Drag-and-drop the probe to one of the following items in the navigation pane:
  - – **Single robot**
  - **Hub** to distribute to all robots in the hub

**NOTE**

In the **Confirm Drop** dialog, select **Update only** to distribute the package to only robots on which the probe exists.

- **Group** to distribute to all robots in the group
- **OS group** under the **Dynamic Views** node to distribute to all the robots running the same OS

A progress window appears on the screen when the distribution process starts.

**Distributing Multiple Probes and Configuration Files as a Super Package**

You can use Infrastructure Manager to consolidate multiple probe packages into a super package. For example, if you want to distribute multiple probes and configuration files to multiple systems in one operation. Systems receive the same probes with identical configuration parameters.

A super package can be distributed to a:

- single robot.
- hub, including all underlying robots.
- domain, including all underlying hubs and robots.

**NOTE**

When including the cdm probe in a package, you must ensure that the target computers have the same disk partitions as defined in the cdm configuration file (*cdm.cfx*) distributed with the package. For example, If the configuration file has defined a C: and a D: partition, and you distribute the package to a computer with only a C: partition, the cdm probe reports an error.

**Create the Super Package**

The package editor is used to create and then modify packages for distribution to robots.

**Follow these steps:**

1. In Infrastructure Manager, open the archive, right-click in the list, and select **New** to launch the package editor.
2. Name the new package.
3. (Optional) Select a group to set the category for the super package in the archive.
4. Click **OK**. The new package appears in the package archive.

**Save the Probe Configuration Files****NOTE**

Verify that the probe has the desired configuration settings saving the probe configuration (.cfg) file.

1. Drag and drop a probe to add to the Super Package probe into the archive. A version of the probe with your defined configuration settings is saved in the archive.
2. Verify that **Configuration Only** is selected, rename the probe package, and click **OK**.
3. Select the probe package in the package archive, right-click and select **edit**.
4. Right-click the probe .cfx file in the files list, click **Save file as**, and save the file.

**NOTE**

The new file name cannot have more than one period in the name.

Repeat this procedure for each of the probes you want to include in the Super Package.

## Add the Probe Configuration Files to the Super Package

### Follow these steps:

1. Right-click on the Super Package in the archive and select **Edit**.
2. Right-click the **OStype** tab and select **Add section**.
3. Name the section based on the operating system of the target systems. The following operating systems are supported:
  - AIX\_5
  - AIX\_5\_64
  - HPUX\_11
  - HPUX\_11\_64
  - HPUX\_11\_ia64
  - LINUX\_23
  - LINUX\_23\_64
  - LINUX\_23\_ppc64
  - SOLARIS\_10\_amd64
  - SOLARIS\_10\_i386
  - SOLARIS\_8\_sparc
  - SOLARIS\_8\_sparcv9
  - TRU64
  - win32
  - win64
  - win64\_ia64
4. Select the operating system from the **OStype** drop-down menu.
5. Click the **Dependencies** tab, right-click in the window, and select **Add dependencies**.
6. Enter a probe name.
7. (Optional) Enter the probe version number. Without a probe version number, the package is only distributed to the systems where it is not currently deployed. Entering a version number expands deployment to systems with an older version of the probe.

### NOTE

If you do not also set **Type**, the latest version of the probe is used. To control which version of the probe is distributed, set a type using one of the following operators:

- **ge** - greater than or equal to.
- **le** - less than or equal to.
- **eq** - equal to.
- **gt** - greater than.
- **lt** - less than.
- **Any**

8. Create a section called *<probename>-cfg* (for example, cmd-cfg).
9. Select **Configuration of existing probe** and enter the probe name. Click **OK**.
10. Select the **Files** tab, right-click in the window, and select **Add file**.
11. Select **Browse** to find the saved .cfx file for the probe and click **OK**.
12. Repeat steps 6-12 for all the probes you want to include in the super package.
13. Click **OK**. The super package can now be distributed using drag-and-drop.



## **.cfx Directives**

Directives to determine merging behavior are added to the beginning of a section. The following directives are supported:

“

No directive: add keys from this section if they are not already present in the target configuration file.

### **‘overwrite’**

Add keys from this section overwriting existing keys in the target configuration file. Changed sections are moved to the end of the containing section. This behavior is needed when adding or changing a set of sections which need to be in a particular order.

### **‘edit’**

Add or change keys from this section overwriting existing keys. The section position is not changed when using this option.

### **‘delete’**

Remove keys mentioned.

### **‘clear’**

Remove the whole section. If the section contains any keys, then re-create the section adding these keys.

The same section can occur several times, for example:

```
<a> delete
existing_key_to_delete_1 = value_to_be_removed

<a>
new_key2 = new_value_to_be_added

```

This removes key1 from section a and adds key2.

Subsections do not inherit directives. Directives must be specified explicitly for each. The ‘clear’ directive is an exception, since it affects all subsections.

## **Configure a Probe**

You must be logged in to the robot that the probe is deployed under to configure a probe.

### **Open the Probe Configuration GUI**

#### **Follow these steps:**

1. Select a Robot under a child-node.
2. Double-click the probe in the main window pane. The probe configuration GUI opens.

### **Open the Raw Configure Utility and Add Parameters**

Many probes have their own custom configuration GUI. For the probes that do not, Infrastructure Manager presents the probe configuration data in an editor similar to regedit.

Raw configure lets you add, delete, and modify the nodes in the configuration file, and the variable name/value elements.

#### **Follow these steps:**

1. Select the robot in the navigation pane. If you cannot see the robot, expand the navigation tree.
2. Select a probe.

3. **Shift+Right-Click** and select **Raw Configure**.
4. Click the folder you want to add the new parameter to.
5. Click the **New Key** button.
6. Enter the Key Name and Value, and click **OK**.
7. Repeat the process for all the required parameters for your probe.
8. Click **Apply**.

### **Copy Probe Configuration Settings**

If you have configured a probe on one robot, you can copy your settings to the same probe deployed on a different robot.

#### **Follow these steps:**

1. Log on to the hub where the robot with the probe configuration you want to copy is deployed.
2. Select the probe from the probe list.
3. Drag and drop the probe into the Archive. The **Update packages** dialog opens.
4. Click **Rename** and give the package a descriptive name.
5. Ensure that the **Configuration Only** option is checked and click **Ok**.
6. Select the renamed probe configuration package.
7. Drag-and-drop the probe package onto the robots you want to copy the probe configuration settings to.

### **Add a New Probe Definition**

#### **Follow these steps:**

1. Log in to Infrastructure Manager
2. Select a robot in the Navigation Pane.
3. Right-click on the desired probe, select **Edit**. You can then change the following probe properties:
  - **Probe** - The name of the probe.
  - **Type** - The type of the probe, daemon, on\_demand, or timed.
  - **Command** - The name of the executable, relative to the working directory, or the full path if specifying an executable elsewhere in the directory structure.
  - **Arguments** - The argument list accompanying the command.
  - **Working directory** - The working directory for probe.
  - **Configuration file** - The name of the probe configuration file.
  - **Data file** - The name of the probe data file.
  - **Time specification** - Specifies when the probe is active. Use the time format described in the following section.
  - **Execution** - Specifies when and how often the probe is executed.
  - **Group** - The name of the group the probe belongs to.
  - **Description** - A short description of the probe.
  - **Log file** - Name of the log file for the probe.

### **Time Specification Format**

The format of the time specification that is used in the *Range From / To and Execution / Start at* fields is:

- <minute>
- <hour>:<minute>
- <weekday> <hour>:<minute>
- <day of month> <hour>:<minute>
- <month> <day of month> <hour>:<minute>

**Examples:**

- **Range From: 03:15, Range To: 06:00** - Activate the Probe in this interval. The Probe is terminated when it passes its window of time.
- **Start at: 04:20** - Start the timed Probe at 04:20.
- **Interval: 5 min** - Start the timed Probe at a 5-min interval. This Interval can be combined with a range specification.

**Find Hubs or Probes in a System**

You can use the find dialog in Infrastructure Manager to locate hubs or probes cross-domain in a system.

**Follow these steps:**

1. In Infrastructure Manager, select the Domain Node in the Navigation Pane.
2. Click **Tools, Find**.
3. Enter your search criteria in the Find dialog and click the OK button. The search results are listed in a separate window, and include detailed probe information.

**View the Probe Log File**

Most probes record various run-time events to a log file. To open the log viewer window, right-click the probe and select *View Log*.

**NOTE**

You can set the logging level for most probes using the probe's Raw Configure option.

**Use the Probe Utility**

Use the probe utility to run a probe command, and view the output in the right pane. The probe utility can assist you with debugging.

**Follow these steps:**

1. In Infrastructure Manager, select the probe in the main window.
2. Left-click on the probe and click CTRL + P simultaneously.

The Probe Utility window contains the following four sections:

- The Toolbar, containing six buttons.
- The Probe Command set section, consisting of:
  - a drop-down menu where you can select one of the commands available.
  - a parameter list, where parameters belonging to the selected command will be listed. Note that not all commands have associated parameters.
  - an input field, where you can specify a value for the parameter selected in the parameter list.
- The *Command output* window.
- The Status bar (at the bottom of the Probe Utility window), shows the status of the last command sent. For example, OK or Communication error.

**The Toolbar**

- The toolbar contains the following six buttons:
- The **Info** button. The *Command output* window lists general probe information, such as probe name, probe version, and library version.
- The **Restart** button. Restart the probe. You are asked to confirm that you really want to restart it.
- The **Stop** button. Stop the probe. You are asked to confirm that you really want to stop it.
- The **Run** button. Run the command selected in the *Commandset* section. Optional, command parameter.
- The **Options** button. Open the properties dialog for the probe. The option box contains:
  - The IP address of the computer hosting the probe.
  - Request timeout is the maximum time to wait for a response from the probe to the command. No response within this period results in an error status.
  - Show variable type (and size). When selected, the command output field shows the variable name, value, size, and type, such as integer, PDS, or string.
  - Expert Mode. Select to show an additional set of commands for advanced users.

## Manage Robots in Infrastructure Manager

Robots manage the probes deployed in a CA UIM environment. A robot starts and stops probes at the required times, and collects, queues, and forwards monitoring data. Install a robot on each computer you want to monitor.

Each robot has three dedicated tasks:

- **Control the probes** attached to the robot. Robots use the *controller* probe to start and stop probes.
- **Collect, queue and forward** the probe messages. Robots use the *spooler* probe to relay messages to and from probes.
- **Provide a simple database service** for the probes. Robots use the *hdb* probe to store data for threshold monitoring and data trending to ensure that data survives power outages.

The controller, spooler, and hdb probes are service probes that are present on every robot.

All robots are identical. Robots are only distinguishable by the collections of probes they manage. You can group probes into *packages* so that you can appropriately deploy them to different types of servers.

This article describes the robot management tasks that you can perform in the UIM Infrastructure Management tool. For more information about configuring robots and probes, see the following articles on Probes Documentation:

- [Controller](#)
- [Spooler](#)
- [Configure a Robot for Marketplace Probes](#)

### Contents

#### Locate a Robot

Use Infrastructure Manager to find the location of a robot.

To find the location of a robot, follow these steps:

1. Select the robot that you wish to connect to in the left tree pane.
2. Enter Ctrl+R, or select the menu item **Tools, Connect Robot**.
3. Click **Get Info**.

The information area contains the names of the primary and secondary hubs, or *NO hub* if the robot is unmanaged.

If the robot is *not* listed in the left tree pane, follow these steps:

1. Select the menu item **Tools, Connect Robot**.
2. In the field **Enter Robot IP Address or Name**, enter the robot IP address, or the UIM domain address in the form / *domain/hub/robot*.
3. Click **Get Info**.

The information area contains the names of the primary and secondary hubs, or *NO hub* if the robot is unmanaged.

### **Move an Active Robot to Balance the Hub Load**

A robot is configured to communicate with a specific parent hub during installation. You can manually move the robot to a different parent hub to balance the workload between hubs.

#### **Follow these steps:**

In the Infrastructure Manager navigation tree, either:

- Drag-and-drop a robot from one hub to another.
- Use the **Move** command:
  1. Right-click the robot and select **Move**.
  2. *(Optional)* To move the robot to a hub in another domain, select **Show hubs in all domains**.
  3. In the **Move** dialog, either:
    - Select the hub that you want to be the new parent.
    - Select **Use DNS Lookup**, and enter the DNS name of the system hosting the desired parent hub.
  4. Click **OK**.

### **Move a Passive Robot to Balance the Hub Load**

To move a passive robot, remove the robot from one hub and add it to the other hub.

#### **Follow these steps:**

1. Remove the passive robot from the current hub:
  - a. Right-click the parent hub of the passive robot in the left navigation tree, and select **Properties**.
  - b. Select the **Robots** tab.
  - c. In the list of Registered Robots, right-click the desired robot and select **Remove**.
2. Add the passive robot to the new hub:
  - a. In the navigation tree, right-click the new parent hub, and select **Properties**.
  - b. Select the **Robots** tab.
  - c. Right-click within the Registered Robots pane and select **Add Passive Robot**.
  - d. Enter the robot IP address and specify the port. Default, 48000.
  - e. Click **Verify**. When the robot successfully connects, click **OK**, then click **OK** again to add the robot.
3. Click **OK** to restart the probe.

## **Locate or Move a Robot**

Use Infrastructure Manager to find the location of a robot, or move a robot to a new hub or domain.

To find the location of a robot, follow these steps:

1. Select the robot that you wish to connect to in the left tree pane.
2. Enter Ctrl+R, or select the menu item **Tools, Connect Robot**.
3. Click **Get Info**.

The information area contains the names of the primary and secondary hubs, or *NO hub* if the robot is unmanaged.

If the robot is *not* listed in the left tree pane, follow these steps:

1. Select the menu item **Tools, Connect Robot**.
2. In the field **Enter Robot IP Address or Name**, enter the robot IP address, or the UIM domain address in the form */domain/hub/robot*.
3. Click **Get Info**.

The information area contains the names of the primary and secondary hubs, or *NO hub* if the robot is unmanaged.

When you have located the robot, you can move it to a different hub. Follow these steps:

1. Click **Move**.
2. Select the destination hub. If you select the checkbox **Show hubs in all domains**, you can move the robot to a hub in a new domain.

## Connect a Passive Robot to a Hub

After you install a passive robot, you must add the robot to a hub's registered robots. This makes the robot a child of the specified parent hub and enables the robot to communicate on the message bus.

Follow these steps:

1. In Infrastructure Manager, navigate to the hub that will be the parent of the passive robot.
2. Display the hub's probes, then right-click the hub probe and select **Configure**.
3. Select the **Robots** tab.
4. In the **Registered Robots** pane, right-click and select **Add Passive Robot**.
5. Enter the robot's IP address and first probe port (default is 48000).
6. Click **Verify**, then click **OK** to exit the dialogs.

The parent hub is now configured to request messages from the robot.

If you plan to deploy marketplace packages to the robot, make sure you specify the marketplace user.

## Add or Modify Users in Infrastructure Manager

Using Infrastructure Manager, you can create new ACLs and bus users.

### Contents

#### Add a New ACL Using Infrastructure Manager

You can create different ACLs and assign them permissions that different types of users need to do their work. For example, you can create an ACL and assign it permissions so that users attached to that ACL see only information from a specific hub.

#### Follow these steps:

1. Click **Security, User Administration**.
2. Right-click anywhere within the **User Administration** dialog box and select **New User**.
3. In the **New User** dialog box, click **Manage ACL**.
4. Under the Access Control List, click **New**. In the dialog:
  - Give the new ACL a name.
  - Select an ACL to copy the permission and filter settings from.

5. (Optional) Change the permissions by clicking the desired Permissions boxes.

### **Add a New Bus User in Infrastructure Manager**

Follow these steps to create a new bus user.

#### **NOTE**

Avoid creating bus users and LDAP users with identical user names.

1. Click **Security, User Administration**.
2. In the User Administration window, right-click and select **New User**.
3. Enter the following information about the user:
  - **User** (required) – Usernames must be 1 to 254 characters long; cannot contain control characters, right or left arrows (< or >), or forward slashes ( / )
  - **Full name**
  - **Description**
  - **Password** (required) – must be 5 to 254 characters long; cannot be the user name
  - **Access Control List** (required) – select the access control list assigned to the user
  - **Profile** (required)
  - **Phone number**
  - **Mobile Phone Number**
  - **Email Address**
4. Click **OK**.  
The user is added to the **User Administration** window.
5. Close the **User Administration** window  
The user information is saved in the security file, **<Nimsoft>/hub/security.cfg**.

### **Define User-actions in Infrastructure Manager**

You can add your own user-defined menu commands that will show up in the popup menu when you right-click on the robot list.

Follow these steps:

1. Select a hub in the navigation pane.
2. Right-click on the robot list and then click **Actions, Configure**.
3. In the **Configure** dialog, click **New** to add a new command. Use **Move Up** and **Move Down** to change the command order.
4. (Optional) Use the argument field to specify tokens that are expanded to the correct value when the command is initiated. For example, \$ROBOT is replaced with the name of the selected robot when you activate the command.

#### **TIP**

Supported tokens names are the same as the column name headers in the robot list. Simply add a \$ to the column name and capitalize all of the letters in the word. For example, Address would become \$ADDRESS. You will need to save your user defined menu configurations to a profile if you want them to persist between sessions.

## **Manage Licenses for Components in Infrastructure Manager**

#### **NOTE**

The functionality explained in this article is no longer applicable for CA UIM 9.2.0. From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv

versions released with CA UIM 9.2.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).

Hubs and probes have licenses that eventually need to be updated. This article describes the procedures for updating licenses in Infrastructure Manager.

### **Add a Hub License**

#### **Follow these steps:**

1. In Infrastructure Manager, double-click the hub probe.
2. On the **General** tab, click the **Modify** button.
3. Copy the license text string into the Edit License dialog, click **apply**.
4. Restart the hub probe.

### **Add a Probe License**

#### **Follow these steps:**

1. Select the Licenses icon under the Archive Node in the Navigation Pane.
2. Right-click on a white space in the right pane, select **Add License** from the context menu, paste the license string in the dialog, and click **OK**. The message **License has been successfully applied** appears.

## **Using Account Admin**

The Account Admin allows bus users to manage account contact users and access control lists (ACLs) for user groups. You must have appropriate ACL permissions to view and make changes within the Account Admin.

In Account Admin, you can add, modify, or delete accounts and account contact users and set passwords for account contacts. You can also add, copy, or delete an ACL and turn permissions within an ACL on or off. You can also associate LDAP groups with ACLs and accounts. Changes that you make to ACLs in the Account Admin are reflected in Infrastructure Manager.

The Account Admin is accessed through the Operator Console (OC). To open the Account Admin, go to Settings in the left pane of OC and click on the Account Admin.

## **Change a User Password in the Account Admin**

The Account Admin allows users to change passwords and other personal information.

If you have the Account Administration permission, you can change a user's password using the Edit User pane. See specifics steps in [Using Account Admin](#).

If you only have the Change Password permission, you will see a pane containing your user information. Fields that cannot be changed will be grayed out.

#### **Follow these steps:**

1. Open the Account Admin view.
2. Enter the new password in the **New Password** and **Confirm Password** fields. Passwords must be at least six characters long and be identical.
3. Click **Update**.



## Add or Modify Users with Account Admin

The Account Admin allows bus users to manage account contact users and access control lists (ACLs) for user groups. You must have appropriate ACL permissions to view and make changes within the Account Admin view.

In Account Admin, you can add, modify, or delete accounts and account contact users, and set passwords for account contacts. You can also add, copy, or delete an ACL and turn permissions within an ACL on or off. You can also associate LDAP groups with ACLs and accounts.

Changes that you make to ACLs in the Account Admin view are reflected in Infrastructure Manager.

### Contents

#### Create, Edit, or Delete an Account

The Account Admin allows you to create, edit, and delete accounts and account contact users.

The **Account Admin** window has two tabs: **Accounts** and **ACLs & LDAP**. When **Accounts** is selected, the left-hand pane displays existing accounts and the right-hand pane displays users currently assigned to the selected account.

#### NOTE

To create, edit, and delete accounts, you must have Manage ACL permission. If you are an account administrator, non-editable fields will appear in gray.

#### To add an account:

1. Select the **Accounts** tab at the top of the page.
2. Click on the **New** icon to the right of the Accounts header in the left-hand pane.
3. Enter the description of the account name in the right-hand pane.
4. Select the **Ownership** for the account.
5. Fill in any additional information for the account, such as **Description** or **Web Site**.
6. Click on the **Create** button at the lower-right corner of the pane.

The **Account Name** and **Ownership (origin)** fields are mandatory. The account name must be a character string. By default, no origin is selected. None of the other fields is validated and any input will be saved.

#### NOTE

Once you create an account, the account name is displayed in grey and cannot be changed. To use a different account name, you must create a new account.

The **Ownership** is the set of origins assigned to the account, which determines what information is visible for account contact users. You can assign more than one origin to an account. If you are an MSP, for example, you might designate the primary hub for each customer as the origin, thereby separating customer information. In OC, account contact users can only see devices, alarms and QoS metrics from origins assigned to the account.

#### To edit existing account information:

1. Click the **Edit** icon to the right of the account name or double-click the account name in the left-hand pane.
2. Enter changes and then click on the **Update** button at the lower-right of the right-hand pane.

#### To delete an existing account:

#### NOTE

Deleting an account also deletes any users that are not associated with other accounts.

1. Click on the **Delete** icon to the right of the account name.
2. Click **Yes** in the dialog box that appears.

## **Add, Edit, or Delete a User**

### **NOTE**

To create, edit, and delete users, you must have the Account Administration permission.

### **To add a user to an account:**

1. Click on the account of interest. A list of assigned users will appear in the right-hand pane.
2. Click on the **Add** icon at the right-hand side of the pane header.
3. Enter information for the user in the right-hand pane. Note that:
  - The associated account and ACL can be selected through the dropdown menus.
  - The language selected will be applied to entire OC.
  - You must associate a user with at least one account.
4. Click on the **Create** button at the lower-right corner of the pane.

### **NOTE**

On logging in, users cannot see or assign ACLs with a higher access level than their own.

If CA UIM has been installed to authenticate users using Login IDs, the Login ID, Password, and E-mail fields are mandatory. The Login ID must be a unique alphanumeric string, may contain periods, dashes, and underscore characters, but may not begin or end with a period. The email address must also be unique. The password must be at least six characters long.

If CA UIM has been installed to authenticate users using email addresses, the Login ID field must be a valid email address.

### **To edit user information:**

### **NOTE**

Users appear under each account they are assigned to. To edit a user account, you can select it from any account it is listed under.

1. Click on the **Edit** icon to the right of the user name.
2. Change the user information. You can edit the following fields:
  - **Password**
  - **ACL**
  - **Email**
  - **Name** (first and last)
  - **Language**
  - **Accounts**
3. Click on the **Update** button at the lower-right corner of the pane.

### **To delete a user:**

### **NOTE**

If you have users assigned to multiple accounts, the behavior for user deletion is dependent on the permissions assigned to the deleting user:

- **Bus Users**  
The user is deleted from **all accounts**.
- **Users with the Account Administration Permissions for ALL Accounts the User Belongs To**  
The user is deleted from **all accounts**.
- **Users with the Account Administration Permissions for SOME Accounts the User Belongs To**

The user is removed from the accounts visible to the user performing the deletion.

1. Select the account and find the user of interest.
2. Click on the **Delete** icon for that user.
3. Click **Yes** on the dialog box that appears.

### **Manage ACLs and LDAP in Account Admin**

You may sometimes need to give a unique set of permissions to an account contact user. To do so, you can change the permissions associated with the user's ACL or create a new ACL, define its permissions, and apply it to the user. Data visible to users with an ACL can be restricted by including alarm filters.

You may also want to associate an LDAP group with an ACL, giving all members of that group certain permissions within OC. LDAP groups can be given access to all account data or only data for a specific account.

A bus user with the Manage ACL permission can create, copy, edit, or delete ACLs.

In the Account Admin window, click the **ACLs & LDAP** tab at the top of the page to open the Edit ACL screen. The left-hand pane then displays the existing ACLs and the right-hand pane displays the permissions and other functions associated with the selected ACL.

### **Create a New ACL**

#### **Follow these steps:**

1. Click on the **New** button on the right of the left-hand pane.
2. Enter a name in the ACL Name field in the right-hand pane.
3. Click on the **Create** button in the lower-right corner of the screen.

### **Copy an Existing ACL**

#### **Follow these steps:**

1. Locate the name of an ACL in the left-hand pane.
2. Click on the **Copy** icon to the right of the name.
3. Enter the name of the new ACL on the right-hand pane.
4. Click on the **Create** button in the lower-right corner of the screen.

### **Delete an ACL**

#### **Follow these steps:**

1. Locate the name of an ACL in the left-hand pane.
2. Click on the **Delete** icon to the right of the name.
3. Click **Yes** in the dialog box that appears.

### **Edit an ACL**

The right-hand pane contains tabs for turning permissions on and off, defining alarm filters, and associating an LDAP group to an ACL and account. The header for the pane will change from Edit ACL to Copy ACL based on the operation being completed.

### **Properties**

The Properties window includes the ACL name and its permissions. On logging into Account Admin, a bus user will see all ACLs and their permissions. The user must have the **Manage ACL** permission to see and change permissions.

Permissions are sortable on any column: Permission, Type, and Access. In order to redefine permissions, all permissions can be assigned or deactivated, and selected permissions can be sorted to appear at the top of the list.

An ACL associated with one or more users cannot be deleted.

These restrictions become important if, for instance, someone is assigned the task of changing permissions for groups but does not have the Manage ACL permission.

#### Follow these steps:

1. Click on the ACL name of interest in the left-hand pane.
2. Click the box to the left of **Permissions** at the top of the permissions list to select and deselect all permissions.
3. Click on boxes to the left of individual permissions to turn them on or off.
4. Click on the **Permissions** header to sort the list of permissions.
5. If further changes are not needed, click on the **Update** button at the lower-right corner of the pane.

#### Alarm Filters

You can define alarm filters for each ACL.

You can use the following menus and buttons in the Account Admin view to filter alarms for the ACL currently selected:

| Field                                     | Description                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| and/or pull-down menu                     | Choose the <b>and</b> or <b>or</b> operator to apply to this row of the filter definition. This operator is present only in the second and subsequent rows.                                                                                                                                                              |
| menu(Blank)/not pull-down menu            | Choose <b>not</b> in order to search for all systems except those that meet this row of the filter definition. Otherwise, leave blank.                                                                                                                                                                                   |
| Criterion pull-down menu                  | Choose the criterion to filter for, such as <b>Severity</b> , <b>Hostname</b> , <b>Origin</b> , and so on.                                                                                                                                                                                                               |
| Operator pull-down menu                   | Choose the appropriate operator, such as <b>is</b> , <b>contains</b> , <b>starts with</b> , and so on.<br>If you select Severity, the following operators are available: = , <= , >=                                                                                                                                     |
| Text field/Alarm severity-level pull-down | Enter the appropriate text for the criterion you selected.<br>If you select Severity for the criterion, a pull-down menu listing alarm severity-levels is displayed. Choose from the following: <b>Clear</b> (0), <b>Informational</b> (1), <b>Warning</b> (2), <b>Minor</b> (3), <b>Major</b> (4), <b>Critical</b> (5). |
| Add Filter/Remove Filter icons            | Click to add or remove rows for the filter definition. The Add icon is at the top of the page; the Remove icon is in line with the condition.                                                                                                                                                                            |
| Dragger icons                             | Drag to move the row up or down. Filter rows are applied in sequential order.                                                                                                                                                                                                                                            |

#### LDAP

You can link an LDAP group to an ACL and specific accounts. LDAP must be enabled to use this feature; if it is not, the ACL tab title will be grayed out.

1. Select an ACL from the list in the left-hand pane.
2. Click on the **LDAP** tab in the right-hand pane.
3. If 50 or fewer LDAP groups exist, the drop-down list for **LDAP Group** is displayed in the right-hand pane. Select a group name from this drop-down list.

If more than 50 LDAP groups exist, no drop-down list will appear and you must enter the name of the LDAP group. The name must match an LDAP group name; an error will be displayed until the names match. If the LDAP group name or spelling is unknown, refer to the list of groups on the LDAP server and copy the name into the input field.

4. Select all accounts that apply under the **Account Link** field below the LDAP Group name. See details below on this field.
5. Click on the **Update** button at the bottom-right corner of the pane.

The LDAP group is now associated with the ACL in the left-hand pane and any selected accounts (if appropriate). Repeat the steps for each ACL to associate it with an LDAP group as needed.

The Account Link field associates an LDAP group with all selected accounts. If the Account Link field is left blank, members of the LDAP group can view data according to their permissions for all accounts. If accounts are specified in the Account Link field, LDAP group members will have permissions to view data for any of the accounts that were selected.

### **Additional Considerations for Users in Multiple Accounts**

#### **WARNING**

Admin Console does not currently support users in multiple accounts.

#### **NOTE**

Only bus users or account contact users in the Account Administrator ACL can edit the accounts that a user is in.

You can assign a user to more than one account in two ways: through the **Account** tab for an individual user and through the **ACLs & LDAP** tab for all users in an LDAP group.

#### **Follow these steps:**

1. Open the **Account Admin** page through the **Configuration** page.
2. Select an account under the **Accounts** tab.
3. Select a user in the right-hand pane and click on the **Edit** icon at the right.
4. Click on the box next to the name of the account(s) to be added under **Accounts**.

#### **OR**

1. Open the **Account Admin** page through the **Configuration** page.
2. Select the ACL for the user under the **ACLs & LDAP** tab.
3. Select the **LDAP** tab in the **Edit ACL** pane.
4. Click on the box next to the name of the account(s) to be added under **Accounts Link**.

A user can view data for any of the accounts to which he or she belongs. However, a user assigned to multiple accounts can only have one account active at a time. For example, a user may be assigned to the following accounts:

- Business\_One
- Business\_Two
- Business\_Three

When the user is logged into Business\_One, he or she will only see information for that account and no information specific to Business\_Two or Business\_Three. The name of the active account is displayed in the right-hand side of the dockbar.

To see information for the other accounts, the user must change accounts using one of the following methods:

- Specify the account during log in. For example, if the user wants to log in to their Business\_One account, their user name would be **Business\_One/User**.
- Add the **?account=** parameter to an OC URL. For example, if you wanted to view the Azure Unified Dashboard for Business\_One, the URL is **http://<oc\_IP>/user/<user\_name>/azure?account=Business\_One**.

**NOTE**

Using a URL with the **?account=** parameter only works when you are either logged out of OC or already logged in to the specified account.

## Types of Users

Two types of users exist in the CA Unified Infrastructure Management solution—*bus* users and *account contact* users. The permissions for both user types are set in the access control list (ACL). Administrators can create users of these two types to meet their security or multi-tenancy needs.

The following chart describes the key differences between bus users and account contact users.

| Bus Users                                           | Account Contact Users                                                                                 |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Managed in Admin Console or Infrastructure Manager. | Managed in the Account Admin view.                                                                    |
| Stored in the hub security file.                    | Stored in CM_ database tables.                                                                        |
| Can see all data, systems, and alarms within UIM.   | Can only see data, systems, and alarms with origins that match at least one of the account's origins. |
| Can access legacy Windows UIs.                      | Cannot access legacy Windows UIs.                                                                     |
| Can access the bus, callbacks, and messages.        | Cannot access the bus.                                                                                |

**NOTE**

An LDAP group configured for Bus specific ACLs is not recommended to map with Account Contact specific ACLs.

**NOTE**

All usernames for any type of users should be unique. Creating LDAP users, Bus users, and/or Account Contact users with identical usernames will create confusion about which credentials are being used to authenticate in OC.

**NOTE**

Always create the custom ACLs in OC and map the LDAP groups in it. If LDAP groups are configured at default ACLs in OC then Bus Admin users may behave like Account Contact users

## ACL Permissions List

| Permission             | Administrator | Guest | Operator | Superuser | Description                                                 |
|------------------------|---------------|-------|----------|-----------|-------------------------------------------------------------|
| Accept                 | Y             | -     | Y        | Y         | Assign alarms to yourself.                                  |
| Account Administration | Y             | -     | -        | Y         | Manage Account contacts and customize their portal content. |
| Acknowledge            | Y             | -     | Y        | Y         | Close alarms.                                               |
| Alarm Details          | Y             | Y     | Y        | Y         | General access to alarm lists and alarm details             |
| Alarm History          | Y             | -     | Y        | Y         | Transaction history and alarm queries.                      |

|                                          |   |   |   |   |                                                                                                                                                      |
|------------------------------------------|---|---|---|---|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alarm Management                         | Y | - | - | Y | Various alarm management features.                                                                                                                   |
| Alarm Summary                            | Y | Y | Y | Y | Display alarm summary information.                                                                                                                   |
| Archive Management                       | Y | - | - | Y | Create and modify packages.                                                                                                                          |
| Assign                                   | Y | - | - | Y | Assign alarms to another user.                                                                                                                       |
| Automation - View Items                  | Y | - | Y | Y | Unimplemented.                                                                                                                                       |
| Automation - Change configuration items  | Y | - | Y | Y | Unimplemented.                                                                                                                                       |
| Automation - Manage Workflows            | Y | - | Y | Y | Unimplemented.                                                                                                                                       |
| Automation - Create and Modify Workflows | Y | - | Y | Y | Unimplemented.                                                                                                                                       |
| Basic Management                         | Y | - | - | Y | Manage (create, read, update, delete) the monitoring infrastructure.                                                                                 |
| Change Password                          | Y | - | Y | Y | Contact can change own password.                                                                                                                     |
| Cloud UE Monitor                         | Y | - | Y | Y | Access to Cloud User Experience Monitor view.                                                                                                        |
| Custom Dashboards                        | Y | Y | Y | Y | Display custom dashboards.                                                                                                                           |
| Custom Reports                           | Y | Y | Y | Y | Display customer reports.                                                                                                                            |
| Dashboard Designer                       | Y | - | - | Y | Create, modify, and delete private dashboards.                                                                                                       |
| Default Customization                    | Y | - | - | Y | Customize default portal content for bus users.                                                                                                      |
| Discovery                                | - | - | - | Y | Discover and create template panels.<br><br><b>Note:</b> Only bus users with the Discovery Management permission in their ACL can perform discovery. |
| Discovery Management                     | - | - | - | Y | Set computer system properties.                                                                                                                      |

|                                 |   |   |   |   |                                                          |
|---------------------------------|---|---|---|---|----------------------------------------------------------|
| Discovery Pie                   | - | - | - | Y | Display discovery information,                           |
| Distribution                    | Y | - | - | Y | Distribute archive packages.                             |
| Dynamic Views                   | Y | - | Y | Y | Display Dynamic Views.                                   |
| Dynamic Views Dashboards        | Y | - | Y | Y | Display Dynamic Views dashboards.                        |
| Dynamic Views Reports           | Y | Y | Y | Y | Display Dynamic Views Reports.                           |
| Dynamic Views States            | Y | - | Y | Y | General access to Dynamic Views alarm state information. |
| Edit Maintenance Mode Devices   | Y | - | - | Y | General access to Dynamic Views alarm state information. |
| Edit Maintenance Mode Schedules | Y | - | - | Y | Create, edit and delete maintenance mode schedules.      |
| Edit URL Actions                | Y | - | Y | Y | General access to Dynamic Views alarm state information. |
| Execution Level1                | Y | - | - | Y | Probe Command Execution Level 1.                         |
| Execution Level2                | Y | - | - | Y | Probe Command Execution Level 2.                         |
| Execution Level3                | Y | - | - | Y | Probe Command Execution Level 3.                         |
| Extended Security               | Y | - | - | Y | Various security maintenance features.                   |
| Invisible Alarms                | - | - | - | Y | Show alarms that are set to be invisible.                |
| Launch URL Actions              | Y | - | Y | Y | Launch URL actions that are associated with alarms.      |



|                        |   |   |   |   |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|---|---|---|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| License Management     | Y | - | - | Y | Add and delete licenses. From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required). |
| List Designer          | Y | - | - | Y | Create, modify, and delete lists and groups.                                                                                                                                                                                                                                                                                                                                                                                     |
| List Viewer            | Y | - | Y | Y | View lists and groups.                                                                                                                                                                                                                                                                                                                                                                                                           |
| Maintenance Mode       | Y | - | - | Y | Robot maintenance mode management.                                                                                                                                                                                                                                                                                                                                                                                               |
| Manage ACL             | Y | - | - | Y | Create, modify, and delete ACLs.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Manage Profiles        | Y | - | - | Y | Create, rename, and delete user profiles.                                                                                                                                                                                                                                                                                                                                                                                        |
| Management Tools       | Y | - | - | Y | Various tools (find/connect, etc.).                                                                                                                                                                                                                                                                                                                                                                                              |
| Modify Profiles        | Y | - | - | Y | Modify and save user profiles.                                                                                                                                                                                                                                                                                                                                                                                                   |
| NetFlow                | Y | - | Y | Y | Access to NetFlow view.                                                                                                                                                                                                                                                                                                                                                                                                          |
| NetFlow Configuration  | Y | - | Y | Y | Allow view users to configure NetFlow probe settings.                                                                                                                                                                                                                                                                                                                                                                            |
| NFA Manage Reports     | Y | - | - | Y | Create, modify, delete, and execute reports.                                                                                                                                                                                                                                                                                                                                                                                     |
| NFA Run Reports        | Y | - | Y | Y | View and execute defined reports.                                                                                                                                                                                                                                                                                                                                                                                                |
| NFA View Conversations | Y | - | Y | Y | Allow users to see specific client conversations.                                                                                                                                                                                                                                                                                                                                                                                |
| NFA View Hosts         | Y | - | Y | Y | Allow users to see specific client host conversations.                                                                                                                                                                                                                                                                                                                                                                           |

|                                 |   |   |   |   |                                                                         |
|---------------------------------|---|---|---|---|-------------------------------------------------------------------------|
| NFA View Protocols              | Y | - | Y | Y | Allow users to see protocol information.                                |
| NFA View ToS                    | Y | - | Y | Y | Allow users to see the Type of Service information in applicable views. |
| OC Self Service ReadOnly Access | Y | - | Y | Y | Read-only view access for any self-service profiles.                    |
| Operator Console Basic          | Y | - | - | Y | Allows access to Operator Console view.                                 |
| Policy Basic                    | Y | - | - | Y | Read-only views of the policies.                                        |
| Policy Management               | Y | - | - | Y | Manage (create, read, update, change state and delete) the policies.    |
| Portal Administration           | Y | - | - | Y | Web portal admin access.                                                |
| Probe Basic                     | Y | - | Y | Y | Read-only view of the probe configuration.                              |
| Probe Configuration             | Y | - | - | Y | Probe configuration tool management.                                    |
| Probe Security                  | Y | - | - | Y | Manage probe security settings.                                         |
| Probe Template Basic            | Y | - | - | Y | Read-only views of probe templates.                                     |
| Probe Template Management       | Y | - | - | Y | Create, Modify, and delete probe templates.                             |
| Program Options                 | Y | - | - | Y | Change various program attributes.                                      |
| QoS Access                      | Y | - | Y | Y | Allow users to browse QoS series.                                       |
| Reassign                        | Y | - | - | Y | Override assignment at Assign/Acknowledge.                              |
| Report Designer                 | Y | - | - | Y | Create, modify, and delete reports.                                     |
| Report Scheduler                | Y | - | Y | Y | Access to ReportScheduler view.                                         |
| Restrict View to User Assets    | - | - | - | Y | Restrict dashboard views to account users.                              |
| Service Desk                    | Y | - | Y | Y | Access to Service Desk and My Tickets views.                            |

|                                                    |   |   |   |   |                                                             |
|----------------------------------------------------|---|---|---|---|-------------------------------------------------------------|
| SLM Admin                                          | Y | - | - | Y | Run Service Level Manager with full access.                 |
| SLM View                                           | Y | - | Y | Y | Run Service Level Manager in read-only mode.                |
| SLO Access                                         | Y | - | Y | Y | Allow view users to browse SLO data.                        |
| Unassign                                           | Y | - | - | Y | Unassign alarms.                                            |
| Unified Reports                                    | Y | - | - | Y | Access to Unified Reports.                                  |
| User Administration                                | Y | - | - | Y | Create, modify, and delete users.                           |
| User Customization                                 | Y | Y | Y | Y | Customize own portal content.                               |
| User Monitoring                                    | Y | - | - | Y | Display and disconnect user sessions.                       |
| OC Automatic Robot Installation                    | Y | - | Y | Y | Automatically deploy and install robots to targeted system. |
| OC Basic                                           | Y | Y | Y | Y | Access to OC view.                                          |
| OC Edit Monitoring Station Groups                  | Y | - | Y | Y | Create, edit, and delete monitoring station groups.         |
| OC Edit Monitoring Templates                       | Y | - | Y | Y | Create, edit, and delete monitoring templates.              |
| OC Geo View Modification                           | Y | - | Y | Y | Create, edit, and delete geo views.                         |
| OC Group Modification                              | Y | - | Y | Y | Create, edit, and delete groups.                            |
| OC Modify Individual Monitors for Computer Systems | Y | - | Y | Y | Create, modify, and delete individual SOC monitors.         |
| OC Modify Shared Alarm Filters                     | Y | - | Y | Y | Create, edit, and delete shared alarm filters.              |

|                                     |   |   |   |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|---|---|---|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OC Self Service ACL Based Only      | - | - | - | - | <p>Allow users to access only those profile templates that have appropriate ACLs assigned to them and users have access to those ACLs. Users can then access only those templates; they cannot view any other template.</p> <p>This permission overrides various other permissions (for example, viewing all the templates) that you might have. Therefore, we recommend that you review your scenario properly before you enable this permission.</p> |
| OC Monitoring Configuration Service | Y | - | Y | Y | Enable or disable out-of-box monitoring template.                                                                                                                                                                                                                                                                                                                                                                                                      |
| OC Self Service Monitoring          | Y | - | Y | Y | Function that is assumed by OC Monitoring Configuration Service.                                                                                                                                                                                                                                                                                                                                                                                       |
| Web Publish                         | - | - | - | Y | CA UIM Server HTML management.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Web Service                         | Y | - | - | Y | Access to CA UIM Web Service API.                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Permissions Reference for OC Features

To access the Operator Console (OC) features, users must have the appropriate permissions set in the Access Control List (ACL). ACL permissions are set in the Account Admin view. A "permission denied" message is displayed when users try to access a feature for which they do not have the required permission.

### Contents

#### NOTE

The SLM does not allow access to account contact users, regardless of permissions set.

### Account Admin

#### Required Permission for Access:

- Account Administration

---

**Other Available Permissions:**

- Manage ACL - create, modify, and delete ACLs.

**Change Password****Required Permission for Access:**

- Change Password

**NOTE**

In addition to having the Change Password permission set in the ACL, the user must be an account contact user in order to access this feature.

**Dashboard****Required Permission for Access:**

- Dashboard Design - allows bus users to create, edit, and publish dashboards

**NOTE**

By default, account contact users have read-only access to the Dashboard view. If an ACL with the Dashboard Design permission is assigned to an account contact user, it is not honored for the account contact user.

## Discovery Status

**Required Permission for Access:**

- Discovery Pie

**NetFlow****Required Permission for Access:**

- Netflow

**SLA Reports****Required Permission for Access:**

- SLM View

**SLM****Required Permission for Access:**

- SLM Admin

## Start, Stop, or Uninstall a Robot (Command Line)

This topic provides the commands to stop, start, or remove a robot. The information is organized by Operating System.

**Contents**

**Windows**

| Action | Command                                        |
|--------|------------------------------------------------|
| Start  | C:\Program Files\nimsoft\bin\nimbus.exe -start |
| Stop   | C:\Program Files\nimsoft\bin\nimbus.exe -stop  |
| Remove | C:\Program Files\nimsoft\unistall.exe          |

**AIX**

| Action | Command                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start  | /usr/bin/startsrc -s nimbus                                                                                                                                                                                                                                                                                                                                                                             |
| Stop   | /usr/bin/stopsrc -s nimbus                                                                                                                                                                                                                                                                                                                                                                              |
| Remove | <pre>rmmdir -rf /opt/nimsoft rmssys -s nimbus rmssys -s nimsh</pre> <p><b>Note:</b> rpm -e nimsoft-robot removes the robot rpm. Use this command if the robot was installed using ADE.</p> <p><b>Note:</b> rmmdir -rf /opt/nimsoft removes the associated robot files and directories.</p> <p><b>Note:</b> Use rmssys -s nimbus nimsh to ensure that the service (subsystem) is completely removed.</p> |

**Debian Linux**

| Action  | Command                         |
|---------|---------------------------------|
| Confirm | dpkg-query -s nimsoft-robot     |
| Start   | /etc/init.d/nimbus start        |
| Stop    | /etc/init.d/nimbus stop         |
| Remove  | (sudo)<br>dpkg -r nimsoft-robot |

**HP-UX**

| Action  | Command                                                             |
|---------|---------------------------------------------------------------------|
| Confirm | swverify -v controller                                              |
| Start   | /opt/nimsoft/bin/niminit start<br>(or)<br>/sbin/init.d/nimbus start |
| Stop    | /opt/nimsoft/bin/niminit stop<br>(or)<br>/sbin/init.d/nimbus stop   |

|        |                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remove | <pre>/opt/nimsoft/bin/niminit stop swremove controller rm -rf /opt/nimsoft</pre> <p><b>Note:</b> <code>rm -rf /opt/nimsoft</code> removes the robot files and directories.</p> |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Linux - RC-compatible

(RHEL 5.x and prior, CentOS 5.x and prior, SUSE, Debian)

| Action   | Command                                                                          |
|----------|----------------------------------------------------------------------------------|
| Confirm* | <code>rpm -q nimsoft-robot</code>                                                |
| Start    | <code>/etc/init.d/nimbus start</code>                                            |
| Stop     | <code>/etc/init.d/nimbus stop</code>                                             |
| Remove*  | <code>rpm -e RPM_package</code><br>( <i>RPM_package</i> = robot name minus .rpm) |

#### **NOTE**

Confirm and Remove instructions apply to robots installed by ADE.

If you installed the robot with `nimldr`, no rpm packages are installed, so the confirm and remove steps do not apply.

To remove a robot installed by `nimldr`:

- `/opt/Nimsoft/bin/niminit stop`
- `/opt/Nimsoft/bin/inst_init.sh remove`
- `cd /opt/`
- `rm -rf Nimsoft`

### Linux - Upstart Method

(RHEL 6.0 and newer, CentOS and newer, Ubuntu)

#### **NOTE**

If you want to use the Upstart `initctl` function, you must write your own `nimbus.conf` script.

| Action   | Command                                                                          |
|----------|----------------------------------------------------------------------------------|
| Confirm* | <code>rpm -q nimsoft-robot</code>                                                |
| Start    | <code>initctl start nimbus</code>                                                |
| Stop     | <code>initctl stop nimbus</code>                                                 |
| Remove*  | <code>rpm -e RPM_package</code><br>( <i>RPM_package</i> = robot name minus .rpm) |

#### **NOTE**

Confirm and Remove instructions apply to robots installed by ADE.

If you installed the robot with `nimldr`, no rpm packages are installed, so the confirm and remove steps do not apply.

To remove a robot installed by nimldr:

- `/opt/Nimsoft/bin/niminit stop`
- `/opt/Nimsoft/bin/inst_init.sh remove`
- `cd /opt/`
- `rm -rf Nimsoft`

## Solaris

| Action  | Command                                                          |
|---------|------------------------------------------------------------------|
| Confirm | <code>pkginfo nimsoft-robot</code>                               |
| Start   | <code>/etc/init.d/nimbus start</code>                            |
| Stop    | <code>/etc/init.d/nimbus stop</code>                             |
| Remove  | <code>(sudo or su -c)</code><br><code>pkgrm nimsoft-robot</code> |

## Ubuntu Linux

| Action  | Command                                                                  |
|---------|--------------------------------------------------------------------------|
| Confirm | <code>dpkg -query -s nimsoft-robot</code>                                |
| Start   | <code>(sudo, su -c, or root)</code><br><code>initctl start nimbus</code> |
| Stop    | <code>(sudo, su -c, or root)</code><br><code>initctl stop nimbus</code>  |
| Remove  | <code>(sudo)</code><br><code>dpkg -r nimsoft-robot</code>                |

## Hub Information

A hub is a robot that has additional responsibilities. Just as a robot manages probes, a hub manages robots. Every deployment has one or more hubs. All hubs perform these tasks:

- **Collect all messages** coming from the robots
- **Quickly dispatch the messages** to connected subscribers and/or queues
- **Maintain system information**, such as name-tables

Hubs have the following designations depending on their purpose:

- The **Primary Hub** communicates with the database. Every deployment has one, and only one, primary hub. This hub is created when you install the CA UIM server software.
- **Secondary hubs** can be used to scan the network (device discovery), perform baseline calculations on QoS metrics, or group robots according to function, geographical location, departmental code, or other criteria. Although secondary hubs are optional, almost all deployments have them. Secondary hubs are created after the UIM server software is installed. They can be created or removed as needed to meet the needs of your IT environment.
- A **failover hub** is a secondary hub that performs the primary hub's actions if the primary hub changes state (becomes unavailable).
- **Tunnel hubs** use VPN-like connections to communicate through firewalls.

For information about managing and configuring hubs, refer to the [hub](#) documentation on the Probes Documentation Space.



## Move the UIM Database (MS SQL Server)

You can move the UIM database from one SQL server to another.

### Follow these steps:

1. Log in to Admin Console.
2. Deactivate any probes that directly access the UIM database, these probes include:
  - ace
  - alarm\_enrichment
  - baseline\_engine
  - data\_engine
  - discovery\_server
  - maintenance\_mode
  - nas
  - nis\_server
  - prediction\_engine
  - sla\_engine
  - udm\_manager
  - trellis
3. Using the SQL Server Enterprise Manager or SQL Server Management Studio for SQL server 2005/2008, detach the database from the existing database server.
4. Move the database files (.mdf) and the log file (.ldf) to the new location or new database server.
5. Using the SQL Server Enterprise Manager or Management Studio, reattach the database from the new location to the database server or the new database server.
6. Open the data\_engine probe configuration GUI, select the Database Configuration folder.
7. Change the Data Source, User ID, and password to match the new database settings.
8. Activate the data\_engine, and then any other probes that you deactivated.

## Run Probe Commands from a Command Prompt

Use the **Probe Utility (pu)** command to run probe commands from a command prompt. This utility is useful for running scripts to complete repetitive tasks (such as deleting multiple probes or multiple instances of a probe) or to avoid navigating through multiple levels of a user interface to complete an action. You must have a valid username and password to run commands.

### NOTE

PU is shipped as a separate package you install from the archive.

The command has the following format:

```
$UIM_HOME/bin/pu -u <username> -p <password> <options> <nim_address> <probe command> <data>
```

- **-u <username>** - The UIM user name
- **-p <password>** - The UIM password
- **<nim\_address>** - The UIM address of the probe in the form */domain/hub/robot/probe*
- **<probe command>** - The command to execute

The following example executes the **get\_info** command on the CDM Probe at */Dev\_domain/Dev\_hub/Dev\_robot*. The user name is *rune*, and the password is *1234admin*.

```
$UIM_HOME/bin/pu -u rune -p 1234admin /Dev_domain/Dev_hub/Dev_robot/cdm get_info
```

## List Commands Available for a Probe

The commands available for a probe differ for each probe. Use the pu command to list the commands available for a probe.

```
$UIM_HOME/bin/pu -u <username> -p <password> </domain/hub/robot/probe>
```

The controller probe contains many commands to control other probes. To list the commands that are available from the controller probe:

```
$UIM_HOME/bin/pu -u <username> -p <password> /Dev_domain/Dev_hub/Dev_robot/controller
```

A partial example of the return:

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Nimsoft\bin>pu.exe -u administrator -p ***** /Dev_domain/Dev_hub/
Dev_robot/controller
Nov 8 17:06:18:278 pu: SSL - init: mode=0, cipher=DEFAULT, context=OK
Nov 8 17:06:18:279 pu: nimCharsetSet() - charset=
=====
Address: /Dev_domain/Dev_hub/Dev_robot/controller Request: _command
=====
_status PDS_PCH 9 detail%d
_command PDS_PCH 9 detail%d
_debug PDS_PCH 40 level%d,trunc_size%d,trunc_time%d,now%d

~

_stop PDS_PCH 0 NULL
_restart PDS_PCH 0 NULL
checkin PDS_PCH 14 hubaddr,hubip
probe_checkin PDS_PCH 7 type%d
iptoname PDS_PCH 10 ip,port%d
nametoip PDS_PCH 5 name
login PDS_PCH 7 type%d
verify_login PDS_PCH 0 NULL
change_password PDS_PCH 0 NULL
probe_list PDS_PCH 11 name,robot
probe_register PDS_PCH 113 name,active,type,timespec,command,arguments,
workdir,config,datafile,logfile,description,group,fail_window,realip

~

probe_unregister PDS_PCH 15 name,noforce%d
probe_activate PDS_PCH 5 name
probe_deactivate PDS_PCH 29 name,noforce%d,waitforstop%d
probe_store PDS_PCH 9 filename
probe_config_lock PDS_PCH 31 name,locktype%d,lockid%d,robot

~

probe_config_lock_list PDS_PCH 5 name
```

```

probe_config_get PDS_PCH 15 name,robot,var
probe_config_set PDS_PCH 38 name,section,key,value,lockid%d,robot

~

probe_set_port PDS_PCH 18 name,port%d,pid%d
probe_start PDS_PCH 5 name
probe_stop PDS_PCH 5 name
probe_change_par PDS_PCH 15 name,par,value
probe_tail_logfile PDS_PCH 26 name,size%d,prev_record%d
probe_tail_logfile_session PDS_PCH 31 name,max_buffer%d,from_start%d

...

```

### Set a Key-Value Pair

You can use the `pu` command to set probe key-value pairs. Use the following command format to set a key-value pair for a probe.

```

$UIM_HOME/bin/pu -u <username> -
p <password> controller probe_config_set <probe name> <config file section> <key> <value> lockid = "" <robot>

```

- **-u <username>** - The UIM user name
- **-p <password>** - The UIM password
- **<probe name>** - The name of the probe
- **<config file section>** - The fully qualified name of the configuration section, for example, `/auto_operator/definitions/Email`
- **<key>** - The key to change
- **<value>** - The new value for the key
- **<robot>** - The fully qualified name of the robot controlling the probe, for example, `/my_domain/my_hub/my_robot`

#### WARNING

Reread the probe configuration file for changes to take effect.

The following example updates the **active** value to **yes** for the auto-operator that is named **methodName** in the `nas` configuration file.

```

$UIM_HOME/bin/pu -u administrator -p password controller probe_config_set nas /
auto_operator/definitions/methodName active yes "" /Dev_domain/Dev_hub/Dev_robot

```

Reread the `nas` configuration file using the **\_restart** command.

```

$UIM_HOME/bin/pu -u administrator -p password /Dev_domain/Dev_hub/Dev_robot/nas _restart

```

Commands return a completion message for actions as appropriate.

## Set Up Automated Usage Metering and Billing

*Automated Usage Metering and Billing* is an automated billing process for customers who have:

- Licenses based on quantity and minimum commitment (Min-Commit) subscriptions, or
- Non-subscription contracts that require periodic auditing for renewals

**NOTE**

From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).

For more information about usage metering and billing, see the article [Set Up Automated Usage Metering and Billing](#) on the Probes Documentation Space.

## Robot Commands for the IBM System i Computer

**Contents:**

Use the following commands to manage a robot on an IBM System i computer:

**Start the Robot**

Start the robot with the following command:

```
STRSBS SBS (NIMBUS/NIMBUS)
```

**Stop the Robot**

Stop the Robot with the following command:

```
ENDSBS SBS (NIMBUS)
```

**Create a Schedule**

You can create a schedule that will stop or start a robot automatically with the following command:

```
ADDJOBSCDE JOB (NIMBUS_END) CMD (ENDSBS SBS (NIMBUS) DELAY (120)) FRQ (*WEEKLY) SCDDATE (*NONE) SCDDAY (*ALL)
SCDTIME (010000) USER (NIMBUS) TEXT ('End Nimbus subsystem')
```

The following example creates a schedule that automatically stops the robot at 1am, and starts it again at 7am daily:

```
ADDJOBSCDE JOB (NIMBUS_STR) CMD (STRSBS SBS (NIMBUS/NIMBUS)) FRQ (*WEEKLY) SCDDATE (*NONE) SCDDAY (*ALL)
SCDTIME (070000) USER (NIMBUS) TEXT ('Start Nimbus subsystem')
```

**Change a Schedule**

To change a schedule that has already been created, use the following command:

```
WRKJOBSCDE JOB (NIMBUS*)
```

## Enable Sub-Tenancy

You can enable or disable access for multiple users to the resources based on an origin using REST APIs (*contact\_origins*). As an MSP administrator, you can globally modify the user-origin association of existing or new users by mapping them to specific origins for a Tenant. By default, when you add a user to an account, they do not have access to any resources, such as Alarm Viewer, OC Dashboards, until you enable the pre-provisioned white list of the origins for them. You can enable multiple origins for multiple UIM contact users and LDAP users. This feature is supported when

you enable `contact_origins_enabled` flag on the wasp probe raw configuration on the primary hub and the OC(if the OC is deployed on a separate server).

Imagine you are an MSP selling software to various customers. As an MSP, you provide ensure for the software and also support your customers with setting up the software and performing various optimizations. You (the MSP) become a CA UIM customer and your customers become Subtenants. Based on the nature of the customer's business, you (MSP) offer various services like online support, predictive maintenance, and remote performance optimization. You are able to view the collected data for the software while they are residing at the customers environment. You can offer various resources to the customers (Subtenants) like Performance Reports, Alarm Viewing, and Dashboards among others to optimize their business.

## Contents:

### Prerequisites

The following requirements exist:

- CA UIM 9.0.2 (or later)
- Deploy the uimapi-20.3 package on the primary hub robot in your CA UIM 20.3.0 environment. For more information, see [Deploy the uimapi Package](#).

#### **NOTE**

Do not deploy the package on the CABI robots.

- Ensure that the Account Administration privileges are available to the user to update origins to users.
- Create or identify the users that you want to map to specific origins. For more information, see [Add or Modify Users with Account Admin](#).
- Ensure that the LDAP setup is available if you are mapping the LDAP users to an origin. For more information, see [Add or Modify Users with Account Admin](#).

### Enable Sub-Tenancy

#### **WARNING**

If you enable sub-tenancy without mapping the users to one or more origins, **all** the users fail to log in to the OC server unless either the users are mapped to the origins or you disable the feature. To allow the users to log in to the OC server, you **must** complete all the steps in the following procedure. To disable sub-tenancy, follow the procedure [Disable Sub-Tenancy](#).

### Step 1: Enable the Sub-tenancy Feature

#### **NOTE**

The OC server and the primary Hub can be on the same server. If the OC and primary Hub are deployed on different servers, then perform this procedure on both the servers.

#### **Follow these steps:**

1. On the OC server, navigate to **Hub, Robot, Probes**, and open the **Raw Configure** page for the **wasp** probe.
2. Select **setup** to view the configuration sections.

Raw Configure: wasp

🔍 🏠 / setup

| setup Sections  | Key                     | Value                                                               |
|-----------------|-------------------------|---------------------------------------------------------------------|
| http_connector  | ajp_max_threads         | 250                                                                 |
| https_connector | ajp_port                | 8009                                                                |
| log             | connection              | yCFxFyqpvcH3i/FusH8MXZKmGlrBkOLZHNW0VIRf66vyCrDxamfeLy0ckeSMYR0tFyX |
|                 | contact_origins_enabled | false                                                               |
|                 | data_engine             | data_engine                                                         |
|                 | dbcp_max_active         | 100                                                                 |
|                 | dbcp_max_idle           | 5                                                                   |
|                 | dbcp_max_wait           | 10000                                                               |
|                 | http_max_threads        | 500                                                                 |
|                 | http_port               | 80                                                                  |
|                 | https_ciphers           | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256  |

CANCEL UPDATE

3. Select the option **Edit value** for the *contact\_origins\_enabled* parameter.

|   |                         |             |
|---|-------------------------|-------------|
| ⋮ | contact_origins_enabled | false       |
| ✎ |                         | data_engine |
| 🗑 |                         | 100         |

4. Define the value of the parameter as *true* to enable the sub-tenancy option and select **UPDATE**.

**Edit Key/Value**

Key

Value

CANCEL UPDATE

5. Select **UPDATE** on the **Raw Configure** page to save the changes to the server.

6. Set the **contact\_origins\_enabled** parameter to **true** on the remaining OC servers and wherever the adminconsoleapp package is deployed.
7. Restart **wasp** on all the servers running OC and Administration Console.
8. Access the REST client and verify that the API endpoints appear in the list.  
For example, use the following URL:

`http://<<hostname>>:<<port>>/uimapi/docs/index.html#/contact_origins`

## Step 2: Create or Edit Users

Create or edit users, associate the origins to the accounts, and define the ACLs.

### NOTE

The character limit for loginName is 64 characters and for origin is 255 characters.

### Follow these steps:

1. As the MSP administrator, log into OC and navigate to **Settings** -> **Account Admin**.
2. Create or edit the existing user, as required. For more information, see [Add or Modify Users with Account Admin](#).

The screenshot shows the 'Account Admin' page in the CA Unified Infrastructure Management (UIM) console. The breadcrumb navigation is 'Home > Settings > Account Admin'. The page title is 'Accounts ACLs & LDAP'. On the left, there is a sidebar with a list of account types: Employee, Healthcare, HR, Infrastructure, IT, and Security. The 'Employee' account is selected, and the 'Edit User' form is displayed on the right. The form fields include: Login ID (user1), Password (\*\*\*\*\*), ACL (Guest), Account (Employee), E-mail (user@user.com), First Name (user), Last Name (user), and Language (English (United States)).

Edit account details, if necessary.

The screenshot shows the 'Account Admin' page in the CA Unified Infrastructure Management (UIM) console. The breadcrumb navigation is 'Home > Settings > Account Admin'. The page title is 'Accounts ACLs & LDAP'. On the left, there is a sidebar with a list of account types: Employee, Healthcare, HR, Infrastructure, IT, and Security. The 'HR' account is selected, and the 'Edit Account' form is displayed on the right. The form fields include: Account Name (HR), Description (HR Account), and Ownership (origin) with a list of checkboxes: DDW12VM2\_hub, lvnqa012407\_hub (checked), lvnqa012408, and myOrigin.

**NOTE**

As there is no user-origin mapping, the login to the OC server fails.

**Step 3: Map Users to Origins**

Map each user or users to one or more required origins by using the REST client.

**Follow these steps:**

1. Open the REST client using the following URL:

```
http://<<hostname>>:<<port>>/uimapi/docs/index.html#/contact_origins
```

2. For each user or users, using the POST (addorigins) API, define the number of origins that they are entitled to. For example, you want to add contact users *acme\_user1*, *acme\_user2*, to the origins *win2k12-m-sh03* and *win2k12-m-ph\_hub*, define the following parameters:

- a. In **body**, define the user in **loginName** parameter and the list of accounts in **origin**.

```
[
 {
 "loginName": "acme_user1",
 "origin": [
 "win2k12-m-sh03", "win2k12-m-ph_hub"
]
 },
 {
 "loginName": "acme_user2",
 "origin": [
 "win2k12-m-sh03", "win2k12-m-ph_hub"
]
 }
]
```

- b. In **Parameter content type**, select *application/json*.
- c. Select **Try it out** to execute the query.
- d. In **Response Body**, verify that the origins are returned in the response.

The following response indicates that for the user *acme\_user1* and *acme\_user2*, the association with *win2k12-m-ph\_hub* and *win2k12-m-sh03* origins is available.

```
[
 {
 "loginName": "acme_user1",
 "origin": [
 "win2k12-m-ph_hub", "win2k12-m-sh03"
]
 },
 {
 "loginName": "acme_user2",
 "origin": [
 "win2k12-m-ph_hub", "win2k12-m-sh03",
]
 }
]
```

3. Using the GET API, verify that the users and origins are associated.
  - a. In **loginname**, define the userID. For example, define *acme\_user1*.



GET /contact\_origins/{loginname} Returns contactorigins config

**Implementation Notes**  
 Authorized users are:  
 -Account contact users  
 -Bus Users

**Response Class (Status 200)**  
 Success

Model | Model Schema

```

{
 "login_name": "string",
 "origin": [
 "string"
]
}

```

Response Content Type: application/xml

| Parameter | Value      | Description       | Parameter Type | Data Type |
|-----------|------------|-------------------|----------------|-----------|
| loginname | acme_user1 | contact loginname | path           | string    |

**Response Messages**

| HTTP Status Code | Reason                                                  | Response Model |
|------------------|---------------------------------------------------------|----------------|
| 401              | Insufficient privilege for specified contact loginname. |                |
| 404              | Loginname does not exist.                               |                |
| 500              | Unexpected Internal Error.                              |                |

- b. In **Response content type**, select *application/json*.
- c. Select **Try it out** to execute the query.
- d. In **Response Body**, verify that the origins are returned in the response.

```

{
 "loginName": "acme_user1",
 "origin": [
 "win2k12-m-ph_hub", "win2k12-m-sh03"
]
}

```

4. Using the POST API getcontactorigins, verify that the users and origins are associated.
  - a. In **body**, define the login names. For example, define ["acme\_user1","acme\_user2"].

**contact\_origins**

POST /contact\_origins/addorigins Show/Hide | Li

DELETE /contact\_origins/deletecontactorigins Remove list of origins for multiple con

POST /contact\_origins/getcontactorigins Returns list of ori

**Implementation Notes**  
 Authorized users are:  
 -Account contact users  
 -Bus Users

**Response Class (Status 200)**  
 Success

Model | Model Schema

```
[
 {
 "login_name": "string",
 "origin": [
 "string"
]
 }
]
```

Response Content Type: application/json

**Parameters**

| Parameter | Value                        | Description                                           | Parameter Type | Data Type     |
|-----------|------------------------------|-------------------------------------------------------|----------------|---------------|
| body      | ["acme_user1", "acme_user2"] | contact loginnames payload containing loginnames list | body           | Array[string] |

Parameter content type: application/json

**Response Messages**

| HTTP Status Code | Reason                           | Response Model |
|------------------|----------------------------------|----------------|
| 400              | Loginname array can not be empty |                |
| 500              | Unexpected Internal Error.       |                |

Try it out! [Hide Response](#)

- b. In **Response content type**, select *application/json*.
- c. Select **Try it out** to execute the query.
- d. In **Response Body**, verify that the origins are returned in the response.

```
[
 {
 "loginName": "acme_user1",
 "origin": [
 "win2k12-m-ph_hub", "win2k12-m-sh03"
]
 },
 {
 "loginName": "acme_user2",
 "origin": [
 "win2k12-m-ph_hub", "win2k12-m-sh03",
]
 }
]
```

**Step 4: Verify the Configuration**

**Follow these steps:**

1. In OC, navigate to the Alarms view and verify that the user (acme\_user1) has access to the origins that they are mapped to in the steps above.

Filter Results 6 Show Historical

**Alarm By Severity**

**Alarm By Probes**

**Top Alarming**

| Host                                | Count |
|-------------------------------------|-------|
| nicholas-vm01.dhcp.broadcom.net     | 2     |
| one-129-aiops.dhcp.broadcom.net     | 1     |
| ss642021-centvm01.dhcp.broadcom.net | 1     |
| svstemrh1-node2.dhcp.broadcom.net   | 1     |

| <input type="checkbox"/> |  | Device ...         | Actions | Alarm T... | Owner      | Alarm Message                         | Duration  | Probe | Origin           |
|--------------------------|--|--------------------|---------|------------|------------|---------------------------------------|-----------|-------|------------------|
| <input type="checkbox"/> |  | ss642021-centv...  | ⋮       | Memory     | Unassigned | Memory usage 15% is at or above th... | 17 hours  | rsp   | lvnqa0124_Origin |
| <input type="checkbox"/> |  | systemrh1-node...  | ⋮       | Memory     | Unassigned | Memory usage 37% is at or above th... | 14 hours  | rsp   | lvnqa012407_hub  |
| <input type="checkbox"/> |  | one-129-aiops.d... | ⋮       | Memory     | Unassigned | Memory usage 10% is at or above th... | an hour   | rsp   | lvnqa012407_hub  |
| <input type="checkbox"/> |  | Nicholas-vm01      | ⋮       | Memory     | Unassigned | Memory usage 29% is at or above th... | 10 hours  | rsp   | lvnqa012407_hub  |
| <input type="checkbox"/> |  | Nicholas-vm01      | ⋮       | CPU        | Unassigned | Paging data not currently available   | 10 hours  | rsp   | lvnqa012407_hub  |
| <input type="checkbox"/> |  | dm672442-cento...  | ⋮       | Host       | Unassigned | Connection to dm672442-centos02.d...  | 2 minutes | rsp   | lvnqa012407_hub  |

**NOTE**

If the Origin column is not visible by default, navigate to **Actions, Edit Columns**, and then select **Origin**.

**Supported API Functions**

| API Name                                     | Description                                                |
|----------------------------------------------|------------------------------------------------------------|
| POST /contact_origins/addorigins             | Adds the list of origins for multiple contact login names. |
| DELETE /contact_origins/deletecontactorigins | Removes list of origins for multiple contact login names.  |
| POST /contact_origins/getcontactorigins      | Returns list of origins for multiple contact login names.  |
| POST /contact_origins/removeorigins          | Removes list of origins for the contact login name.        |
| POST /contact_origins/setorigins             | Sets list of origins for the contact login name.           |
| DELETE /contact_origins/{loginname}          | Removes the list of origins for the contact login name.    |

|                                  |                                                                                      |
|----------------------------------|--------------------------------------------------------------------------------------|
| GET /contact_origins/{loginname} | Returns the contact origins that are configured for the provided contact login name. |
|----------------------------------|--------------------------------------------------------------------------------------|

| API Name                                     | Request URL                                                     | Parameter                                                                                             | Response                                                                                                                                                                                                         |
|----------------------------------------------|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /contact_origins/addorigins             | http://<uim_server>/uimapi/contact_origins/addorigins           | login name (specify the username)<br>origins (specify the list of origins to associate with the user) | [<br>{<br>"loginName": "acme_user1",<br>"origin": [<br>"win2k12-m-ph_hub", "win2k12-m-sh03"<br>]<br>},<br>{<br>"loginName": "acme_user2",<br>"origin": [<br>"win2k12-m-ph_hub", "win2k12-m-sh03",<br>]<br>}<br>] |
| DELETE /contact_origins/deletecontactorigins | http://<uim_server>/uimapi/contact_origins/deletecontactorigins | login name (specify the usernames for which you want to delete the corresponding origins)             | No content                                                                                                                                                                                                       |
| POST /contact_origins/getcontactorigins      | http://<uim_server>/uimapi/contact_origins/getcontactorigins    | login name (specify the usernames for which you want to retrieve the corresponding origins)           | [<br>{<br>"loginName": "acme_user1",<br>"origin": [<br>"win2k12-m-ph_hub", "win2k12-m-sh03"<br>]<br>},<br>{<br>"loginName": "acme_user2",<br>"origin": [<br>"win2k12-m-ph_hub", "win2k12-m-sh03",<br>]<br>}<br>] |

|                                         |                                                                  |                                                                                                                                                                      |                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /contact_origins/<br>removeorigins | http://<uim_server>/<br>uimapi/contact_origins/<br>removeorigins | login name (specify the<br>username for which you want to<br>remove the origins)<br>origins (specify the list of origins<br>that you want to remove for the<br>user) | <pre>{   "Message": "Success",   "ContactOrigins": [] } {   "Message": "Partial success,   Login name does not exist in DB   for these contacts",   "ContactOrigins":   [ { "loginName": "acme_user1",     "origin": [] },     { "loginName": "acme_user2",     "origin": []   }   ] }</pre> |
| POST /contact_origins/<br>setorigins    | http://<uim_server>/<br>uimapi/contact_origins/<br>setorigins    | login name (specify the<br>username)<br>origins (specify the list of origins<br>that you want to set for the user;<br>this replaces any previously set<br>origins)   | <pre>[   {     "loginName": "acme_user1",     "origin": [       "win2k12-m-       ph_hub", "win2k12-m-sh03"     ]   },   {     "loginName": "acme_user2",     "origin": [       "win2k12-m-ph_hub",     ]   } ]</pre>                                                                        |
| DELETE /contact_origins/<br>{loginname} | http://<uim_server>/<br>uimapi/contact_origins/<br>User1         | login name (specify the<br>username for which you want<br>to delete the corresponding<br>origins)                                                                    | No content                                                                                                                                                                                                                                                                                   |
| GET /contact_origins/<br>{loginname}    | http://<uim_server>/<br>uimapi/contact_origins/<br>User1         | login name (specify the<br>username for which you want<br>to retrieve the corresponding<br>origins)                                                                  | <pre>{   "loginName": "acme_user1",   "origin": [ "win2k12-m-   ph_hub", "win2k12-m-sh03"   ] }</pre>                                                                                                                                                                                        |

### **Disable Sub-Tenancy**

You can disable the **contact\_origins\_enabled** option and can revert to the initial state where the users can view all the devices and other resources that are associated with the account. When you disable, all the previously configured contact origins are cleared from the system. The data on OC for the user is not honored based on corresponding origin association.

#### **Follow the steps:**

1. As an administrator, log into the Administration Console.
2. Disable the sub-tenancy feature:
  - a. On the OC server, navigate to **Hub, Robot, Probes**, and open the **Raw Configure** page for the *wasp* probe.

- b. Select **setup** to view the configuration sections.

Raw Configure: wasp

🔍 🏠 / setup

| setup Sections  | + | Key                   | Value                                                                                 | + |
|-----------------|---|-----------------------|---------------------------------------------------------------------------------------|---|
| http_connector  | ⋮ | ajp_max_threads       | 250                                                                                   |   |
| https_connector | ⋮ | ajp_port              | 8009                                                                                  |   |
| log             | ⋮ | connection            | yCFxFyqqpvcH3i/FusH8MXZKmGlrBkOLZHNW0VIRf66vyocrDxamfeLy0cKeSMYR0tFyXRWWw/Mtoe3M/9... |   |
|                 | ⋮ | contact_origins_en... | true                                                                                  |   |
|                 | ⋮ | data_engine           | data_engine                                                                           |   |
|                 | ⋮ | dbcp_max_active       | 100                                                                                   |   |
|                 | ⋮ | dbcp_max_idle         | 5                                                                                     |   |
|                 | ⋮ | dbcp_max_wait         | 10000                                                                                 |   |
|                 | ⋮ | http_max_threads      | 500                                                                                   |   |
|                 | ⋮ | http_port             | 80                                                                                    |   |
|                 | ⋮ | https_ciphers         | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS...  |   |

CANCEL UPDATE

- c. Select the option **Edit value** for the *contact\_origins\_enabled* parameter.

|   |                         |      |
|---|-------------------------|------|
| ⋮ | contact_origins_enabled | true |
| ✎ | Edit value              |      |
| 🗑 | Delete key              |      |
|   | data_engine             |      |
|   | dbcp_max_active         | 100  |

- d. Define the value of the parameter as *false* to disable the sub-tenancy option and select **UPDATE**.

**Edit Key/Value**

Key

Value

CANCEL UPDATE

- e. Select **UPDATE** on the **Raw Configure** page to save the changes to the server.

- f. Set the **contact\_origins\_enabled** parameter to **false** on the primary Hub and the remaining OC servers and wherever the `adminconsoleapp` package is deployed.
3. Restart **wasp** on all the OC servers and Admin Console.

## Configure Telemetry for the PLA Model

Telemetry is a foundational element of the Enterprise Software Portfolio License Agreement (PLA) model. The initial requirement of the Telemetry effort is to collect and report product-specific usage daily in support of the new consumption model. Broadcom uses its own endpoint to support the Enterprise Software Telemetry rollout. This endpoint provides a centralized platform for the collection and routing of usage data through various pre-built integrations and destinations.

It is mandatory for a customer under Enterprise Software PLA to enable telemetry and share the usage data. This article describes how to enable telemetry and route the usage data to Broadcom.

### Contents:

#### Data Collected by Telemetry

Telemetry collects two types of details for each PLA customer:

- **Customer data:**  
This data identifies the customer, its site through the site ID, and an optional Charge back ID to identify the division or group to be charged for usage. For this, you must configure the customer details in the `esdplatelemetry_customerinfo.properties` file.
- **Usage data:**  
This is the actual usage data based on the consumption, which is collected and shared on to Broadcom API. You must enable the upload of the usage data in `wasp.cfg` file. For more information on how to enable the telemetry uploads, see [Enable Telemetry Uploads](#).

#### **NOTE**

The collected Telemetry data is stored at: `'probes/service/wasp/esdplatelemetry/'`.

Both the customer and usage data is shared over API for internal reporting purpose.

#### **WARNING**

Telemetry does not collect any personally identifiable information (PII) or sensitive information. For additional information about how the your information is collected and used, read our [privacy statement](#).

#### Frequency of Data Collection

By default, telemetry collects and stores the data daily at 12.00 a.m. If the scheduler is not active at 12.00 a.m., the data is collected only in the next day run. The data is collected only once per day.

#### Enable Telemetry Uploads

#### Prerequisite

Ensure that the `uimesdplatelemetry web service` is deployed on the `uimserver wasp`.

#### **Step 1: Define the Customer Details in the `esdplatelemetry_customerinfo.properties` File**

1. Copy the `wasp/conf/esdplatelemetry_customerinfo.properties.template` file to `wasp/conf/esdplatelemetry_customerinfo.properties`.

2. Edit the `wasp/conf/esdplatelemetry_customerinfo.properties` file and define the following properties with the appropriate customer information:
  - a. `domain_name`: the customer domain name.
  - b. `site_id`: customer site ID. To find the customer ID, log into the Broadcom Support site and view the customer site ID information from your profile.
  - c. `pla_enabled`: define the value as true or false, to determine whether an install or upgrade is related to incremental use as a result of PLA. Contact the Broadcom sales team for more details on whether an installation is incremental or not.
  - d. (Optional) `chargeback_id`: define the division or group to be charged for consumption usage reported to broadcom.com. Defining the charge back details is useful in understanding which Unified Infrastructure Management environment the report originates from.

## Step 2: Configure the Telemetry Properties in wasp

You can configure the telemetry properties using one of the following options:

- Update the properties in `wasp.cfg`, or
- Update the properties from Infrastructure Manager, or
- Update the properties from the Administration Console

### Update the Properties in the wasp.cfg File

1. Edit the `./wasp.cfg` file and define the following parameters in the `<webapps>`
  - a. `esdplatelemetryconfig.upload_enabled_flag`: it is mandatory for all PLA customers to set this property as `true` to upload the data to Broadcom. By default, the flag is set to `false`.
  - b. (Optional) `esdplatelemetryconfig.proxy_url`: define the URL to the proxy server from the UIM Server. For example: `esdplatelemetryconfig.proxy_url = http://testproxy:8080`
  - c. (Optional) `esdplatelemetryconfig.proxy_auth_username`: configure the authenticated username using the Infrastructure Manager (IM) or Administration Console (AC) only. For more information, see Update the Properties from Infrastructure Manager and Update the Properties from the Administration Console.
  - d. (Optional) `esdplatelemetryconfig.proxy_auth_password`: configure the authenticated password using the Infrastructure Manager (IM) or Administration Console (AC) only. For more information, see Update the Properties from Infrastructure Manager and Update the Properties from the Administration Console.

#### WARNING

Do not configure the `esdplatelemetryconfig.proxy_auth_username` and `esdplatelemetryconfig.proxy_auth_password` parameters in the `wasp.cfg` file. Doing so leads to proxy authentication failure and a loss of transmitted payloads to Broadcom.

- e. (Optional) `esdplatelemetryconfig.envtype`: if you want to override the default endpoint where the data is uploaded, specify the appropriate value for the environment type. By default, the value is `prod`. You can change the value (for example) to `qa`.

```
<webapps> <uimesdplatelemetry> path = /uimesdplatelemetry load_on_startup = true reloadable
= true cross_context = true reinitialize = true unpack_war = true <custom>
<uncrypted> customerinfo.properties_filepath = ./conf/esdplatelemetry_customerinfo.properties
esdplatelemetryconfig.upload_enabled_flag = true esdplatelemetryconfig.proxy_url
= esdplatelemetryconfig.proxy_auth_username = esdplatelemetryconfig.envtype =
prod usage_metering_address = usage_metering </uncrypted> <crypt>
esdplatelemetryconfig.proxy_auth_password = </crypt> </custom> </uimesdplatelemetry></webapps>
```

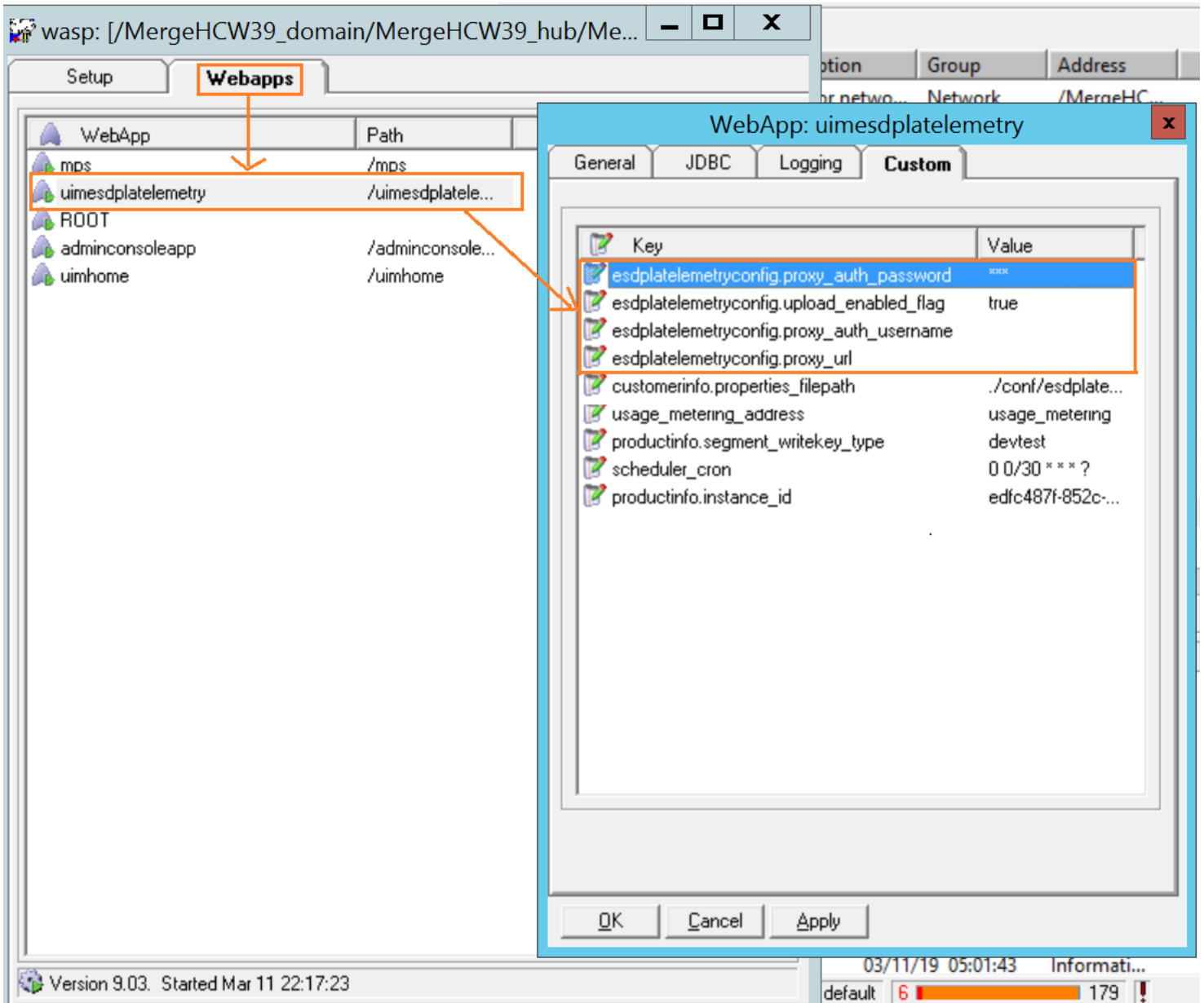
### Update the Properties from Infrastructure Manager

1. In Infrastructure Manager, double-click on `wasp` to open the `wasp` configuration UI.



2. Navigate to the **uimesdplatelemetry** webapp.
3. Right-click on **uimesdplatelemetry** and select **Edit**.
4. Navigate to the **Custom** tab.
5. Update and save the values for properties that are related to telemetry:
  - a. *esdplatelemetryconfig.upload\_enabled\_flag*: it is mandatory for all PLA customers to set this property as *true* to upload the data to Broadcom. By default, the flag is set to *false*.
  - b. (Optional) *esdplatelemetryconfig.proxy\_url*: define the URL to the proxy server from the UIM Server. For example: *esdplatelemetryconfig.proxy\_url* = `http://testproxy:8080`
  - c. (Optional) *esdplatelemetryconfig.proxy\_auth\_username*: define the authentication username to access the proxy
  - d. (Optional) *esdplatelemetryconfig.proxy\_auth\_password*: define the authentication password to access the proxy
  - e. (Optional) *esdplatelemetryconfig.envtype*: if you want to override the default endpoint where the data is uploaded, specify the appropriate value for the environment type. By default, the value is *prod*. You can change the value (for example) to *qa*.
6. Select **OK** to exit the properties dialog.

The following screenshot shows the mandatory and some of the optional parameters that are being set:

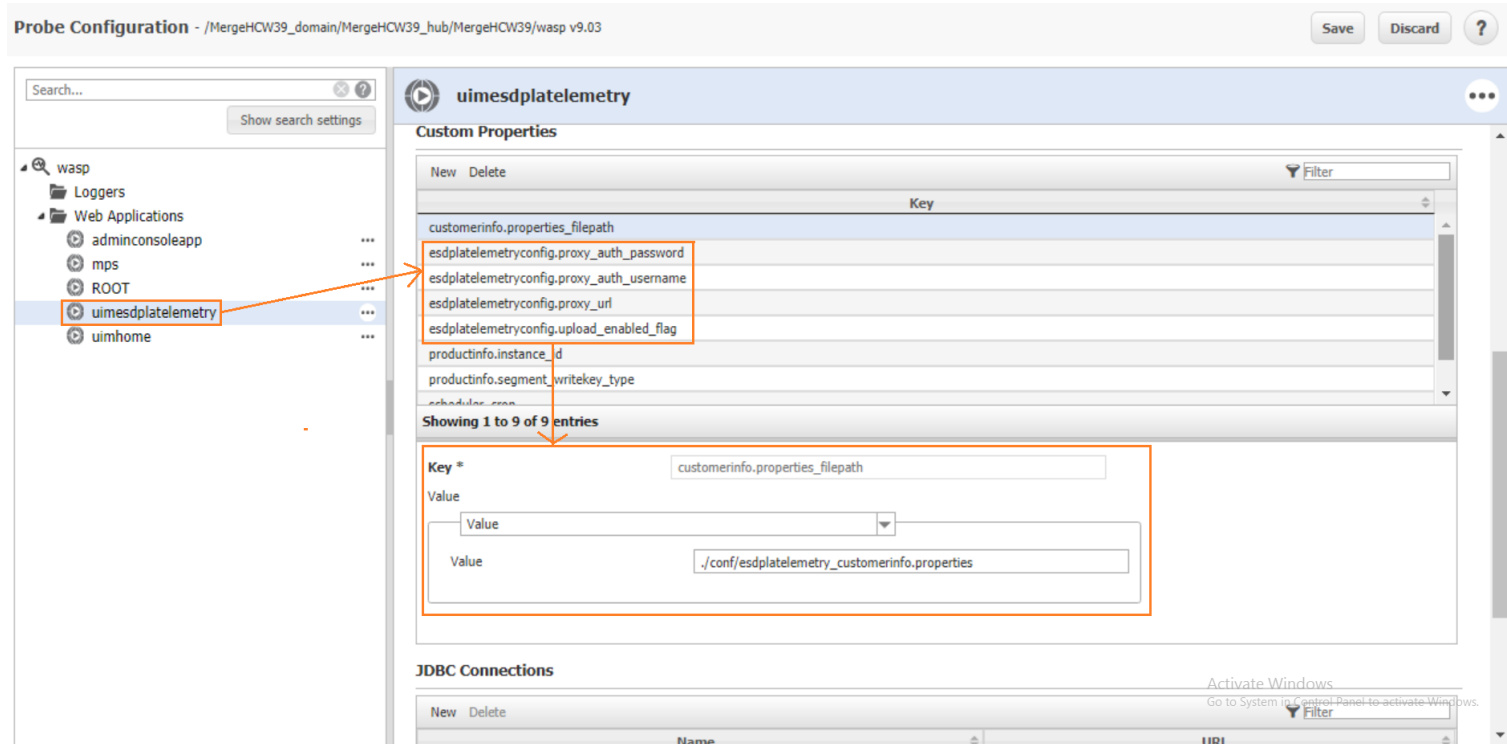


### Update the Properties from the Administration Console

1. In Administration Console, navigate to wasp and click Configure from the context menu open the wasp configuration UI.
2. Navigate to Web Applications and select **uimesdplatelemetry**.
3. In the properties pane, navigate to the **Custom Properties** section.
4. Update the values for properties that are related to telemetry and then select **Save**:
  - a. *esdplatelemetryconfig.upload\_enabled\_flag*: it is mandatory for all PLA customers to set this property as *true* to upload the data to Broadcom. By default, the flag is set to *false*.
  - b. (Optional) *esdplatelemetryconfig.proxy\_url*: define the URL to the proxy server from the UIM Server. For example: *esdplatelemetryconfig.proxy\_url = http://testproxy:8080*
  - c. (Optional) *esdplatelemetryconfig.proxy\_auth\_username*: define the authentication username to access the proxy

- d. (Optional) `esdplatelemetryconfig.proxy_auth_password`: define the authentication password to access the proxy
- e. (Optional) `esdplatelemetryconfig.envtype`: if you want to override the default endpoint where the data is uploaded, specify the appropriate value for the environment type. By default, the value is `prod`. You can change the value (for example) to `qa`.

The following screenshot shows the mandatory and some of the optional parameters that are being set:



### Step 3: Restart wasp

Restart the uimserver wasp for the uimesdplatelemetry web service to initialize using the newly created configuration values.

### Troubleshoot

For any errors, review the `uimesdplatelemetry.log` file stored in the directory 'probes/service/wasp/'. The web service performs a validation at startup, and errors are logged if the configuration is in error. The uploads are performed once a day at midnight, we recommend that you review the log file next day as a final validation.

## Operator Console (OC) Host Header Validation

In Operator Console (OC), when a user changes the hostname value in the OC API and runs it, the API response shows a success message, 200 OK. Instead of the success message, the response should have thrown an error. To restrict this behavior, you can add a list of OC hostnames to ensure that when any user tries to change the listed hostname value in the API, the response displays an appropriate error instead of the success response.

### Follow these steps:

1. Deactivate the wasp probe.
2. Open the `<Nimsoft>\probes\service\wasp\webapps\ROOT\WEB-INF\web.xml` file in an editor.
3. Locate and uncomment the following section:

```

<filter>
 <filter-name>HostHeaderFilter</filter-name>
 <filter-class>com.liferay.portal.kernel.servlet.filters.invoker.HostHeaderFilter</
filter-class>
</filter>
<filter-mapping>
<filter-name>HostHeaderFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>

```

4. Save the changes.
5. Open the `<Nimsoft>\probes\service\wasp\conf\config.properties` file in a text editor.
6. Add a comma-separated list of OC hostnames to the following parameter:
  - `host.header.list`
7. When anyone tries to change
8. Save the changes.
9. Restart the wasp probe.

Now, when any user tries to change the value of any listed hostname that is present in this list, an error is thrown.

## Auditing in UIM Interfaces

Auditing in UIM interfaces helps you monitor the administrative activities that are performed in UIM through Operator Console or related APIs. Administrative activities include creating, updating, or deleting objects such as device groups and policies. The information is collected and stored in the database tables: **wasp\_audit\_log** and **wasp\_audit\_details**.

### Enable/Disable Auditing

By default auditing is set to disabled. To enable/disable the auditing, do the following:

Open `wasp.cfg` and add the below settings under `setup/auditing` to enable/disable auditing

To enable: Add the key “`enabled=true`”

To disable: Set the key “`enabled=false`”

### Access the Auditing Information

User information including the actions performed, datetime information and the change details are stored in these tables.

The database tables need to be queried for the auditing purposes.

Below are few sample queries:

```
select * from wasp_audit_log order by timestamp desc
```

```
select * from wasp_audit_details
```

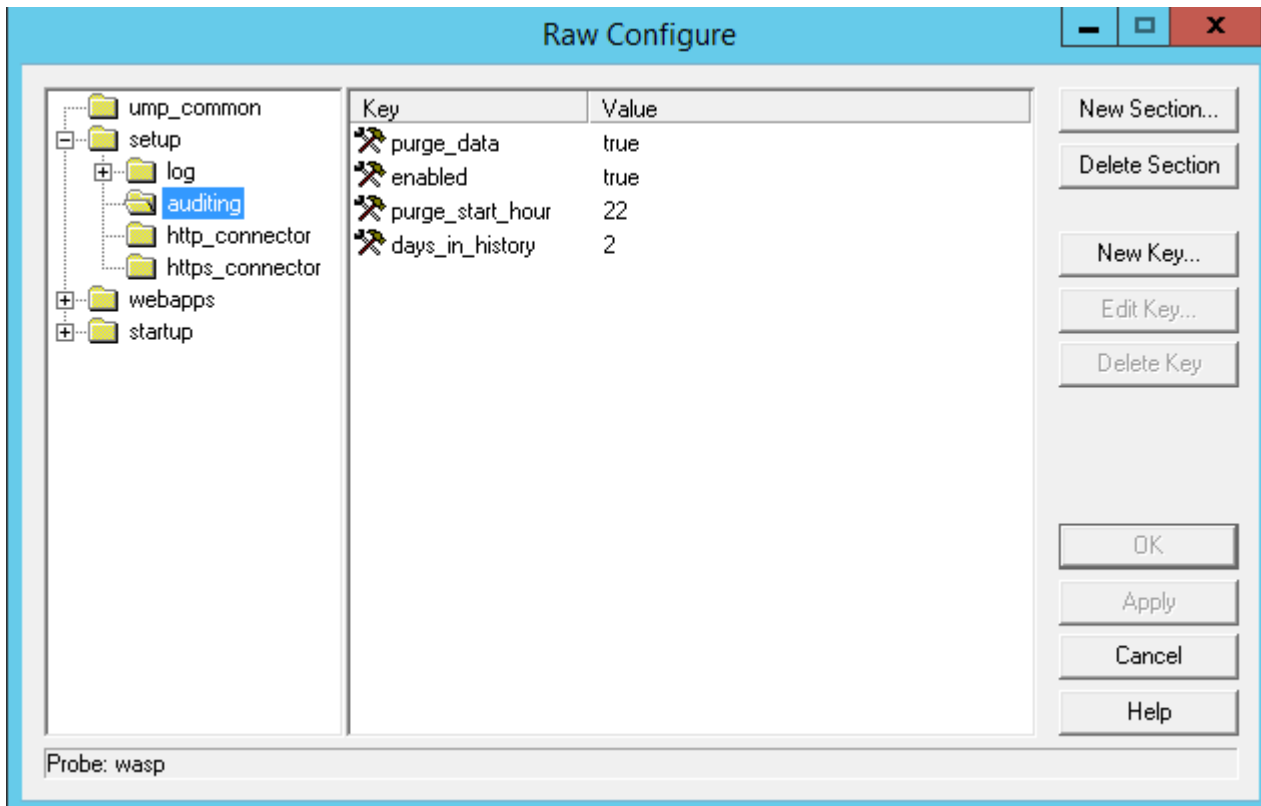
By default, auditing is in disabled state. Auditing need to be enabled on the wasp server and can be configured using the following configuration information:

### Maintain Auditing Data

When auditing is enabled, the database size increases. It is recommended that you clear the data periodically to control the database size. A purge task runs daily to clear the data beyond data retention policy of 30 days. This task is scheduled to run at 2300 hours daily (as per the UIM Server timezone) and can be configurable. General recommendation is to set Audit data purging task at the hour of the day during which there is usually less load on the database. Audit data purging is enabled by default and stores 30 days of audit data. This can be configured as per below.

Open wasp.cfg and add the below settings under setup/auditing:

- To enable audit data purging: Add the key “purge\_data =true” under setup/auditing section. Supported values - true/false.
- To disable audit data purging: Add the key “purge\_data =false” under setup/auditing section.
- To configure data retention policy: Add the key “days\_in\_history=<no\_of\_days\_to\_keep\_data>” under setup/auditing section [default value is 30 days]. Supported values - any number.
- To configure when to run data purging: Add the key “purge\_start\_hour =<hour\_when the purging should start>” under setup/auditing section [default is 2300 hours daily]. Supported values 0-23.



#### NOTE

If auditing is disabled, then Audit data purging will not happen.

#### **Information of Events tracked Under Auditing:**

Any creation, updation or deletion of UIM configuration performed using UIM Operator console or its related APIs are recorded as per auditing.

The example UIM configurations are Inventory, Groups, Discovery Scopes etc.

## White Labeling in Operator Console

UIM 20.3.0 comes with a refreshed login screen in Operator Console with the option to login through SSO along with the regular login method. Operator Console screens are enhanced to provide personalization offering consistency and cognitive workflow for user login. You can label UIM user interface as per your company brand name and the product names. You can use your Company logo instead of CA UIM on Operator Console. You can also add Custom welcome note and login instructions on the Login screen.

#### **Contents**

### **Update Logo**

You can change the logo that is visible on the Operator Console login screen and the other Operator Console screens.

To update the logo, follow the below instructions:

1. Go to folder <Nimsoft Directory>\probes\service\wasp\conf\logo.
2. Navigate to the file logo.svg.
3. Replace it with your desired logo.
4. Restart the wasp probe.

#### **NOTE**

The logo should be added with the name logo.svg and the supported format is .svg.

### **Update Company Name**

You can change the Company name that is visible on the Operator Console login screen and the other Operator Console screens.

To update the Company name, follow the below instructions:

1. Open the wasp.cfg in Raw Configure.
2. Navigate to webapps/operatorconsole\_portlet/custom/uncrypted.
3. Update the key brand\_name with your Company name.
4. Save the file.
5. Restart the wasp probe.

### **Update Product Name**

You can change the Product name that is visible on the Operator Console login screen and the other Operator Console screens.

To update the Product name, follow the below instructions:

1. Open the wasp.cfg in Raw Configure.
2. Navigate to webapps/operatorconsole\_portlet/custom/uncrypted.
3. Update the key **brand\_product** with the Product name.
4. Save the file.
5. Restart the wasp probe.

### **Update Footer Message**

You can change the footer message that is visible on the Operator Console login screen and the other Operator Console screens.

To update the footer message name, follow the below instructions:

1. Open the wasp.cfg in Raw Configure.
2. Navigate to webapps/operatorconsole\_portlet/custom/uncrypted.
3. Update the key **footer\_bar** with the desired footer message.
4. Save the file.
5. Restart the wasp probe.

#### **NOTE**

To use a copyright symbol in the footer, you need to provide unicode value. \u00A9 is the unicode value for copyright symbol.

## Update Note on the Login Screen

You can change the default note that is visible on the Operator Console login screen. You can add customized welcome note and any instructions to the users about the application and a customized link for additional information.

To update the note in the login screen, follow the below instructions:

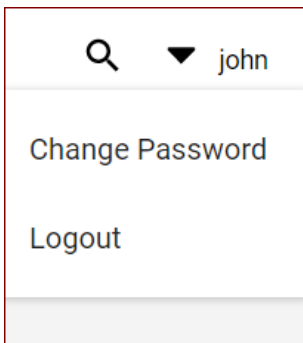
1. Open the data.html file in the location <Nimsoft Directory>\probes\service\wasp\conf\logo.
2. Update the keys with the required information in the note.
  - <h2> for the title of the note.
  - <div class="boxInsideContent"> with the Welcome note or Product Overview or any Customized instructions.
  - <a> anchor tag with any link for more details.
3. Save the file.
4. Restart the wasp probe.

## Change Your Password

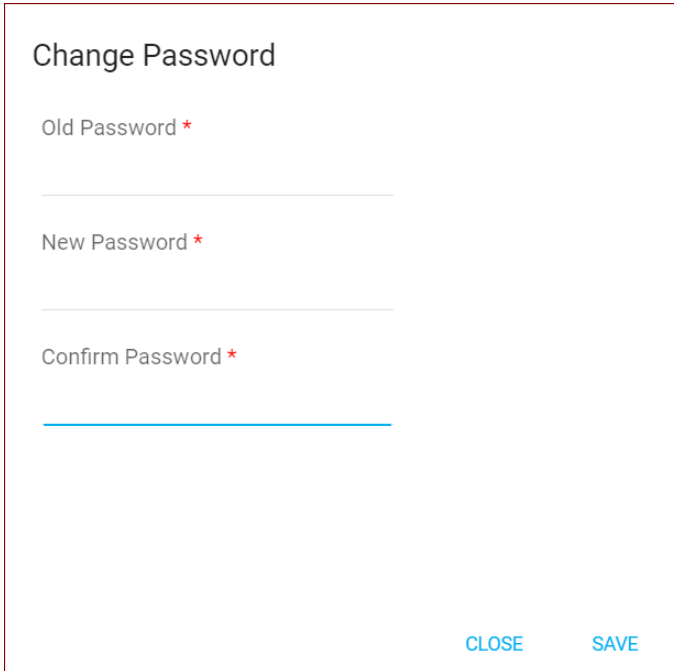
As an account contact user, you can now change your own password in UIM 20.3.3. If the "Change Password" ACL is enabled for an account, then the related account contact users can change their own password. This ability reduces the chances of the password getting compromised.

### Follow these steps:

1. Log in to Operator Console (OC) with your credentials.
2. Locate the Change Password option in the top-right area of the UI (under the logged-in user name). The following screenshot shows the required information:



3. Click the Change Password option.  
The Change Password dialog opens.



Change Password

Old Password \*

\_\_\_\_\_

New Password \*

\_\_\_\_\_

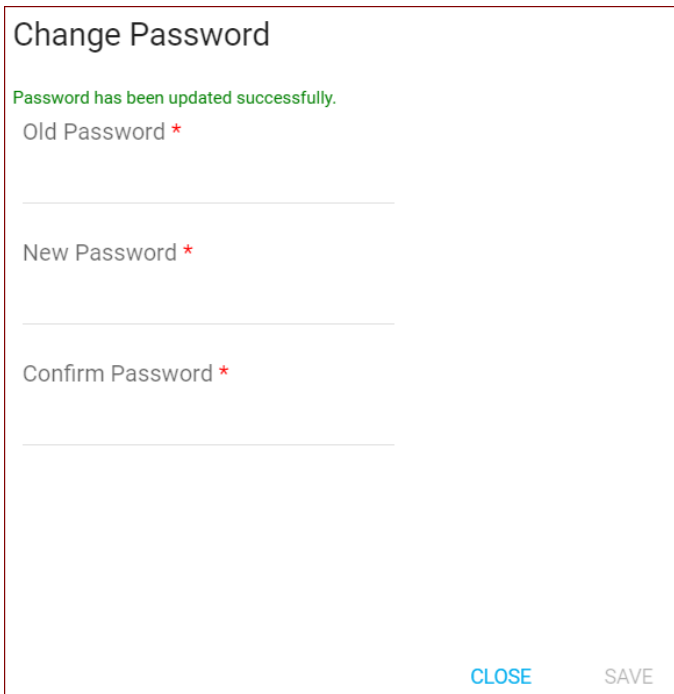
Confirm Password \*

\_\_\_\_\_

CLOSE SAVE

4. Enter information in the following fields:
  - a. Old Password: Enter your existing password.
  - b. New Password: Enter the new password.
  - c. Confirm Password: Confirm the new password.
5. Click Save.

A confirmation message displays stating that the password has been changed.



Change Password

Password has been updated successfully.

Old Password \*

\_\_\_\_\_

New Password \*

\_\_\_\_\_

Confirm Password \*

\_\_\_\_\_

CLOSE SAVE

6. Click the Close button to close the dialog.

You have successfully changed your own password.



## Back Up the Licensing Information

From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. We recommend that you take a backup of the existing licensing information before you upgrade to 9.2.0. This will help you re-use the license information if you downgrade to versions prior to 9.2.0 (which use license) or want to revert to the original state

From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. We recommend that you take a backup of the existing licensing information before you upgrade to 9.2.0. This will help you re-use the license information if you downgrade to versions prior to 9.2.0 (which use license) or want to revert to the original state.

### Follow these steps:

1. Navigate to the distsrv folder (../Nimsoft/probes/services/distsrv).
2. Take a backup of the distsrv.cfg file. This file includes licensing information.
3. Copy the license-related information from the backed-up distsrv.cfg file and put it into the required distsrv.cfg file. An example of the license information available in the distsrv.cfg file is as follows:

```
<licenses>
 <interface_traffic>
 version =
 info = CA
 ip = * number = 2147483647
 expire = 31-dec-2025
 code = NOLL ARE CAP PAN MORN BUG
 </interface_traffic>

</licenses>
```

4. Restart the distsrv probe.

## Configuring and Viewing Monitoring Data

The Operator Console (OC) is a web-based interface that allows you to:

- Discover and monitor systems
- Graph QoS data
- View and manage alarms
- Create SLAs and view SLA performance reports
- Create, view, and schedule reports
- Create and view dashboards
- Manage users
- Configure probes

### Features and Components

The Operator Console provides users to manage membership in devices, groups, and device monitoring profiles, and view dashboards, alarms, discovery, metrics and interfaces.

The Operator Console provides you with a graphical, clickable means to navigate through system operations and monitoring results. Summary views of monitored technologies, devices and groups, and alarms are linked to in-depth views of system components and metrics. Some of these components require an additional purchase.

#### NOTE

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5.

### Contents

#### Prerequisites

- To view the data in Operator Console, ensure that you have the Operator Console Basic permission. When upgrading to UIM 9.0.2, users will not have access to the Operator Console. You must add the *Operator Console Basic* ACL permission in the Account Admin view. By default, this permission is only available to Administrators and Superusers.
- To manage groups using Operator Console, ensure that you have OC Group Modification permission. For more information, see [Permissions Reference for OC](#).
- The Operator Console is supported only on Edge, Chrome and Firefox browsers. For more information, see [Compatibility Matrix](#).

#### Access Operator Console

1. Log in to Operator Console.
2. Based on your access permissions you can perform related actions.

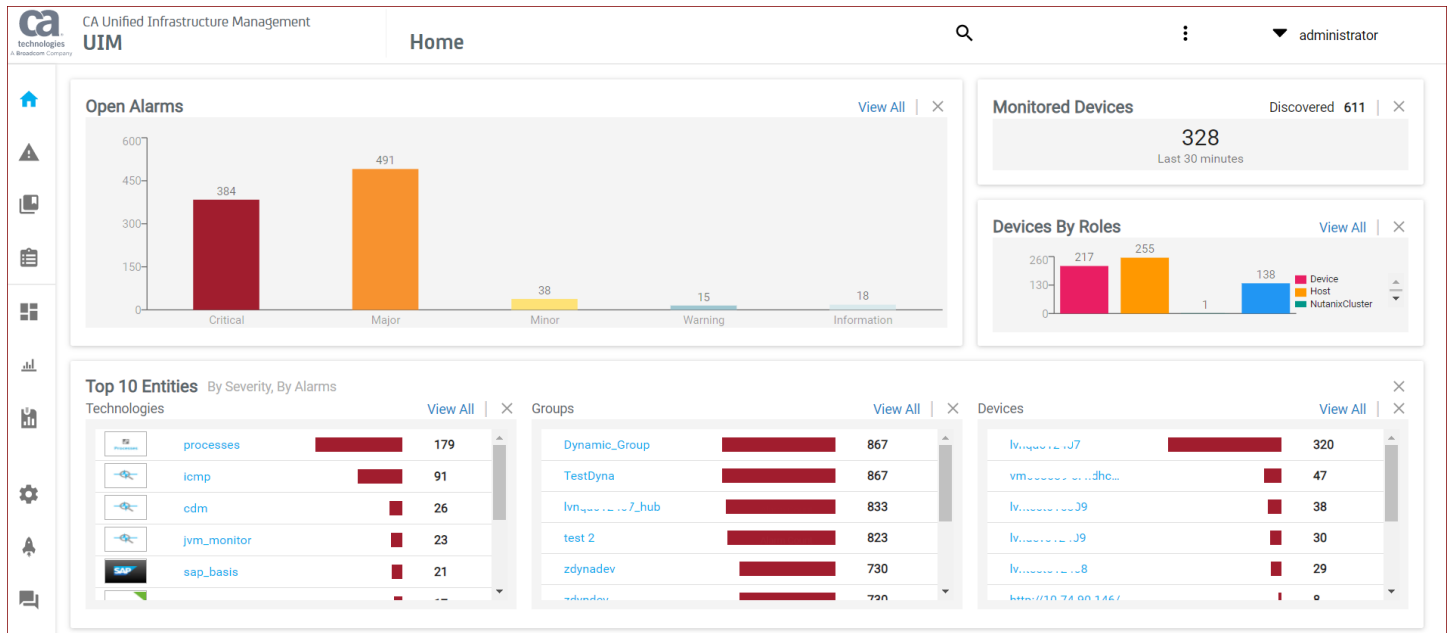
#### Home View

The Home



view provides a quick at-a glance view of the state of your deployment in terms of what is being monitored. The following

screenshot shows the Home page view (native OC screen) in UIM 20.3.3. This view is rendered by using HTML5; it is not dependent on CABI in UIM 20.3.3:



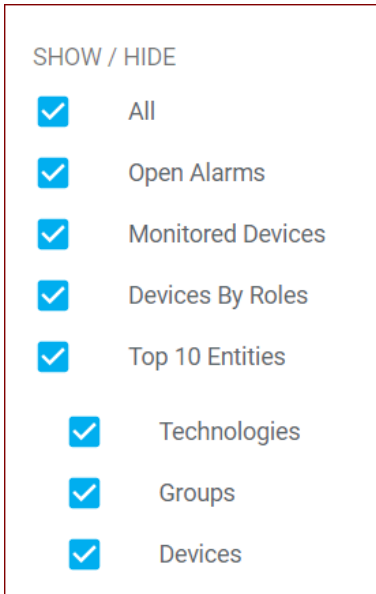
The Home page view helps you as follows:

- **Open Alarms**
  - View the count of the alarms that are generated in your environment.
    - Click the View All link to navigate to the Alarms view page, which contains more details.
    - Click the respective bar on the chart to navigate to the Alarms view, which contains more details.
- **Monitored Devices**
  - View the devices discovered and actively monitored.
- **Devices By Roles**
  - View the role spread of monitored devices.
    - Click the View All link to navigate to the inventory view that provides detailed information.
- **Top 10 Entities**
  - Technologies: View the top monitored technologies that are sorted by alarm severity and count. For example, an entity having one critical alarm is displayed first in the list when compared with the entity having two major alarms. The alarm count is considered after the severity. Click the View All link or the respective entity link to further drill-down for more information.
  - Groups: View the top groups sorted by alarm severity and count. Click the View All link or the respective entity link to further drill-down for more information
  - Devices: View the top devices sorted by alarm severity and count. Click the View All link or the respective entity link to further drill-down for more information

## Working with Tiles

- **Remove a Tile**
  - Click the **X** icon on the specific tile if you want to remove that tile from the page.
- **Access Specific Tile Details**
  - Click the **View All** link (if available) or the respective entity link (if available) to navigate to the respective page for more information.
- **Show/Hide a Ttile**

- Click the three-dot menu at the top right to remove or add a tile to the page. When you click the menu, the following dialog opens. You can clear or select the required tile, as appropriate:



### Alarms View

The **Alarms** (🚩) view displays all the alarms that are generated in your environment. The following example screenshot shows the alarms view in UIM 20.3.3:

| Actions | Acknowledged | Device Name | Alarm Type | Owner      | Alarm Message                                               | Duration | Device Type |
|---------|--------------|-------------|------------|------------|-------------------------------------------------------------|----------|-------------|
| ☐ ▲ ⋮   | false        | w           | Controller | Unassigned | Max. restarts reached for probe 'wasp' (command = <...)     | 10 days  | Host        |
| ☐ ▲ ⋮   | false        | w'          | Controller | Unassigned | Max. restarts reached for probe 'wasp' (command = <...)     | 10 days  | Host        |
| ☐ ▲ ⋮   | false        | 10          | Network    | Unassigned | Packet Loss is above threshold limit! (profile: 10.17.1...) | 17 days  | Device      |
| ☐ ▲ ⋮   | false        | 10.         | Network    | Unassigned | 10. : Connection to 10. (ping) failed                       | 17 days  | Device      |
| ☐ ▲ ⋮   | false        | 10.         | Network    | Unassigned | 10 : Connection to 10. } (ping) failed                      | 22 days  | Device      |

For more information about the alarms view, see the topic [View Alarms Data](#).

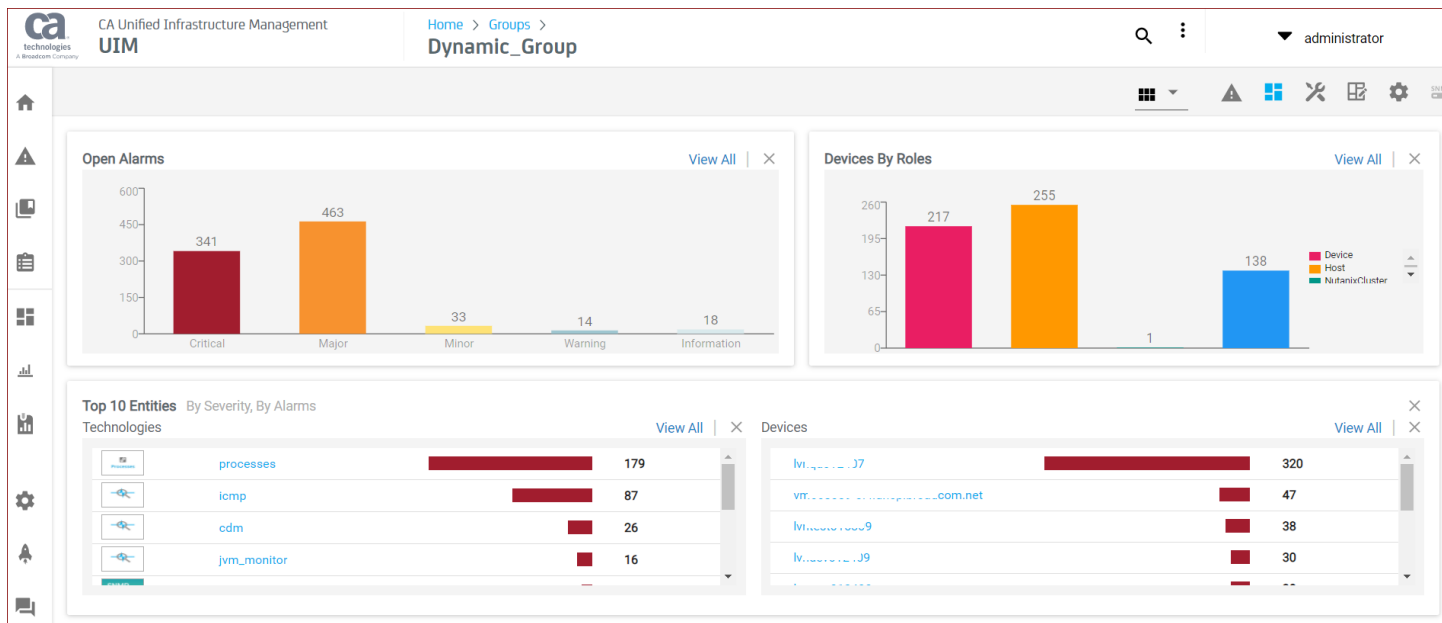
### Groups View

The **Groups**



view displays the list of groups in your environment.

The following screenshot shows the group dashboards view (native OC screen) in UIM 20.3.3. This screen is rendered by using HTML5; it is no longer dependent on CABI in UIM 20.3.3:



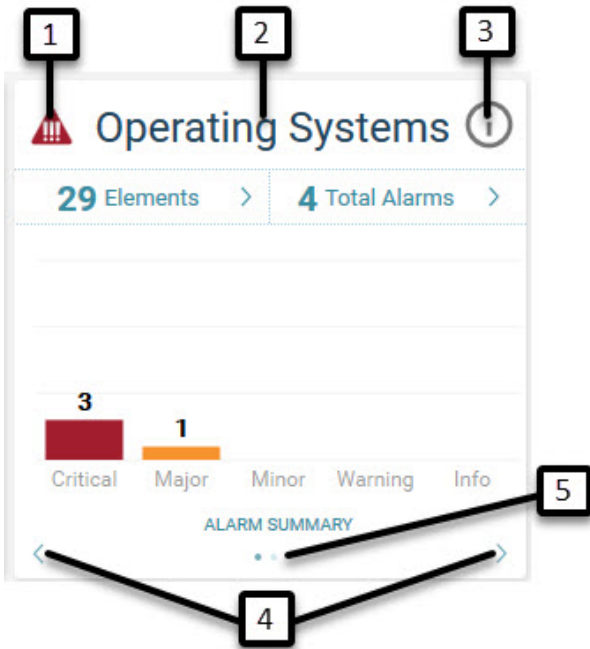
You can perform the following tasks in this view:

- Open Alarms**  
 View the count of opens alarms in the group.
  - Click the View All link to navigate to the Alarms view page, which contains more details.
  - Click the respective bar on the chart to navigate to the Alarms view, which contains more details.
- Devices By Roles**  
 View the role spread of the monitored devices in the group.
  - Click the View All link to navigate to the inventory view, which provides more details.
- Top 10 Entities**  
 View the top monitored technologies/sub-groups and devices in the group. The list is sorted based on the alarm severity and then alarm count. For example, an entity having one critical alarm is displayed first in the list when compared with the entity having two major alarms. The alarm count is considered after the severity.
  - Click the View All link to navigate to the respective view, which provides more details.
  - Click the specific entity (for example, device or monitoring technology) to access the detailed information.
- Properly Created URL**  
 Use the properly formed URL to directly access the group dashboard view: `http://<OC_Server>/operatorconsole_portlet/groups/0/<Group_ID>/dashboard`
- Remove a Tile**  
 Click X to remove a tile from the view.
- Show/Hide a Tile**  
 Click the three-dot menu at the top-right of the UI to show or hide the tiles from the view.

### Accessing Other Group Views

The groups view also displays cards view, list view, and tree view for each group. For example, cards are displayed when the **Card**

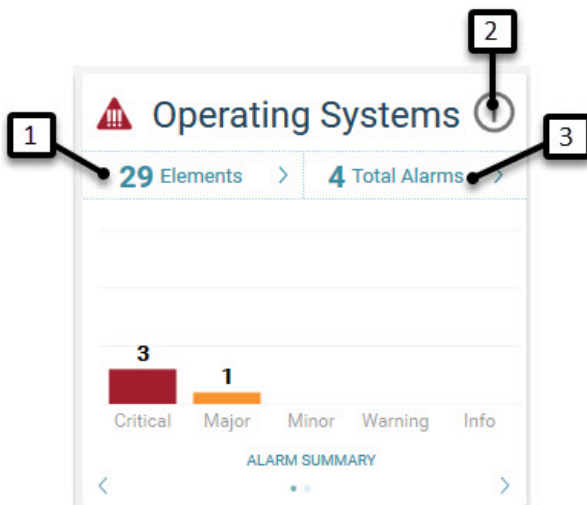
() view is selected. The following image shows the type of information available on the cards.



1. The active highest alarm state for a group
2. The group name
3. Alarm and device summary information for a group
4. The arrows to switch between alarm summary and alarm history over the past 30 days
5. The indicator for the current card view

**Access More Data**

Clicking various parts of a card brings up different views where you can see more information about the status of each group.



1. Lets you navigate down the hierarchy of groups and devices
2. Lets you view information about a group and the generated alarms
3. Displays the alarms for a group

List view is displayed when the **List** view is selected. The list view displays the groups in a List. Clicking on each group in the list will open the list of devices.

CA Unified Infrastructure Management UIM | Home > ... > origin > lvnqa012407\_hub

| Name                                | Device Type    | Operating system               | IP address                    | Monitored by |
|-------------------------------------|----------------|--------------------------------|-------------------------------|--------------|
| aj644227-ose1-n5.dhcp.broadcom.net  | VirtualMachine | Linux-CentOS (3.10)            | 10.143.2.1, 10.17.165.173     | icmp, rsp    |
| r74robot21.dhcp.broadcom.net        | VirtualMachine | Linux-RedHat-Enterprise (3.10) | 10.17.164.221                 | icmp, rsp    |
| r74robot22.dhcp.broadcom.net        | VirtualMachine | Linux-RedHat-Enterprise (3.10) | 10.17.165.33                  | icmp, rsp    |
| Nicholas-vm01                       | VirtualMachine | Linux-CentOS (3.10)            | 10.131.239.144, 10.17.164.152 | icmp, rsp    |
| shield-ose02.dhcp.broadcom.net      | VirtualMachine | Linux-CentOS (3.10)            | 10.140.0.1, 10.17.164.185     | icmp, rsp    |
| as625515-osevm03.dhcp.broadcom.net  | Host           |                                | 10.17.165.141                 | icmp, rsp    |
| r74sechub2.dhcp.broadcom.net        | VirtualMachine | Linux-RedHat-Enterprise (3.10) | 10.17.164.196                 | icmp, rsp    |
| dm672442-centos02.dhcp.broadcom.net | VirtualMachine | Linux-CentOS (3.10)            | 10.17.165.248                 | icmp, rsp    |
| dhcp-10-17-164-1.dhcp.broadcom.net  | VirtualMachine | Linux-RedHat-Enterprise (3.10) | 10.17.164.1                   | icmp, rsp    |
| one-128-aiops.dhcp.broadcom.net     | Host           | Linux-RedHat-Enterprise (3.10) | 10.17.164.163                 | icmp, rsp    |
| mk668511-rh01.dhcp.broadcom.net     | VirtualMachine | Linux-RedHat-Enterprise (3.10) | 10.17.164.22, 172.17.0.1      | icmp, rsp    |

Tree view is displayed when the **Tree** view is selected. The tree view displays the groups in tree view with the associated devices. Clicking on each group node in the tree will show the devices in the group.

CA Unified Infrastructure Management UIM | Home > Groups

Search Group

- Groups (679)
  - 0\_s\_J7 (3)
  - 0\_st\_de (13)
  - 10Aug\_Dy\_Dev (5)
  - 10Aug\_Stat\_dev (5)
  - 10Aug\_dy\_in (0)
  - 10Aug\_stat\_in (0)
  - 18Aug\_SStatint (1)
  - 21Aug\_Interface (2)
  - 22Aug\_cont (19)
  - 22aug\_dur\_in (1)
  - 22aug\_sts\_in (3)
  - 25Aug\_di (0)
  - 29Jul\_Static\_Device (4)
  - 29\_Container\_grp1 (8)
  - 2\_stat\_interface (20)
  - 4aug\_si (2)
  - 7Aug\_Cont (17)
  - Acc\_emp (3)
  - Acc\_emp11 (5)
  - Account (0)

Details

| Member Group | Name               | Type      | Count |
|--------------|--------------------|-----------|-------|
| 12           | origin             | Container | 679   |
| 11           | Cisco              | Container | 188   |
| 11           | Operating Systems1 | Container | 188   |
| 11           | Cisco123           | Container | 186   |
| 11           | Operating Systems  | Container | 188   |
| 8            | NorthRegion        | Dynamic   | 237   |
| 6            | dy_de              | Dynamic   | 372   |
| 3            | FinanceApps1       | Dynamic   | 77    |
| 1            | 22Aug_cont         | Container | 22    |
| 0            | Card_Cont_Grp1     | Container | 22    |
| 0            | 21Aug_interface    | Static    | 2     |
| 0            | Account1           | Static    | 3     |

For more information about managing your groups, see the [Manage Groups](#) topic.

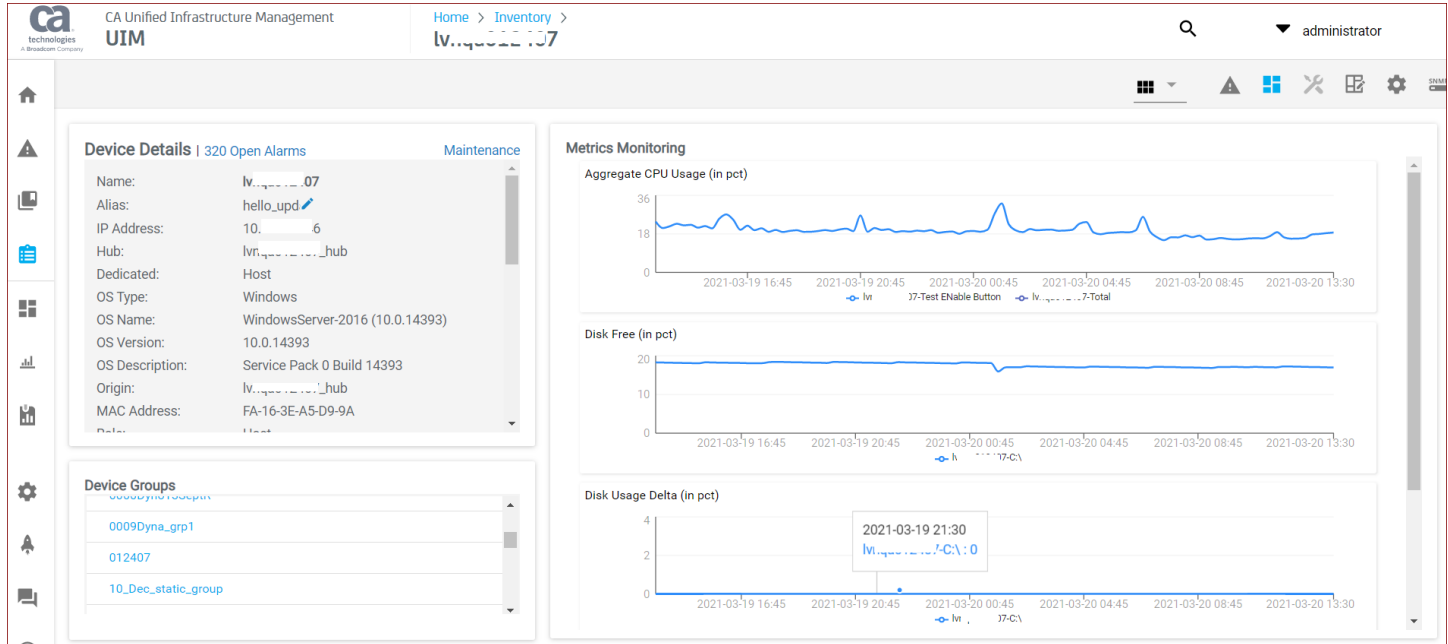
## Inventory View

### The Inventory



view provides an easy way to view the devices in UIM inventory that is generated for environments you are monitoring. You can also view information around them like alarms and see which devices have robots that are deployed.

After you click a device in the inventory view, you can then access the device details (dashboard) view. The following screenshot shows the device dashboards (details) view (native OC screen) in UIM 20.3.3. This screen is rendered by using HTML5; it is no longer dependent on CABI in UIM 20.3.3:



This view helps you as follows:

- **Device Details**

View the the summary about the details of the device. This includes detailed information; for example, name, IP address, hub, OS, information about the maintenance schedule of the device, and so on.

- **Open Alarms Count**

- View the count of the open alarms for the selected device.
- Click the alarm count link to navigate to the detailed view.

**NOTE**

If the device is in maintenance, the alarms count is not displayed. Instead, the maintenance mode symbol is displayed.

- **In-Context Maintenance Link**

- Put the device in the maintenance schedule by using the in-context Maintenance link in the Device Details tile. Click the Maintenance link and specify the maintenance schedule details. The device is then included in the maintenance schedule. The related maintenance information is then displayed at the bottom of the same Device Details tile.

- **Edit the Device Alias**

- Click the edit icon (pencil) next to Alias, provide the appropriate name in the dialog, and click Apply to save the update.

- **Device Groups**

View the groups associated with the selected device.

- Click the respective group link on the tile to navigate to the related Groups view to find more information.

- **Metrics Monitoring**

View the metrics monitoring charts (metric views) for the device. Metrics view that is created for the selected device is displayed under Metrics Monitoring. If no metrics view is defined, then the view based on the default metrics (for



example, CPU) is displayed by default. If the Metrics Monitoring section is empty, it implies that no monitoring is configured for the device.

- **Properly Created URL**

- Use the properly created URL to directly access the device dashboard view: `http://<OC_Server>/operatorconsole_portlet/computer_systems/<CI_ID>/dashboard`

**NOTE**

If you try to access this device view by navigating through the Groups path (Groups view -> Group -> Device), then you need to click the Detail view icon to access this view. The Dashboard view icon is disabled in this case.

For more information about using the Inventory view, see the [View Your Inventory](#) topic.

**Dashboards View**

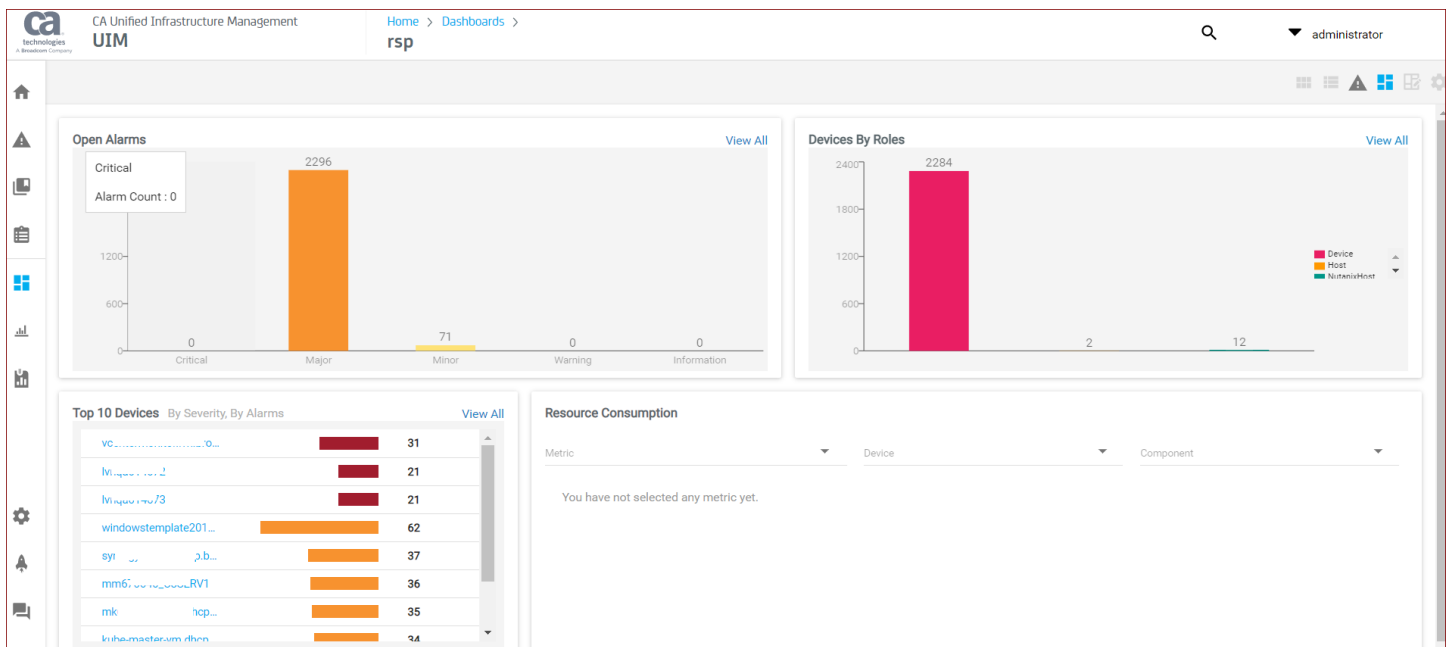
**The Dashboards**



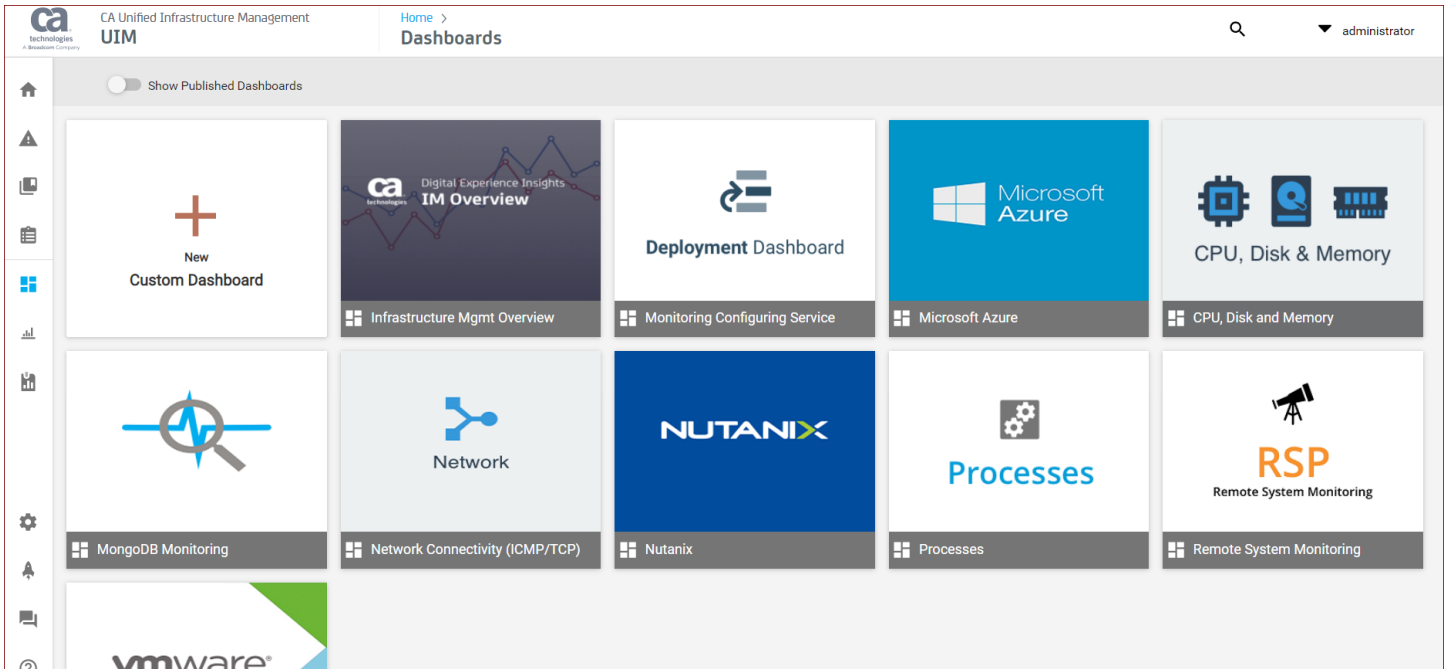
view lets you view your metric and alarm data in pre-defined dashboards after you have configured your monitoring.

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens (including generic dashboards) are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5.

Therefore, the dashboard pages for the monitoring technologies (probes) like processes, rsp, cdm, net\_connect, and so on are rendered by using HTML5, not CABI. When you click a tile on the main Dashboards page, the dashboard pages for such probes are rendered using HTML5. The following screenshot shows an example of the cdm probe dashboard page in UIM 20.3.3:



The main Dashboard page is displayed as follows when accessed using the Dashboard link in the left navigation view:



For more information about dashboards, see the [View Your Dashboards](#) topic.

### **Search, Filter, and Sort Group and Device Cards**

In the Groups view, there are several ways to navigate to specific groups or computer systems, or to sort groups and computer system cards.

1. **Search** (🔍): Displays the devices that match the entered search string.
2. **Action menu** (⋮): This menu provides context-sensitive action choices; for example, add a group, edit a group. The drop-down lists the options that are appropriate for the current view.
3. **Filter**: Filters groups or devices within the current context. For example, click the default Operating Systems group. Next, type **win** in the filter field and only subgroups with 'win' in the name, within the Operating Systems group, appear in the window.
4. **Card filter**: Lets you sort group or device cards by name, severity, alarm count, or member count.

### **Reports**

The Reports view provides reports to show overall compliance, SLA details, SLOs, SLA compliance trend, and graphs on the SLO data. For more information, see the [View Your Reports](#) topic.

### **SLM**

The SLM view is an interface to create service-level agreements (SLAs) and their component service-level objectives (SLOs) and quality of service (QoS) constraints. For more information, see [The SLM View](#) topic.

### **Settings**

Use the **Settings** (⚙️) to perform the following:

- Manage alarms in the [Alarm Policies](#).
- Create dashboards using [Dashboard Designer](#).
- View and manage report schedules using [Report Schedules](#).
- Create custom Restful API monitoring using [RESTMon](#).
- [Device Self-Certification](#) for the SNMP Collector.
- Manage the accounts using [Account Admin](#).
- Manage hubs, robots, and probes using [Admin Console](#).
- Configure auto groups in [Administration](#).

### **Setup Wizard**

Use the **Setup Wizard**, to configure Device Discovery or configure the available remote and cloud monitoring technologies as Tiles.. For more information, see the [View the Using Setup Wizard](#) topic.

## **OC Prerequisites**

While OC is immediately available after installation, several features are dependent on other CA UIM components. This article describes the prerequisites for full OC functionality.

### **Contents**

#### **Run Discovery**

CA UIM must locate your computer systems before you can create groups. Finding and listing all addressable devices and computers within a managed IT environment is the job of automated *discovery*.

When the Operator Console (OC) is installed, the Discovery Wizard starts automatically and prompts you to configure and run discovery. The wizard allows you to specify authentication credentials and define IP address ranges to scan. Discovery finds virtually all connected resources on the network and provides detailed information on device type, configuration, and asset/inventory data. By using ICMP, ARP, DNS, SNMP (v1, v2, and v3), WMI, SSH, and NetBIOS, discovery finds a wide range of devices and device information.

The list of devices, referred to as your *Inventory*, can be augmented by XML file-based device import. When multiple discovery records correspond to a single device, this is recognized by device correlation.

To maintain your inventory, you can re-run discovery through the wizard at any time, scheduling discovery to run on regular intervals and modifying the credentials and ranges as needed. You can also run discovery on a selected subset of scopes to update a portion of the existing inventory.

For more information on how to use discovery, see the articles [Discover Systems to Monitor](#) and [Configuring Discovery in OC](#).

#### **The Details Tab**

The **Details** tab displays information about properties, disk usage, interface traffic, and performance for a selected device. The information displayed depends on the data available. Items that have no value available for the system are omitted.

#### **The Metrics Tab**

The **Metrics** tab displays data for the any metrics monitored on the system. The metrics tab also contains a health index chart for all monitored QoS metrics with health index enabled. These metrics are configured and can be customized through templates in the monitoring templates configuration tool. See the article [Monitoring Configuration Service](#) for details on configuring monitoring probe profiles. For more details on the [health\\_index](#) probe, see the Probes Documentation Space.

## The Device Interface View

Some of the information in the Device Interface View requires deployment and configuration of the v2.0 SNMP Data Monitoring (snmpcollector) probe. The snmpcollector probe populates the interface information within OC.

In snmpcollector v2.0, you can configure metrics for multiple systems by activating a monitoring template. Applying the snmpcollector probe's default monitoring template to your target systems will configure all of the metrics shown in the Device Interface View.

You can activate the default monitoring template using the Template Editor in snmpcollector v2.0. For more information, see the article [SNMP Data Monitoring \(snmpcollector\) - Apply Monitoring v2.0](#) on the Probes Documentation Space.

You can also configure the following snmpcollector metrics for each column heading individually:

| Column Heading      | Required snmpcollector Metric |
|---------------------|-------------------------------|
| Errors % (In)       | PctErrors(In)                 |
| Errors % (Out)      | PctErrors(Out)                |
| Utilization % (In)  | Utilization(In)               |
| Utilization % (Out) | Utilization(Out)              |
| Discards % (Out)    | PctDiscards(Out)              |
| Discards % (In)     | PctDiscards(In)               |

## The Advanced Tab for Interfaces

The Advanced tab for interfaces uses the following snmpcollector v2.1 metrics:

- Utilization(In)
- Utilization(Out)

### NOTE

The Advanced view can also display metrics from probes associated with other CA products, such as CA Network Flow Analysis and CA Application Delivery Analysis. These products must be integrated with UIM and their probes configured in order to view these metrics. For more information, see [Integrating Other Products](#).

## Run Discovery in OC

The first time that you open the Operator Console (OC) and the Discovery Wizard is automatically launched.

After the first time you open OC, you can launch the Discovery Wizard manually if you want to run discovery or change your discovery settings to run discovery automatically on a set schedule. You can launch the Discovery Wizard from the Setup Wizard or from the Inventory View in the left navigation.

### NOTE

The Discovery Wizard will not run after an update of CA Infrastructure Management if there are existing range scopes that define *excluded* IP addresses. You must either accept the system prompt to delete excluded range scopes or remove them manually from the database before discovery will run.

Be aware of the following when using the Discovery Wizard:

- If valid information is entered in the required fields of an authentication profile or network scope, the information is automatically saved when you click **Next**. Required fields are outlined in red.
- Passwords for authentication profiles are displayed as asterisks. If you want to see a password as you enter it, click the *show password* icon next to the **Password** field. When you click **Next**, the password is displayed as asterisks.

Once you have run discovery, you can update the inventory list manually by selecting a root, agent, or scope and clicking on the discovery icon at the top of the inventory list.

---

## Contents

### Launch the Discovery Wizard

#### Follow these steps:

- Click the Discover Devices in Setup Wizard of the left navigation in the Operator Console

Or

- Delect **Discovery Wizard** from the **Actions** menu in the Inventory View.

### Create Authentication Profiles

Authentication profiles allow you to create, edit, view, and delete authentication profiles for discovery. An authentication profile contains credential information necessary for discovery to access and gather information about computer systems and devices in your network.

You can create one or more authentication profiles under each of the WMI, Linux/Unix, and SNMP tabs.

#### **NOTE**

Creating authentication profiles is not required for discovery. However, only IP discovery is used if no authentication profiles exist, and information about discovered systems might be limited.

#### Follow these steps to create an authentication profile:

1. Navigate to Discover Devices and select the desired Discovery agent.
  2. Click **New (+)** in the left pane.
  3. Enter information in all of the required fields. Required fields are outlined in red.
  4. Click **Next**. The information that you enter is saved when you click **Next** and move through the Discovery Wizard.
- To view the properties of an existing profile, select the appropriate authentication tab, and select a profile in the left pane.
  - To modify an existing authentication profile, select it and edit the fields as necessary, then click **Save**. To delete an authentication profile, click the trash can icon next to the name of the profile in the left pane, and click **Update**.

Configuration details are specific to each protocol, such as acceptable credential formats:

### Linux/Unix

Linux/Unix authentication profiles use SSH or Telnet to access and discover Linux and Unix systems.

- **Description** - Name for the authentication profile.
- **ID** -This read-only field is the UIM system ID for this authentication profile, assigned when the profile is saved. It identifies the profile uniquely for reuse in other areas of OC that reference authentication profiles.
- **User** -User name.
- **Password** -The user password. Check the **Show new passwords** check box to verify the text as you enter it.
- **SSH or Telnet** -Select the communication protocol to use, SSH (Secure Shell) or Telnet (no secure authentication or encryption).

#### **NOTE**

Discovery Agent uses password authentication to connect to a target device over SSH. Discovery Agent cannot communicate with a device where SSH is configured for other authentication methods, such as keyboard-interactive or challenge-response authentication.

## SNMP

Discovery supports SNMP versions 1, 2c, and 3. SNMP v3 provides security features that are not available in v1 and v2c. As a result, authentication profile configuration fields in the Discovery Wizard that deal with security and privacy (encryption) are only active when you select **3** in the **Version** pull-down menu.

### NOTE

SNMP authentication profiles can also be imported from an XML file. See [Run File-based Import](#) for details.

We recommend the following best practices:

- Create a minimal set of SNMP authentication profiles that will, in aggregate, provide SNMP access to all your network devices and hosts that support SNMP.
- Set up as many of your network devices as possible to use "universal" read-only credentials. For example, you could define a read-only (get-only) credential to be **nms\_get\_only**. Then set up every device possible to allow read-only SNMP access via this universal credential. This minimizes the number of SNMP authentication credentials that must be attempted on network nodes, and simplifies your discovery configuration.
- If there are devices that accept unique SNMP credentials, create one authentication profile for each of those. You can specify a unique port within the range of 1 to 65535 for the profile. If no port is specified, the default port 161 is used.
- For network devices such as routers and switches, SNMP is the sole source for detailed discovery information. For host systems such as Windows, Unix, or Linux servers, it is recommended that you use WMI or SSH discovery in addition to SNMP. While SNMP provides the most complete network interface information for devices and systems, the host system information available from SNMP, such as processor attributes, is less complete than the information obtained from WMI or SSH discovery. Enabling the combination of WMI or SSH discovery plus SNMP discovery for host systems provides the most comprehensive set of host and network interface information.
- For devices that are enabled with the CA SystemEDGE agent, you can create SNMP authentication profiles and monitor them with the snmpcollector probe (v3.0 and later). For more information, see [Monitor SystemEDGE-enabled Devices with the snmpcollector Probe](#) in the How to Articles section of the [Probes Documentation Space](#).

### SNMP v1 or v2 Fields

The SNMP community string. Check **Show new passwords** to verify the text as you enter it. This string is sent across the network in clear text as part of SNMP v1 or v2c requests, which might pose a security risk.

| Field       | Required | Description                                                                                                                      |
|-------------|----------|----------------------------------------------------------------------------------------------------------------------------------|
| Description | Yes      | Name for the authentication profile                                                                                              |
| ID          |          | The SNMP version that is supported by the monitored device. When version 1 or 2 is selected, only the Community field is active. |
| Version     | No       | The SNMP version that is supported by the monitored device. When version 1 or 2 is selected, only the Community field is active. |
| Community   | Yes      |                                                                                                                                  |

### SNMP v3 Fields

| Field       | Required | Description                                                                                                                                                          |
|-------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | Yes      | Name for the authentication profile                                                                                                                                  |
| ID          |          |                                                                                                                                                                      |
| Version     | Yes      | SNMP version that is supported by the monitored device. Versions 1, 2c, and 3 are supported. When v3 is selected, other fields for security and privacy are enabled. |

|               |                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password      | Enabled and required if <b>AuthNoPriv</b> or <b>AuthPriv</b> is selected (see <i>Security</i> description). | The password that is associated with the SNMP v1/v2c device or SNMP v3 user. Check <b>Show new passwords</b> to verify the text as you enter it. This field is enabled and required if either AuthNoPriv or AuthPriv security is selected. See the following description for the Security field .                                                                                                                |
| User          | Yes                                                                                                         | SNMP v3 user name that is used to access the monitored device. Required for all SNMP v3 security levels. See the description for the Security field below.                                                                                                                                                                                                                                                       |
| Method        | Yes                                                                                                         | SNMP v3 method of encryption, when AuthNoPriv or AuthPriv security is selected (see the following description for the Security field): <ul style="list-style-type: none"> <li>• <b>MD5</b> - MD5 Message-Digest Algorithm (HMAC-MD5-96).</li> <li>• <b>SHA</b> - Secure Hash Algorithm (HMAC-SHA-96).</li> <li>• <b>None</b>.</li> </ul>                                                                         |
| Security      | Yes                                                                                                         | SNMP v3 security level of the user. Depending on what level of security is selected, other security fields are enabled or disabled: <ul style="list-style-type: none"> <li>• <b>NoAuthNoPriv</b> - messages sent unauthenticated and unencrypted.</li> <li>• <b>AuthNoPriv</b> - messages sent authenticated but unencrypted.</li> <li>• <b>AuthPriv</b> - messages sent authenticated and encrypted.</li> </ul> |
| Priv.Password | Enabled and required if <b>AuthPriv</b> is selected.                                                        | SNMP v3 privacy password to use if <b>AuthPriv</b> security level is selected. Must be at least eight characters. Do not confuse with the user password (authentication).                                                                                                                                                                                                                                        |
| Priv.Protocol | Enabled and required if <b>AuthPriv</b> is selected.                                                        | SNMP v3 privacy (encryption) protocol to use. <ul style="list-style-type: none"> <li>• <b>DES</b> - Data Encryption Standard.</li> <li>• <b>AES</b> - Advanced Encryption Standard.</li> </ul>                                                                                                                                                                                                                   |

## WMI

WMI (Windows Management Interface) discovery scans servers and hosts running Windows to gather system information. WMI discovery runs only on discovery agents that are hosted on Windows systems.

- **Description** - Name for the authentication profile.
- **ID** - This read-only field is the system ID for this authentication profile, assigned when the profile is saved. It identifies the profile uniquely for reuse in other areas of OC that reference authentication profiles.
- **User** - User name in the form of **Domain\user name**. **user\_name** and **IP\_address\user\_name** are also allowable.
- **Password** - User password. Check the **Show new passwords** check box to view the text as you enter it.

## Define Scopes

Use the **Define Scopes** tab of the Discovery Wizard to define network seed devices, addresses, ranges, or masks where devices are to be discovered. At least one network range must be entered for discovery to run.

You can assign any combination of SNMP, Linux/Unix, and WMI authentication profiles to a range scope. The discovery process records *any* device within a range that responds to a request on any protocol, including a simple ICMP ping. This means you can include end nodes (such as servers, network printers, network storage systems, or workstations) in a range, even if they don't respond to requests using SNMP or other management protocols.

If no authentication profile is assigned to either a range scope, basic discovery is performed using protocols that do not require authentication, but discovery might not be complete and information about discovered systems is limited.

### **WARNING**

You must use IP addresses when populating scopes. Hostnames are not supported.

### **Best Practices for Creating Scopes**

For each discovery agent, review the assigned range scopes to minimize predictable timeouts. To optimize performance and avoid duplicate entries, each discovery agent should discover an exclusive part of the network.

Tips to decrease discovery run time:

- The discovery agent tries each credential on each IP address and waits for a timeout (or success) with each attempt. Use a single credential in a scope that has a high probability of immediate success on the nodes in that scope to speed up discovery.
- When you apply an authentication profile to a scope, verify that most, if not all, devices that are defined by that scope accept the authentication profile.
- If you include devices that do not respond to requests on any management protocol, place them in a discovery range scope with no authentication profiles assigned to the scope.
- If you use SNMP for a device that accepts only a unique SNMP community string, create a Single type range scope and specify the device IP address. Assign the corresponding authentication profile to the range scope.
- When using SNMP, to avoid unnecessary authentication traps/alerts, assign only one SNMP authentication credential per discovery range.

### **Create Range Scopes**

**Follow these steps:**

1. Click New (+) in the left pane of the **Define Scopes** tab.
2. Enter a name for the range scope.
3. In the Range Scope definition section, specify the area of your network where you want to perform discovery.
  - Mask - Defines a subnet using Classless Inter-Domain Routing (CIDR) notation with a base IPv4 address and a routing prefix. For example, 195.51.100.0/24. The value /24 refers to a Class C subnet of 256 addresses. Other values for reference: /30 (4 addresses) and /16 (65,536 addresses, or a Class B subnet).

### **NOTE**

When you enter a subnet mask, the number of IP addresses the mask represents is displayed (the number of effective hosts minus 2). Only /16 subnets or smaller are supported.

- Range - Range of IPv4 addresses.
  - Single IPv4 or IPv6 address. You can use abbreviated IPv6 address forms, and IPv6 addresses that refer to IPv4 addresses. However, anycast, multicast, link-local, and loopback addresses are not supported.
4. Click **New IP range or single IP address** to add another IP range, address, or mask if desired.
  5. In the Credentials section, you can assign authentication profiles to the selected range. By default, all of the authentication profiles are selected. If you have many authentication profiles in the list, you can enter the name of a profile to filter the list.
  6. To view only the profiles that are selected, click the **Hide unused credentials** check box.



## **Assign Authentication Profiles**

In the Credentials section, you can assign authentication profiles to the selected range. By default, all of the authentication profiles are selected. Seed scopes require at least one SNMP credential. If the LAN checkbox is selected, you must assign the authentication profiles that are applicable to all devices in the local subnets covered by the seed device.

When you have finished defining scopes, click **Next**.

## **Remove a Scope**

You can remove a scope by clicking on the trashcan icon next to a scope on the **Scopes** tab of the Discovery Wizard.

## **View Discovered Systems**

The **Inventory** section allows you to view computers and devices that have been discovered on your network.

The Inventory section contains discovery agents, with network scopes under each discovery agent. The tree also has an Automatic and an External node.

Icons next to the tree nodes help identify the type of node and provide additional information:



Top-level Inventory node or discovery agent.



- Network scope.



- Automatic. Some probes automatically discover systems, and those systems are displayed under this node.



- External. Systems that are listed under this node were imported using file-based discovery.



- A discovery is scheduled. Hover over the icon to see the next scheduled time in the tool tip.



- Discovery in progress. The proportion of blue indicates the progress of discovery.



- No discovery scheduled.

Click a node in the tree to view associated systems and their properties in the table to the right. To view properties for all discovered systems, click the desired node in the tree view of the **Inventory**.

### **NOTE**

Systems that do not respond are eventually purged from the database. By default, 30 days after the last response from a system, the system is deleted from the database.

A Quick Filter field below the response links allows you to filter for text in the **Name**, **IP Address**, **Domain**, **OS Name**, and **Origin** columns of the table.

Click a column header to sort the table by the column.

A key icon in the table indicates that a discovery agent was able to authenticate with the system using one of the defined authentication profiles. Hover over the key icon to view the type and name of the authentication profile used.

You can export data for a discovery agent or network range scope. The data includes more columns than are displayed in the Inventory table. Data is exported to a .csv file, which is saved in a location you choose. To export data, click a discovery agent or network range scope in the tree, then select **Export Group** from the **Actions** menu.

**NOTE**

When you choose **Export Group**, all systems for the selected discovery agent, or selected network range scope, are exported, regardless of whether you filtered the display in the Inventory view.

**Discover Now**

You can focus discovery on an agent or subset of scopes independently of the Discovery Wizard. This allows you to discover devices on a portion of the inventory—for example, to update the inventory after maintenance.

**Follow these steps:**

1. Select an **agent** or **scope** in the Discovery Wizard from the Settings view in OC.
2. Select **Run Discover now**.
3. Click the **Finish** button.

**NOTE**

Only one discovery can be run at a time. Starting a new discovery preempts a currently running discovery.

## Use Application Discovery

Application Discovery enables system administrator bus users to automatically discover, to group, and to monitor devices in their environment. Application Discovery comes with default scripts that determine the discovery of the applications that are running on your monitored systems:

- Apache
- Active Directory
- Exchange Server
- IIS
- MySQL
- Microsoft SQL
- Oracle
- Sharepoint

In the Administration of the Settings View in the Operator Console, you select which applications that you want the Application Discovery scripts to discover. In the Monitoring Configuration Service (MCS), you then select which default monitoring profiles that you want to enable. You view the monitoring data in the CA UIM visualization components, including OC or the CABI Dashboards for CA UIM. If the default scripts do not discover the devices that you want to find in your environment, you can create custom scripts.

**NOTE**

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

**Contents**

## Workflow

Before you start the workflow for the Application Discovery feature, verify that you meet the prerequisites. The prerequisites include installing the robot 9.31 (or later) on your primary hub and all the devices that you want to monitor. You must also have the Attribute Publisher plug-in in your archive. The robot and Attribute Publisher plug-in work with the `nis_server` and the CA UIM database to enable discovery of devices by application.

1. To activate Application Discovery, select at least one of the applications that the feature can discover and monitor. Select them in the Administration pane of the Settings View in Operator Console. In the Administration pane, select one or more of the Application Discovery groups that you want to discover and monitor.  
**Note:** The Application Discovery feature depends on the Application Discovery Unix and Windows groups to push the Attribute Publisher plug-in that contains the discovery scripts to monitoring targets. Therefore, the Application Discovery groups for Unix and Windows are automatically selected when you select any one of the other Application Discovery groups and click **Save**.
2. When you select at least one Application Discovery group and save the change, MCS pushes the Attribute Publisher plug-in out to the robots installed on the devices in your monitoring environment. The plug-in runs a discovery script to identify devices based on the desired attribute. For example, if you select the Application Discovery: Apache group, the discovery script for Apache identifies devices that host an Apache server.
3. In the OC, these identified devices appear in the Discovered Application Systems group. Devices are placed in subgroups based on their attribute, such as Apache server. To configure a monitoring profile for a subgroup, select the desired subgroup in the Groups view. Then click on the **Monitoring Config**



( icon in the right top menu. )

4. When you click the Monitoring Config, the MCS configuration pane appears. The available profile types for each device appear in the MCS pane. MCS automatically determines these available profile types for each subgroup based on its role. For more information, see [Monitoring Configuration Service](#).
5. To activate monitoring for a subgroup, such as Apache, you need *only* to enable the configuration profile for it. It is optional to configure any other profile that is available for the subgroup. To activate monitoring for a subgroup, such as Apache, click on the arrow next to the profile type to expand it. Then, click on the configuration profile for the subgroup, such as Discovered Apache. You can either accept the default configuration or modify it. Apply the profile configuration by clicking **Enable** to activate the profile.

### NOTE

The Application Discovery group profiles appear with an orange pause



( icon that indicates they are in a suspended state. To apply monitoring to a group, accept or modify the default configuration in the profile and then click **Enable**. Once you enable a profile, the suspended icon goes away and a **Save** button replaces the **Enable** button. )

6. When you enable a profile, MCS deploys the necessary probes to all the devices in the subgroup. The probes publish alarms and Key Performance Indicators (KPIs or metrics) for each device that you can view in CA Unified Infrastructure Management, including the OC and the CABI Dashboard for CA Unified Infrastructure Management for the relevant MCS profile.

### NOTE

- If the necessary probes are not in the archive or are missing a license, you see an error message at the top of the profile.
- From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).
- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view

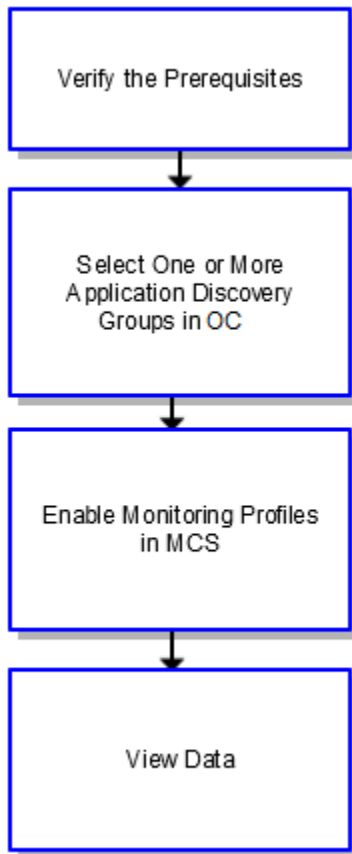
page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

#### NOTE

#### Workflow Diagram

The following diagram shows the workflow for grouping and monitoring devices with the Application Discovery feature:

**Figure 21: ApplicationDiscovery\_workflow**



#### Key Terms

- **Administration Tile and Pane**

To activate Application Discovery, select at least one of the applications that the feature can discover and monitor. Do this in the Settings view of the Operator Console by clicking the Administration tile. When you click on the tile, the Administration pane appears. In the Administration pane, select one or more of the Application Discovery groups that you want to discover and monitor.

**Note:** If you open the Administration pane in OC, and you see that the Application Discovery: Unix and Application Discovery: Windows groups are already selected, then Application Discovery monitoring is already configured. Unless you want to remove the previous Application Discovery configuration, do *not* clear the selection of either group.

- **Attribute Publisher Plug-in**

A plug-in called the Attribute Publisher runs one or more discovery scripts to identify devices based on the attributes of each device. The Attribute Publisher is a plug-in that works with the robot 7.90 or later. An attribute is the role that a device plays, such as an Apache server. You determine the script or scripts that the plug-in runs by selecting one or more Application Discovery groups in the Administration pane of OC.

- **Discovered Application Systems Group**

The Discovered Application Systems group appears in the navigation tree in Inventory view of the OC. The Discovered Application Systems group is populated with subgroups of the devices that are identified and tagged by attribute. An attribute can be an application, operating system, or other role that the device plays in your environment. Once the Discovered Application Systems group is populated with these subgroups, you can select any subgroup. You manage a subgroup, similar to how you manage any other group, using OC. You configure monitoring for a subgroup using MCS.

- **Monitoring Config**

The Monitoring Config appears in the top right of the Groups view in OC, and it is highlighted when a group or subgroup is selected. After you select the desired group or subgroup in the Groups view of OC, you click on the Monitoring Config to open the MCS pane.

- **MCS Pane**

The profile types that you use to create configuration profiles appear in the MCS pane.

- **nis\_server**

When you first install CA UIM, the `nis_server` creates groups of devices. The `nis_server` initiates a discovery to interrogate these devices for the applications that you can discover and monitor with the Application Discovery feature. The `nis_server` tags any active applications that it discovers in your environment with the relevant attributes. An attribute is the role that a device plays, such as an Apache server. The Attribute Publisher then executes application discovery scripts. An application discovery script, such as the one for Apache, searches the CA UIM database for devices that the `nis_server` has tagged with the relevant attribute.

- **Setup Application Discovery Group**

The Setup Application Discovery group appears in the navigation tree in Groups view of OC. The Setup Application Discovery group contains a UNIX subgroup and a Windows subgroup. (*Optional*) The default configuration for the subgroup is applied automatically. Or, if you want to change the default values for the subgroup, select the UNIX or Windows subgroup that is relevant to your environment. Click the Monitoring Config for the MCS pane. Click the add (+) icon and select the desired Application Discovery profile:

- **Application Discovery Scripts Profile** (*Optional*) Use this profile to *change the default values* for the discovery scripts that are provided for the Application Discovery feature. Or, if you have written your own custom discovery script, enter the Package Name and Script Filename for your script in the Script Package Profile section of this profile.
  - **Group Profile Priority:** Enter a Group Profile Priority. The Group Profile Priority is used to determine the precedence of configuration profiles. For devices that are members of several groups, the configuration profile with the higher Group Profile Priority number is applied. Possible values are 0 to 100. The default value is 100.
  - **Package Name:** Enter a package name. The default value is the script filename.
  - **Script Filename:** Enter a script filename.
  - **Interval:** Select the interval at which the scripts, including those which ship with the Application Discovery feature, discover devices to monitor. The default value is 15 minutes. The interval value that you enter here overrides the interval value in the Set Up Application Discovery Defaults Profile.
- **Setup Application Discovery Defaults Profile** (*Optional*) Use this profile to *change the default values* for the Application Discovery feature.
  - **Group Profile Priority:** Enter a Group Profile Priority. The Group Profile Priority is used to determine the precedence of configuration profiles. For devices that are members of several groups, the configuration

profile with the higher Group Profile Priority number is applied. Possible values are 0 to 100. The default value is 100.

- **Interval:** Select the interval at which any custom Application Discovery scripts discover devices to monitor. The default interval value is one day.
- **Grace Period:** Select the interval (seconds) at which devices are deleted if they were previously discovered but now fail to respond. The default value is 259200 (three days).
- **Scripts Path:** If you want to use custom scripts, enter the path that you want to use for your custom discovery scripts. Otherwise, leave the default value.

## **Verify Prerequisites**

### **Meet the Software Requirements**

- On the primary hub:
  - CA Unified Infrastructure Management server v20.3 or later
  - CA Unified Infrastructure Management robot v9.31 or later
- On all the devices that you want to monitor:
  - CA Unified Infrastructure Management robot v9.31 or later
  - Note:** For more information about how to deploy robots, see [Deploy Robots](#).
- In the archive on a hub:
  - nis\_server v20.1 or later
  - Attribute Publisher plug-in (attr\_publisher) v9.31 or later
  - The latest versions of the following probes:
    - ad\_server
    - apache
    - exchange\_monitor
    - iis
    - perfmon (required for iis and exchange\_monitor)
    - processes (required for exchange\_monitor)
    - mysql
    - ntservices (required for exchange\_monitor)
    - sqlserver
    - oracle

For the oracle probe, verify that you meet the prerequisites that are described in the [oracle \(Oracle Database Monitoring\) Release Notes](#) on the Probes Documentation Space.
- (Optional) Install CA Business Intelligence with CA UIM 20.3

**Important!** If you are upgrading from a previous version of CA UIM and want to keep the MCS configuration that you have set in your profile templates for the applications that are affected by Application Discovery, see the [Monitoring Configuration Service Release Notes](#) on the Probes Documentation Space.

### **(Optional) Set Up and Run Discovery in OC**


If you want to ensure that the Discovered Application Systems group contains any recently added devices, you can run Discovery in OC before you configure any monitoring. You can launch the Discovery Wizard whenever you want to run discovery or change your discovery settings.

For more information about Discovery, see [Run Discovery in OC](#).

### **Configure and Enable Monitoring Profiles**

1. In the OC, click on the Administration tile of the Settings View.

2. In the Administration pane, select one or more of the Application Discovery groups that you want to discover and monitor.  
**Note:** The Application Discovery feature depends on the Application Discovery Unix and Windows groups to push the Attribute Publisher plug-in that contains the discovery scripts to monitoring targets. Therefore, the Application Discovery groups for Unix and Windows are automatically selected when you select any one of the other Application Discovery groups. If you open the Administration pane in OC, and you see that the Application Discovery: Unix and Application Discovery: Windows groups are already selected, then Application Discovery monitoring is already configured. Unless you want to remove the previous Application Discovery configuration, do *not* clear the selection of either group.
3. Click **Save**.  
MCS pushes the Attribute Publisher plug-in out to the robots that are installed on the devices in your monitoring environment. The plug-in runs a discovery script to identify devices based on the desired attribute. For example, if you select the Application Discovery: Apache group, the discovery script for Apache identifies devices that host an Apache server. In OC, these identified devices appear in the Discovered Application Systems group. Devices are placed in subgroups based on their attribute, such as Apache server.
4. In the navigation tree of the Groups view, select the desired subgroup.  
For example, Apache.
5. Click on the **Monitoring Config**


(

icon in the right top menu.

The MCS configuration pane appears. The available profile types for each device appear in the MCS pane.

**Note:** The Application Discovery group profiles appear with an orange pause icon that indicates they are in a suspended state.

)
6. Click the profile type to expand it. Then, click on the configuration profile for the subgroup.  
For example, Discovered Apache.
7. Accept the default configuration in the profile or modify it.
8. Click **Enable** (or **Save**) at the bottom of each profile to save your changes and to activate the profile.  
**Note:** When you click **Enable**, the profile is active. Thereafter, the **Enable** button goes away and is replaced by a **Save** button. You cannot put the profile back to a suspended state.
9. Repeat steps 1 through 7 as needed.

#### NOTE

When you use the Application Discovery feature, the rules for group and device configuration in MCS apply as usual. For more information about MCS, see [Monitoring Configuration Service](#).

### View Data in Unified Infrastructure Management

When you activate a profile, MCS deploys the necessary probes to all the devices in the subgroup. The probes publish alarms and Key Performance Indicators (KPIs or metrics) for each device that you can view in CA UIM, including the OC and the CABI Dashboard for CA UIM for the relevant MCS profile.

### View Discovered Application Systems Groups in OC

You view a Discovered Application Systems group like you view any group using OC. The Discovered Application Systems group appears in the navigation tree in the Groups view of OC. The Discovered Application Systems group is populated with subgroups of devices that are identified and tagged by attribute. An attribute can be an application, operating system, or other role that the device plays in your environment. Once the Discovered Application Systems group is populated with these subgroups, you can select any subgroup to manage it in OC.

### **(Optional) Use SQL Queries to Filter Application Groups**

You manage a Discovered Application Systems group like you manage any group using OC. Flexible grouping features allow you to organize your infrastructure into a hierarchy of static and dynamic groups and subgroups. You can organize groups according to concepts, such as service, customer, organization, or technology. You can also create or modify groups based on specific attributes or combinations of attributes in the group filters.

The Application Discovery monitoring profiles create additional SQL queries to define membership for each group. The queries appear as group filters. To view the SQL query, select or hover over a group name and click the **Edit group** (gear) icon to the right. In the filter at the bottom of the screen, click the **Edit query...** link. You can edit these filters to modify the member devices in each group.

**Note:** SQL queries are a powerful way to filter the members of a Discovered Application Systems group in OC. Therefore, we recommend that you use them only if you are familiar with how to format an SQL query.

For more information about using filters for groups, see [Create and Manage Groups in OC](#).

### **(Optional) View Data in the Default CABI Dashboard for CA UIM**

Before you can view data in the Default CABI Dashboard for CA UIM, first you must install CA Business Intelligence with CA UIM.

#### **NOTE**

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

### **Known Issues**

- If you remove a device from monitoring, the device continues to appear in the OC UI for up to three days. This is expected behavior because the grace period, the interval at which devices are deleted if they were previously discovered but now fail to respond, is three days.
- If the hostnames for Windows devices are not unique, device correlation might not be accurate.

### **Known Issues with Workarounds**

#### **Oracle Devices**

##### **Symptom**

You see that no QoS or alarms are generated for the Discovered Oracle monitoring profile in MCS, which you have enabled.

##### **Test Connection in IM**

##### **Follow these steps:**

1. In IM, double-click the probe.
2. Click the Connections tab.
3. Double-click the profile **Discovered Oracle**.
4. Click the **Test** button.
5. You see an error stating that a connection cannot be made. You might also see a message that states: Create OCI environment failed with rc = -1.

##### **Test Connection in AC**



**Follow these steps:**

1. Open **Admin Console**.
2. In the top ribbon, click **Robots**.
3. Click the name of the robot that hosts the oracle probe.
4. In the top ribbon, click **Probes**.
5. Click the Options (...) icon next to the probe and select **Configure**.  
A new browser tab appears.
6. Click **Discovered Oracle**.
7. From the Action button select **Test Connection**.  
You see the error "Message: Unable to start the probe as either the Database client is not installed or any other pre-requisite step is pending."

**Solution**

To use the Application Discovery feature to discover and monitor Oracle devices, you must modify the connection settings in the Discovered Oracle MCS monitoring profile. (Modifying the connection settings in IM does not work because MCS overwrites them when it deploys the oracle probe.) You must also configure the environmental variables for the robot.

**Modify the Profile and Database Instance Connection Settings****Follow these steps:**

1. In the Groups View of the Operator Console, go the Monitoring Config.
2. Select the Discovered Oracle profile.
3. In the Discovered Oracle profile, go to Profile and Database Instance Connection Settings. Enter the following information:
  - **User ID:** defines the user ID with authorization to read the database views.  
Enter: SYS AS SYSDBA
  - **Password:** specifies the password for the defined **User ID**. The password is encrypted and placed into the configuration file.  
Enter: A valid password for the "SYS" User ID
  - **Service Name:** specifies the service name that is defined in the **tnsnames.ora** file.  
For example, ORCL.
4. Click **Save**.

**Configure the Robot Environment Variables**

To configure the robot environment variables, use the controller probe.

**Follow these steps:**

1. In Infrastructure Manager, double-click the controller probe.
2. Select the Environment tab.
3. Right-click in the window. Select **New** or **Edit** to add or edit the following variables and their values:

| Variable        | Example Value                                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
|                 | <b>Note:</b> The example values in the table below might vary from your values. Verify the correct values for your system. |
| LD_LIBRARY_PATH | /home/oracle/app/oracle/product/12.1.0/dbhome_1/lib                                                                        |
| ORACLE_HOME     | /home/oracle/app/oracle/product/12.1.0/dbhome_1                                                                            |
| ORACLE_BASE     | /home/oracle/app                                                                                                           |
| ORACLE_SID      | orcl.ca.com                                                                                                                |
| PATH            | \$PATH:/ /home/oracle/app/oracle/product/12.1.0/dbhome_1/lib                                                               |

TNS\_ADMIN

/home/oracle/app/oracle/product/12.1.0/dbhome\_1/network/admin

## Manage Groups

UIM creates several groups to get you started. You can monitor your cloud accounts and your on-premises devices using these groups. You can create more groups to organize the devices in your environment for the following reasons:

- **More meaningful alarms and dashboards** - You can group your devices with similar monitoring requirements to view metrics and alarms data for specific situations.
- **Easier navigation** - By creating groups that are meaningful to your organization, it can be easier for users to navigate to desired devices and interfaces.
- **Easier to determine monitoring profiles** - You might find it easier to troubleshoot issues when group profiles are applied to devices and interfaces in a group.
- **View dashboards** that generate information about all of the members in each group.
- **Apply the same monitoring settings** to all the devices and interfaces in the group.

### Types of Groups in OC

The following are the different types of groups in Operator Console:

- **Container:** Container groups contain other groups (sub-groups). For example, the default group Operating System is a container group with UNIX and Windows as the sub-groups.
- **Static:** Static groups contain a specified list of devices. Once you specify the list of devices that are members of the group, the membership does not change unless you manually add or remove devices and interfaces.
- **Dynamic:** Dynamic groups contain devices that meet a specified set of criteria. Dynamic groups, such as the Windows and Linux groups, are created automatically based on the OS Type or monitoring technology (for example, VMware or AWS). In addition, you can create your own dynamic groups and can define a filter to add the devices that match the filter to your group. The membership of dynamic groups is updated automatically on a configurable interval. Typically, you create a dynamic group when you want to monitor specific devices that are discovered after a device discovery. For example, you want to monitor all database servers that belong to a specific region. For this, you can create a dynamic group for the region and configure the group to accept only the database servers that are discovered during the device discovery. After the devices are discovered, those that match the dynamic group criteria get added to it.

We recommend that you add a device to only one group for MCS grouping. Always implement non-overlapping management privileges for any element that is managed through CA UIM. All users who can create monitoring profiles for computer systems or elements must be able to see the element, the actual profile, and any potential group profiles. This avoids situations where multiple users can unknowingly apply conflicting configuration profiles to the same device.

#### **NOTE**

In UIM 20.3.3, the new OC Group Add, OC Group Edit, and OC Group Delete ACL permissions provide the required access to create, edit, and delete groups, respectively. These permissions allow you to authorize only the required users to perform the appropriate group operations. For example, if you do not want to give the delete group permission to a specific user, you can disable the OC Group Delete permission for that user, and enable the OC Group Add and OC Group Edit permissions.

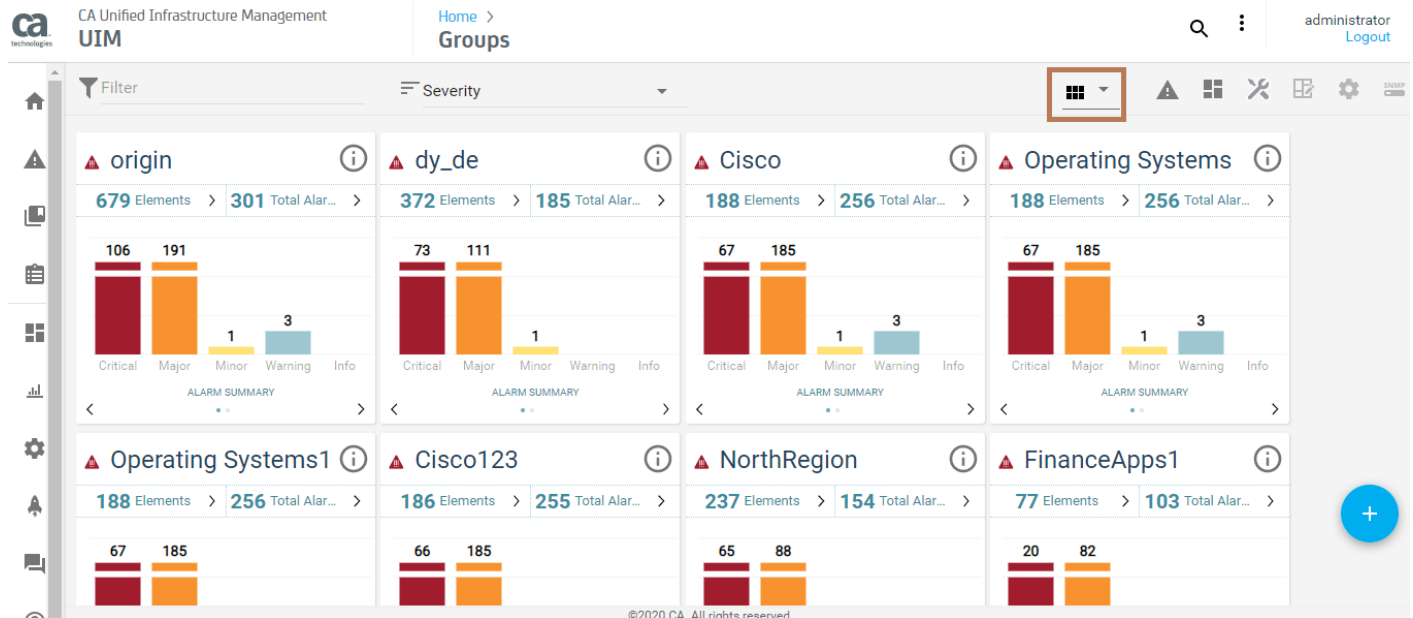
Note that the OC Group Modification permission is also available. Users with this permission are allowed to create, edit, and delete groups. Therefore, with the availability of the three new permissions (OC Group Add, OC Group Edit, and OC Group Delete) along with OC Group Modification, you can decide which permission you want to use for your users. If you want your users to perform all the operations, you can use OC Group Modification. However, if you want to allow only a specific task, you can then use the associated permission.

### View Groups

The Groups View provides 3 types of views to display the Groups and devices. Following are the different types of views.

- **Card View**

Displays all the groups in cards with the alarm summary charts in the card.



- **List View**

Displays all the groups in list with the Group names with the alarms, and elements in the group.

CA Unified Infrastructure Management UIM | Home > Groups | administrator Logout

Filter

| Name                   | Elements |
|------------------------|----------|
| 301 origin             | 679      |
| 185 dy_de              | 372      |
| 256 Operating Systems1 | 188      |
| 256 Operating Systems  | 188      |
| 256 Cisco              | 188      |
| 255 Cisco123           | 186      |
| 154 NorthRegion        | 237      |
| 103 FinanceApps1       | 77       |
| 29 Card_Cont_Grp1      | 17       |

©2020 CA. All rights reserved.

- **Tree View**

Displays the groups in tree like structure for the navigation within the groups.

CA Unified Infrastructure Management  
UIM

Home > Groups

administrator  
Logout

Filter

Search Group

Groups (679)

- 0\_s\_i7 (4)
- 0\_st\_de (11)
- 10Aug\_Dy\_Dev (5)
- 10Aug\_Stat\_dev (5)
- 10Aug\_dy\_in (0)
- 10Aug\_stat\_in (0)
- 18Aug\_Statint (1)
- 29Jul\_Static\_Device (4)
- 29\_Container\_grp1 (8)
- 2\_stat\_interface (20)
- 4aug\_si (2)

Details

Member Group

| Name                   | Type      | Count |
|------------------------|-----------|-------|
| 301 origin             | Container | 679   |
| 185 dy_de              | Dynamic   | 372   |
| 256 Operating Systems  | Container | 188   |
| 256 Cisco              | Container | 188   |
| 256 Operating Systems1 | Container | 188   |
| 255 Cisco123           | Container | 186   |
| 154 NorthRegion        | Dynamic   | 237   |

**NOTE**

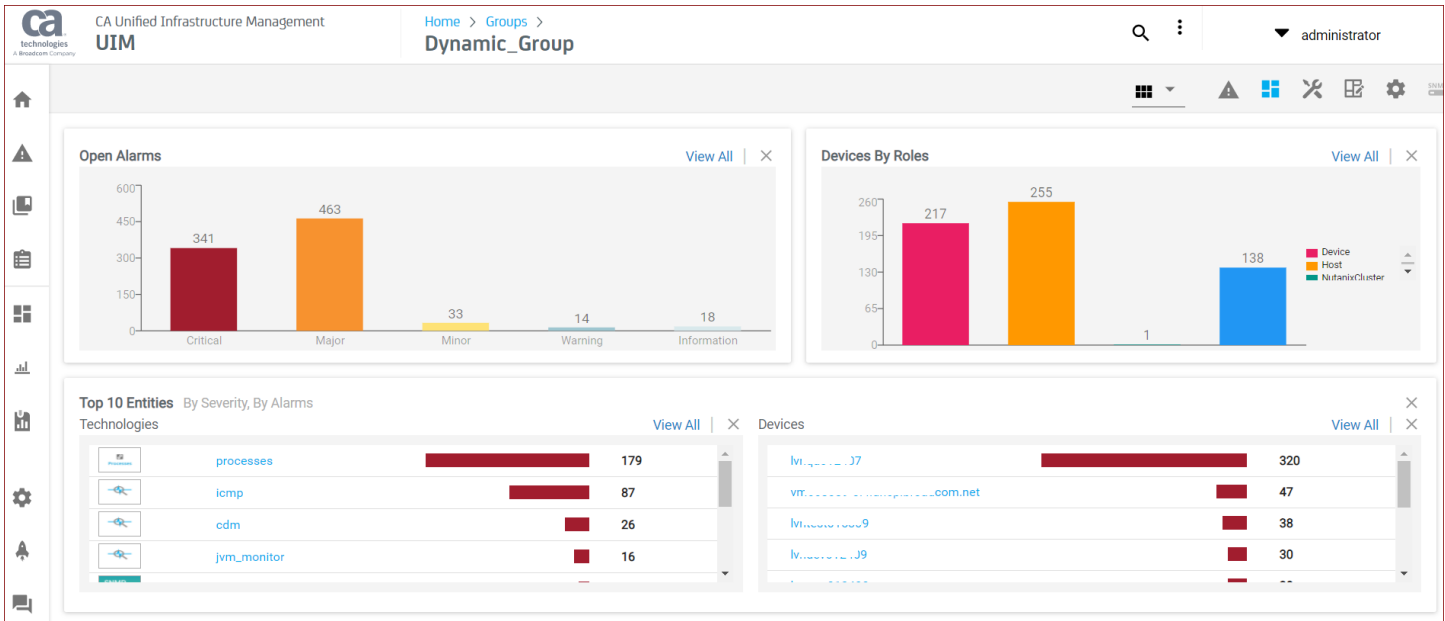
If you are logged in to Operator Console with the Operator role, you can view groups and devices and interfaces in groups. However, you cannot add, delete, or rename groups, or add and remove devices from groups.

**Group Dashboard View Page**

The following screenshot shows the group dashboards view (native OC screen) in UIM 20.3.3. This screen is rendered using HTML5; it is no longer dependent on CABI in UIM 20.3.3:

**NOTE**


UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.



You can perform the following tasks in this view:

- **Open Alarms**  
View the count of opens alarms in the group.
  - Click the View All link to navigate to the Alarms view page, which contains more details.
  - Click the respective bar on the chart to navigate to the Alarms view, which contains more details.
- **Devices By Roles**  
View the role spread of the monitored devices in the group.
  - Click the View All link to navigate to the inventory view, which provides more details.
- **Top 10 Entities**  
View the top monitored technologies/sub-groups and devices in the group. The list is sorted based on the alarm severity and then alarm count. For example, an entity having one critical alarm is displayed first in the list when compared with the entity having two major alarms. The alarm count is considered after the severity.
  - Click the View All link to navigate to the respective view, which provides more details.
  - Click the specific entity (for example, device or monitoring technology) to access the detailed information.
- **Properly Created URL**  
Use the properly formed URL to directly access the group dashboard view:`http://<OC_Server>/operatorconsole_portlet/groups/0/<CI_ID>/dashboard`
- **Remove a Tile**
  - Click X to remove a tile from the view.
- **Show/Hide a Tile**
  - Click the three-dot menu at the top-right of the UI to show or hide the tiles from the view.

## Add a Group

You can add a container, dynamic, or static group in the **Groups** (  ) view.


## Add a Container Group

Container groups contain other groups (sub-groups).

**Follow these steps:**

1. Access the Groups () view.
2. Select **Action Menu**



(  ) in the upper right, and then select **Add group**.

Configure Container Group Add ✕

| Group Name          | Group Description          | Account | Parent     | Group Type | Member Type |
|---------------------|----------------------------|---------|------------|------------|-------------|
| Container Group Add | This is a container group. | HR      | 21Dec_cont | Container  | Devices     |

CANCEL    SAVE

3. Enter the following information:
  - a. Enter a unique name for the container group.
  - b. Enter the group description.
  - c. Select the appropriate account from the drop-down list, if required.
  - d. Select a parent group that contains all the related groups. The container groups that you create gets added to the parent group that you select.
  - e. Select the **Container** option as a group type.
4. Click **Save** to create the container group.  
The container group is created. At this stage, the container group does not contain any sub-groups. You can add another container group, dynamic group, or static group to this container group based on your requirements. For dynamic and static groups, see the relevant sections in this article.

**NOTE**

In the Groups view, container groups display the count of the devices of the group and does not include any interfaces in the count.

**Add a Dynamic Group**

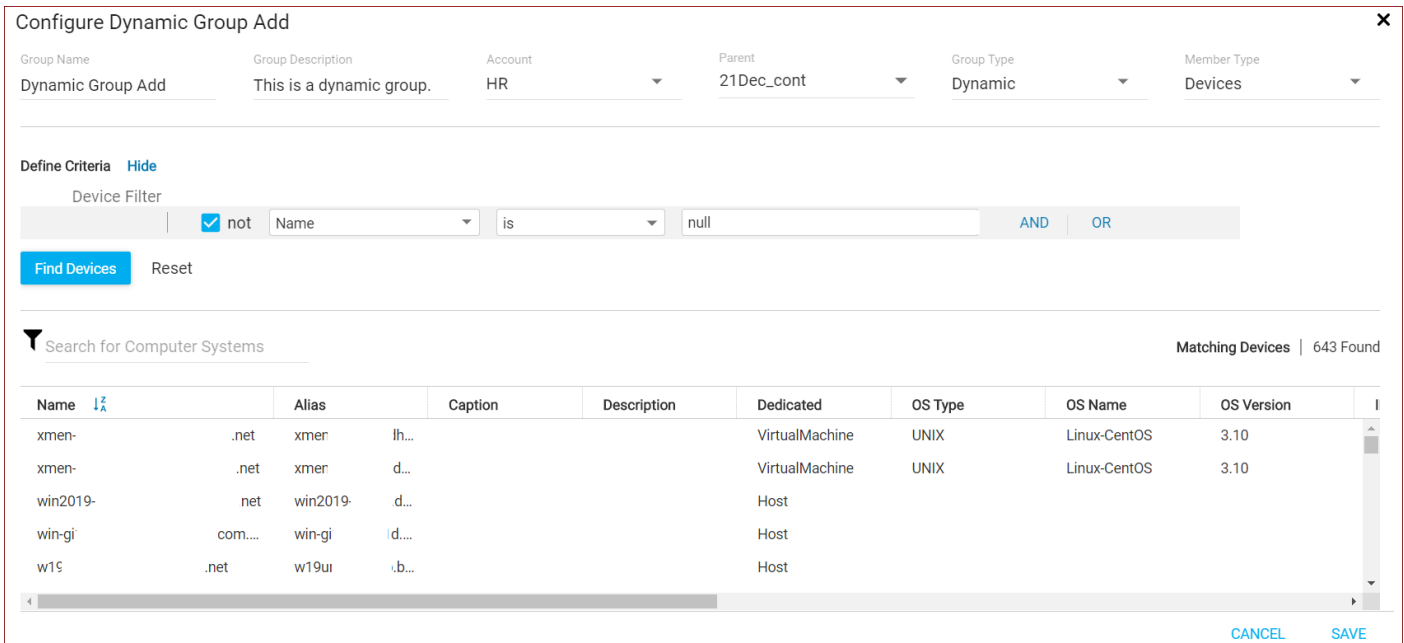
Create a dynamic group when you want to dynamically add any device that matches the filter criteria to the group.

**Follow these steps:**

1. Access the Groups () view.

2.

Select **Action Menu** (  ) in the upper right, and then select **Add group**.



Configure Dynamic Group Add

Group Name: Dynamic Group Add | Group Description: This is a dynamic group. | Account: HR | Parent: 21Dec\_cont | Group Type: Dynamic | Member Type: Devices

Define Criteria [Hide](#)

Device Filter

not Name is null [AND](#) [OR](#)

[Find Devices](#) [Reset](#)

Search for Computer Systems Matching Devices | 643 Found

| Name     | Alias  | Caption  | Description | Dedicated      | OS Type | OS Name      | OS Version |  |
|----------|--------|----------|-------------|----------------|---------|--------------|------------|--|
| xmen-    | .net   | xmer     | lh...       | VirtualMachine | UNIX    | Linux-CentOS | 3.10       |  |
| xmen-    | .net   | xmer     | d...        | VirtualMachine | UNIX    | Linux-CentOS | 3.10       |  |
| win2019- | net    | win2019- | d...        | Host           |         |              |            |  |
| win-gi   | com... | win-gi   | d...        | Host           |         |              |            |  |
| w19      | .net   | w19ut    | .b...       | Host           |         |              |            |  |

[CANCEL](#) [SAVE](#)

3. Enter the following information:

- Enter a unique name for the group.
- Enter the group description.
- Select the appropriate account from the drop-down list, if required.
- Select a parent container group that contains all the related groups. The dynamic groups that you create gets added to the parent group that you select.
- Select **Dynamic** as the group type.
- Select **Devices** or **Interfaces** from the **Member Type** drop-down list.
- Define the filter criteria and then click **Find Devices** to view the devices that match the criteria. For more information about using various filter options, see the Example: Dynamic Group Creation section and Using Filters section that are explained later in this article.

**NOTE**

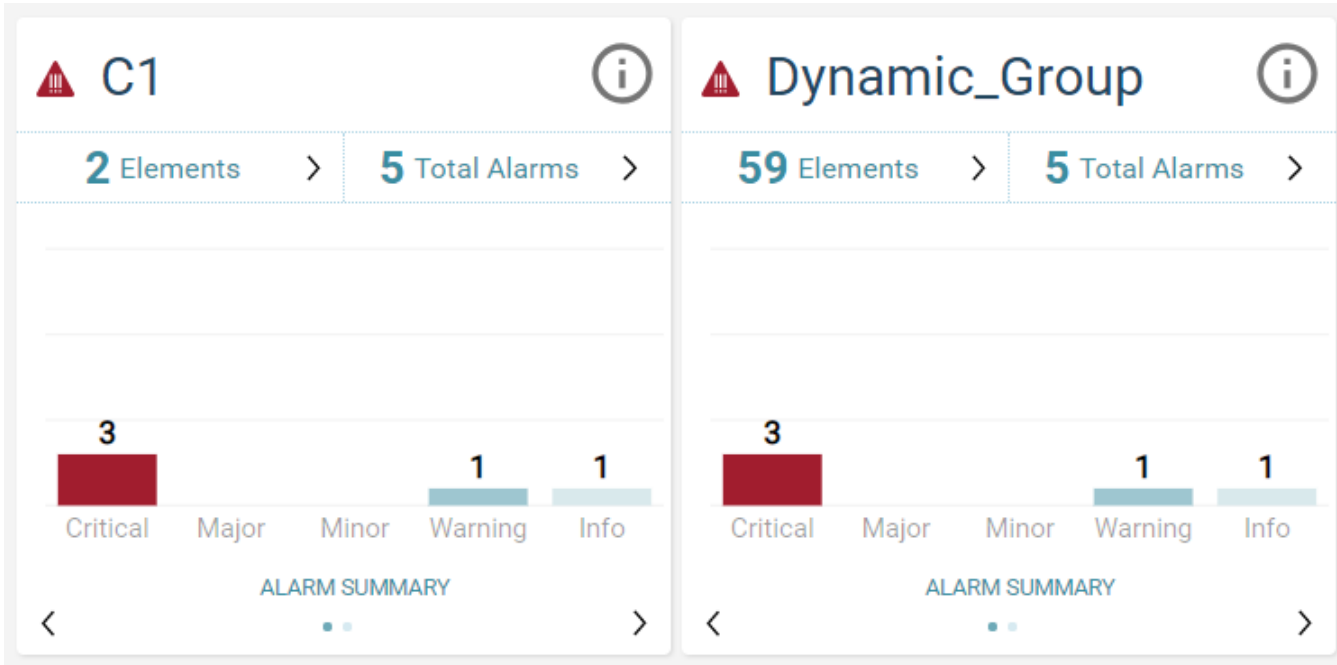
Selecting the advanced filter criteria allows you to select system or technology-specific options. For example, you can filter based on kernel version, storage capacity, or criteria specific to monitoring technologies. The filter criteria that you can view in the drop-down depends on the technologies that are monitoring the environment.

4. Click **Save** to create the dynamic group.

The dynamic group is created and the devices that match the criteria are added to the group. Subsequently, any devices that are added/discovered and match the filter criteria get added to the group.

5. Verify that the dynamic group appears in the parent group.

The following screenshot shows a dynamic group (Dynamic\_Group):



### Example: Dynamic Group Creation

The example screenshot shows how you can create a dynamic group using the following filter criteria:

- Filter all devices that have Windows operating system AND are robots.  
OR
- Filter all devices based on the advanced filter criteria: OSDescription of the virtual machine is Red Hat Enterprise Linux 7 (64-bit).

Define Criteria [Hide](#)

|                              |                         |    |                                     |     |    |   |   |
|------------------------------|-------------------------|----|-------------------------------------|-----|----|---|---|
| <input type="checkbox"/> not | OS Type                 | is | Windows                             | AND | OR | X | ↓ |
| <input type="checkbox"/> not | Bus Type                | is | Robot                               | AND | OR | X | ↑ |
| OR                           |                         |    |                                     |     |    |   |   |
| <input type="checkbox"/> not | Advanced: OSDescription | is | Red Hat Enterprise Linux 7 (64-bit) | AND | OR | X |   |

[Find Devices](#) [Reset](#)

Matching Devices | 64 Found Search

| Name         | Alias        | IP Address | Caption | Description | Dedicated      | OS Type | OS Name            |
|--------------|--------------|------------|---------|-------------|----------------|---------|--------------------|
| 03-mssql4    | 03-mssql4    |            |         |             | VirtualMachine | Windows | WindowsServer-2... |
| d2-R-Hub-Lin | d2-R-Hub-Lin |            |         |             | VirtualMachine | UNIX    | Linux              |
| 03-lrb3      | 03-lrb3      |            |         |             | VirtualMachine | UNIX    | Linux              |
| 03-doc9      | 03-doc9      |            |         |             | VirtualMachine | UNIX    | Linux              |

### Add a Static Groups

A static group is the one where you manually add devices while creating the group.



**Follow these steps:**

1. Access the **Groups** (  ) view.

2. Click **Action Menu**



menu in the upper right, and then select **Add group**.

Configure Static Group Add
✕

|                  |                         |         |            |            |             |
|------------------|-------------------------|---------|------------|------------|-------------|
| Group Name       | Group Description       | Account | Parent     | Group Type | Member Type |
| Static Group Add | This is a static group. | HR      | 21Dec_cont | Static     | Devices     |

---

**Define Criteria** [Hide](#)

Device Filter

not
 

Name ▼

 is ▼

null

AND OR

Find Devices Reset

---

▼ Search for Computer Systems < 1 2 3 4 5 6 ... 71 72 > Matching Devices | 643 Found

| <input type="checkbox"/>            | Name     | Alias    | IP addr... | Caption | Descrip... | Role | OS Type | OS Name | OS Vers... | OS Des... | Origin       | MacAd... | User Ta... | User Ta... |
|-------------------------------------|----------|----------|------------|---------|------------|------|---------|---------|------------|-----------|--------------|----------|------------|------------|
| <input checked="" type="checkbox"/> | 1. ....  | 1. ....  | 1. ....    |         |            |      |         |         |            |           | Ivi ... )... |          |            |            |
| <input checked="" type="checkbox"/> | 10. .... | 10. .... | 10. ....   |         |            |      |         |         |            |           | Ivi ... )... |          |            |            |
| <input checked="" type="checkbox"/> | 10. .... | 10. .... | 10. ....   |         |            |      |         |         |            |           | Ivn ... )... |          |            |            |

CANCEL SAVE

3. Enter the following information:

- a. Enter a unique name for the group.
- b. Enter the group description.
- c. Select the appropriate account from the drop-down list, if required.
- d. Select a parent group that contains all the related groups. The static groups that you create gets added to the parent group that you select.
- e. Select **Static** as the group type.
- f. Select **Devices** or **Interfaces** from the **Member Type** drop-down list.
- g. Define the filter criteria and then click **Find Devices** to view the devices that match the criteria. For more information about using filters, see the Using Filters section explained later in this article.

**NOTE**

Selecting the advanced filter criteria allows you to select system or technology-specific options. For example, you can filter based on kernel version, storage capacity, or criteria specific to monitoring technologies. The filter criteria that you can view in the drop-down depends on the technologies that are monitoring the environment.

h. Select the devices that you want to add to this static group.

4. Click **Save** to create the static group.

The static group is created. At this stage, the static group contains the devices that you have added to it while creating it. If you want to add more devices or remove some of the devices from the static group, you must edit the group and perform the operation.



**NOTE**

- After you create a static group and add devices, the membership does not change unless you manually add or remove devices by editing the group.
- When you save the static group, the filter criteria is not saved.

**Edit a Group**

You can edit a group if you want to perform any changes to the created groups.

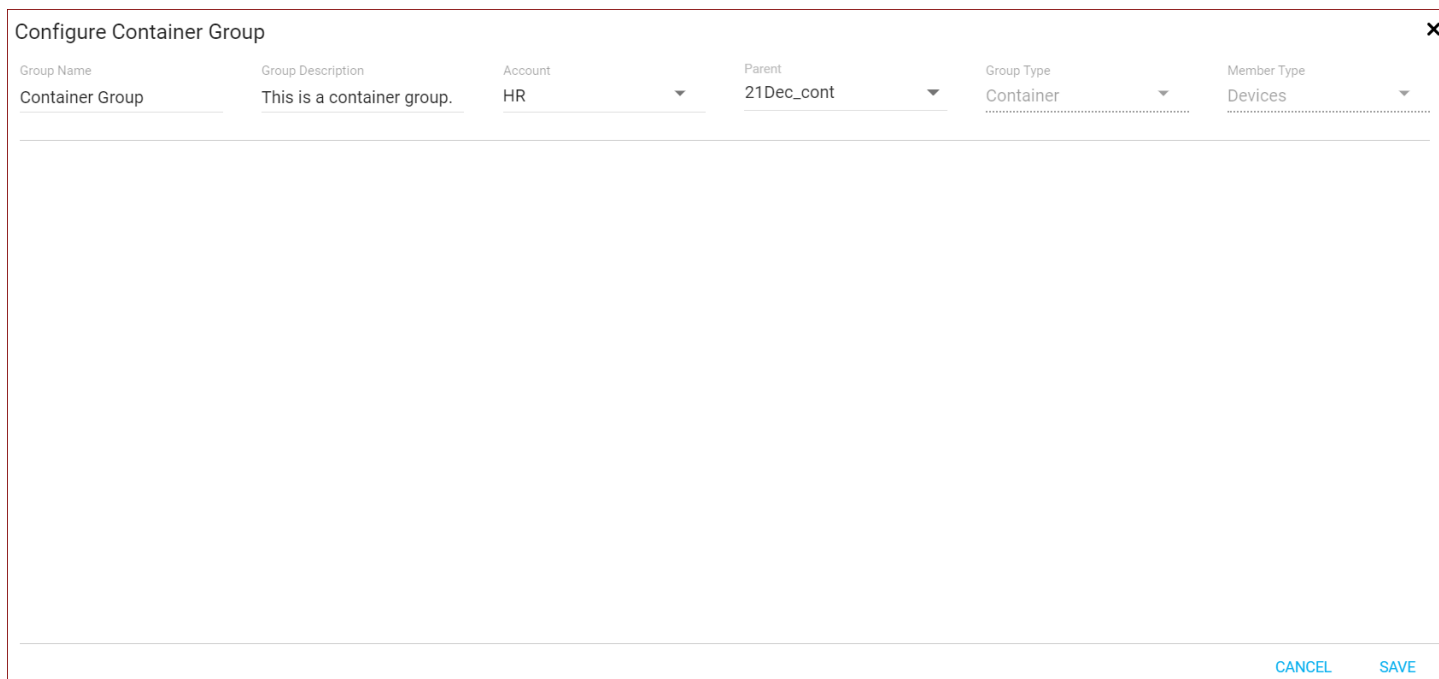
**Follow these steps:**

1. Click **Groups** (  ).
2. Navigate to the group that you want to edit.
3. Click **Action Menu** (  ), and then **Edit Group**.
4. Perform the following operations as appropriate:
  - a. Rename a group. You can rename a group at any level. However, ensure that all group names at the same level are unique.
  - b. Change the group description.
  - c. Modify the account information of the group.
  - d. Move the group from one parent (container group) to another. Ensure that the new parent (to which you are moving the group) belongs to the same account. You cannot move to a parent that has a different account.
  - e. Modify the filter criteria for static or dynamic group.

**NOTE**

For more information about how to add and remove devices from a static group, see the Add and Remove Devices From a Static Group section in this article.

The following screenshot shows the edit dialog for the container group:



| Group Name      | Group Description          | Account | Parent     | Group Type | Member Type |
|-----------------|----------------------------|---------|------------|------------|-------------|
| Container Group | This is a container group. | HR      | 21Dec_cont | Container  | Devices     |

CANCEL SAVE

The following screenshot shows the edit dialog for the dynamic group:

**Configure AdminGroup**

Group Name: AdminGroup | Group Description: Admin group | Account: No Account | Parent: 21Dec\_cont | Group Type: Dynamic | Member Type: Devices

Define Criteria [Hide](#)

Device Filter:  not IP Address contains 10.74 AND OR

[Find Devices](#) [Reset](#)

Search for Computer Systems Matching Devices | 60 Found

| Name   | Alias | IP Address | Caption | Description         | Dedicated | OS Type | OS Name |
|--------|-------|------------|---------|---------------------|-----------|---------|---------|
| 10     |       | 10.74      |         |                     | Device    |         |         |
| lvnapl | n.net | lvn        | p...    |                     | Device    |         |         |
| lvn    | n.net | lvr        | p...    |                     | Device    |         |         |
| lvr    | n.net | lvn        | ip...   | Hardware: Intel6... | Host      | Windows | Windows |
| lvn    | n.net | lvr        | op...   |                     | Device    |         |         |

[CANCEL](#) [SAVE](#)

The following screenshot shows the edit dialog for the static group:

**Configure TestMaint**

Group Name: TestMaint | Group Description: Testing maintenance group | Account: No Account | Parent: 21Dec\_cont | Group Type: Static | Member Type: Devices

Define Criteria [Hide](#)

Device Filter:  not Name is null AND OR

[Find Devices](#) [Reset](#)

Search for Computer Systems Matching Devices | 3 Found

| <input checked="" type="checkbox"/> | Name | Alias | IP addr... | Caption | Descrip... | Role | OS Type | OS Name      | OS Vers... | OS Des...      | Origin | MacAd...       | User Ta... | User Ta... |
|-------------------------------------|------|-------|------------|---------|------------|------|---------|--------------|------------|----------------|--------|----------------|------------|------------|
| <input checked="" type="checkbox"/> | sd   | sd    | 4...       | 10...   |            | Host |         |              |            |                | lvn    |                |            |            |
| <input checked="" type="checkbox"/> | lvn  | lvn   | 10...      |         |            | Host | Windows | WindowsSe... | 10.0.14393 | Service Pac... | lvn    | FA-16-3E-13... |            |            |
| <input checked="" type="checkbox"/> | lvn  | lvn   | 10...      |         |            | Host | Windows | WindowsSe... | 10.0.14393 | Service Pac... | lvn    | FA-16-3E-5B... |            |            |

[CANCEL](#) [SAVE](#)

### Delete a Group

Deleting a group deletes the group, but not the devices in the group. The devices that were members of a deleted group remain in your inventory and as members of other groups.

**Follow these steps:**

1. Click **Groups** ()
2. Navigate to the group that you want to delete.
3. Click **Action Menu**
  - (  ),
  - then **Delete group**.
4. Click **Delete** on the conformation dialog.




**Add and Remove Devices From a Static Group**

You can add and remove devices from a static group, but not from a dynamic group. When you remove a device from a static group, the device remains in the system and as a member of other groups, if applicable.

**NOTE**

If you are logged in to Operator Console with the Operator credentials, you cannot add and remove devices from a group.

**Follow these steps:**

1. Click **Groups** ()
2. Navigate to the group for which you want to modify the members.
3. (Add) To add a device to a group, complete the following steps
  - a. Click **Action Menu**
    - (  ).
  - b. Select **Edit group**.
  - c. Specify the filter criteria, navigate through the device list, and select the additional devices that you want to add to a group.
  - d. Click **Save** to add the selected devices to the static group.
4. (Remove) To remove a device from a static group, complete the following steps:
  - a. Click **Action Menu**
    - (  ).
  - b. Select **Edit group**.
  - c. Navigate through the list and clear the selected devices that you want to remove from a group.
  - d. Click **Save** to remove the devices from the static group.

The static group is updated with your changes.

**Using Filters**

You can set various filter options to select the members for each group you create. Filters for both device and interface type groups include:

- Boolean operators *and*, *or*, and *not*.

Define Criteria [Hide](#)

Device Filter

not Name is null AND OR

[Find Devices](#) [Reset](#)

### NOTE

Precedence among Boolean operators is NOT, then AND, and then OR. The order of multiple filter conditions does not affect the result.

- A drop-down list of previously discovered properties. You can also enter an SQL query from the properties list.

Define Criteria [Hide](#)

Device Filter

not Name is null AND OR

[Find Devices](#) [Reset](#)

Search for Computer Systems

| Name                    | Alias | IP | Role | OS Type | OS Name | OS Vers... | OS Des... | Origin | MacAd |
|-------------------------|-------|----|------|---------|---------|------------|-----------|--------|-------|
| < 1 2 3 4 5 6 ... 71 72 |       |    |      |         |         |            |           |        |       |

### NOTE

To use the SQL query option, you must be a bus user with Portal Administrator permissions. Also, queries must include the column `cs_id` for devices and `me_id` for interfaces.

- A condition list (*is*, *contains*, *starts with*, and so on).

Define Criteria [Hide](#)

Device Filter

not Name is null AND OR

[Find Devices](#) [Reset](#)

Search for Computer Systems

| Name                    | Alias | IP addr | Caption | Description | Type | OS Name | OS Vers | OS Des | Origin | MacAd |
|-------------------------|-------|---------|---------|-------------|------|---------|---------|--------|--------|-------|
| < 1 2 3 4 5 6 ... 71 72 |       |         |         |             |      |         |         |        |        |       |

- A values field.

For static groups, create the filter and then select which of the listed systems to include in the group. For dynamic groups, create a filter to specify the systems to add dynamically to the group. The list of members in the dynamic group is automatically updated every 5 minutes.

### Follow these steps:

1. In the filters section, select items from the drop-down menus and enter the text in the text field as appropriate.

### NOTE

The filter condition *undefined* selects for attributes without defined values. When the option *undefined* is selected, the values field is disabled.

The filter condition *contains* allows you to simplify your filtering rules by use of wildcards: '%' for one or more characters or '\_' for one character.

The filter condition *in* allows you to list attribute values in one filter rather than setting individual filters for each value. You can copy a list of values from another source, paste the list into the values box, and run the filter at once against all values. Each value must occur on a separate line and include no punctuation at the end.

2. Click the Add Filter icon to add filter rows, the Delete Filter icon to delete filters that are not needed, and the Up and Down arrows to change the order of filters.
3. When you have defined the rows for the filter, click the **Find Devices** button to confirm the results in the table.
4. If the filter is for a static group, click the check boxes to select the devices to add to the group.
5. Click **Save**.

The filter is saved.

### Use an Advanced Filter

If you have auto discovery enabled, you can filter on advanced attributes, such as PrimaryDnsName or Virtualization Environment, for system and interface groups. The filter field allows you to select from a list of discovered attributes or enter a known attribute that is not in the list.

#### Follow these steps:

1. In the group dialog, click the first drop-down list in the **Define Criteria** section.
2. From the displayed list, click the **Advanced** option at the bottom of the menu.

#### NOTE

The drop-down list is populated automatically with attributes of discovered group members.

3. Pull down the menu for the operator and select an operator.
4. Enter a value in the values field.
5. Click the **Find Devices** button.
6. Click **Save** to save the group definition.

### Create Groups Automatically

Operator Console can automatically create dynamic groups according to certain criteria.

In order to create groups automatically, you must not be an account contact user. For account contact users, the Configure Automatic Groups tab is not active.

#### Follow these steps:

1. Click the **Settings** in Operator Console.
2. Click the **Administration** tile.
3. Select the type of automatic groups to create.

**NOTE**

Choosing more than one type of automatic group does not combine the types; each property you select creates groups for that property.

- If you want to create a group to be a parent of the automatic groups, enter a name in the **Parent Group** field. For example, if you are an MSP and create automatic groups by origin, you can name the parent group Customers. If you leave the **Parent Group** field blank, the automatic groups are created under the root node.
- Click **OK**.

**The Servers Group**

The **Servers** group is an automatic group that comes pre-configured with OC. The **Servers** group creates sub-groups according to OS Type (Windows, Unix, and so on).

You cannot edit the properties of the **Servers** group or its sub-groups. However, you can assign monitoring templates and report templates. For the subgroups, you can also click the Apply Filters icon to view the results for the update of the group.

**Configure the Update Interval for Automatic Groups**

You can change the update interval for automatic groups by configuring the nis\_server probe. **Follow these steps:**

- In Infrastructure Manager or Admin Console, select the system robot running OC.
- Open the nis\_server probe in Raw Configure.
- Navigate to the Setup section.
- Edit the value for the parameter group\_maintenance\_interval.  
Interval units are given in minutes.

The nis\_server probe automatically restarts after the configuration change is made.

**Set Maintenance Windows for Groups**

The maintenance mode feature lets you temporarily suppress monitoring so that only informational alarms are generated for systems.

You can schedule recurring maintenance to perform routine system updates. Or, you can place systems in a schedule that runs once only.

You can also create an adhoc maintenance schedule if an unplanned outage occurs so that you can quickly respond to the outage.

To manage maintenance schedules, you must have the *Edit Maintenance Mode Schedules* permission set in the Access Control List (ACL). To manage the systems in maintenance schedules, you must have the *Edit Maintenance Mode Devices* permission set in the UIM ACL.

**Create or Edit a Maintenance Schedule**

A maintenance schedule must be created before you can add systems to the schedule.

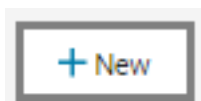
**Follow these steps:**

- Select a group in the Groups view in OC, then select the **Maintenance**



( icon on the top-right Actions menu. )

- 



Click the button.

Or, to edit an existing schedule, select the **Action Menu**



to the schedule you want to edit.

It has the following options:

- a. **Edit Maintenance** - to edit the maintenance
  - b. **Delete maintenance** - to delete the maintenance schedule
  - c. **Remove Maintenance System** - to remove all the devices from the Maintenance
  - d. **End Maintenance** - to stop the maintenance
  - e. **Update Devices.** - to add the devices to the maintenance
3. In the **Create Maintenance Schedule** dialog:
- a. Enter a name, or update the existing name. If desired, enter a description.
  - b. Select an account for the maintenance schedule if desired.
  - c. Make a selection for the **Schedule** option.  
The schedule recurrence options update dynamically based on your selection.
  - d. Select the options for the schedule recurrence and maintenance window as desired.

) next

### Create Maintenance Schedule

Name\*

Description:

Accounts

Schedule  Once  Daily  Weekly  Monthly

Week Starting  ending: Never

Every

Maintenance AT  :  AM FOR  Hour :  Minute

- 4. Click Save to save the scheduled maintenance.

The new schedule is displayed, and you can add groups and systems.



### **Add Devices from Groups to a Maintenance Schedule**

After a maintenance schedule is created, you can add devices from groups to the schedule.

#### **NOTE**

Devices from groups can be added to multiple maintenance schedules.

#### **Follow these steps:**

1. Browse to a group in the Groups view navigation tree, and select the **Maintenance**




(  ) on the top-right Actions menu.

#### **NOTE**

You can expand groups to display individual systems, but the **Maintenance** on the top-right Actions menu is only enabled when a group is selected in the navigation tree.

2. Select the **Action Menu**



(  ) next to the schedule for which you want add the devices from the groups.

3. Select the **Update Devices** option and select the devices from the groups to add to the maintenance schedule.
4. Click **Update Devices**. The maintenance schedule is updated and lists the devices from the groups that you added.

### **Devices by Alarms**

From the **Card** view in the Groups view of Operator Console, you can quickly assess which groups need your attention by looking at the number of alarms that are displayed on each group card.

Click **Information** (  ) on a card, and then click the **Devices by Alarm** tab. The devices in the group generating alarms, and the number of generated alarms are listed.

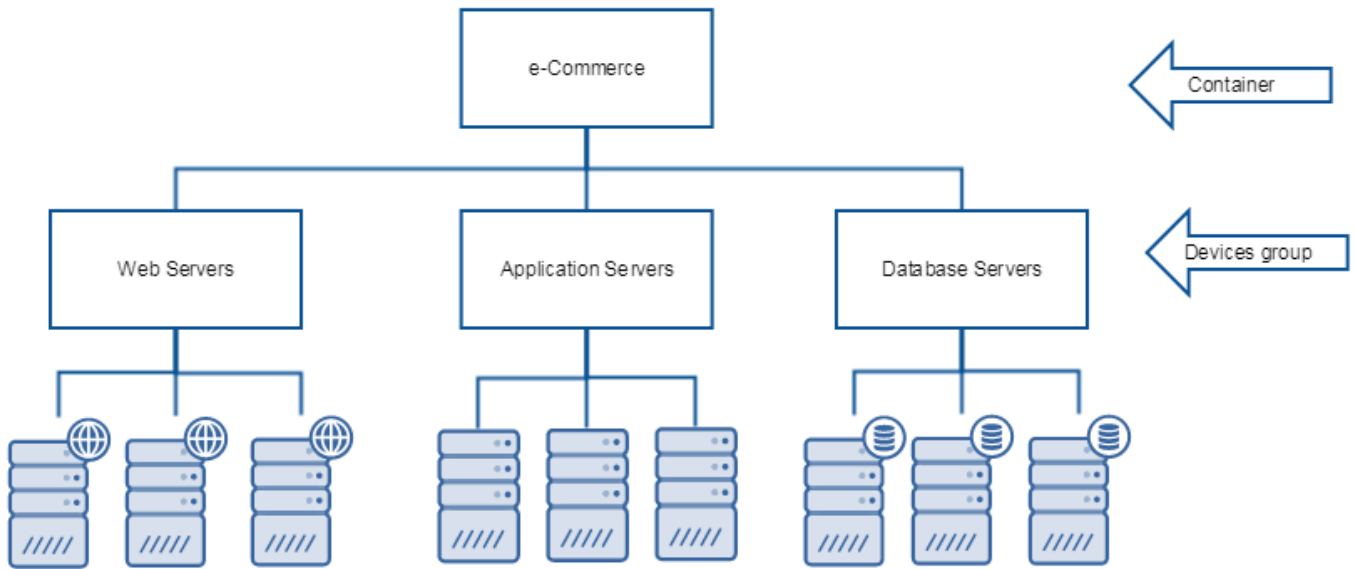
### **Group Examples**

This section provides some examples of grouping structures that you can use for your devices.

#### **Grouping by Device Type**

This grouping example shows a container group (e-Commerce) with three subgroups that contain different types of servers. You could use this grouping structure if you want to look at metrics and alarms for the different types of servers in your environment.

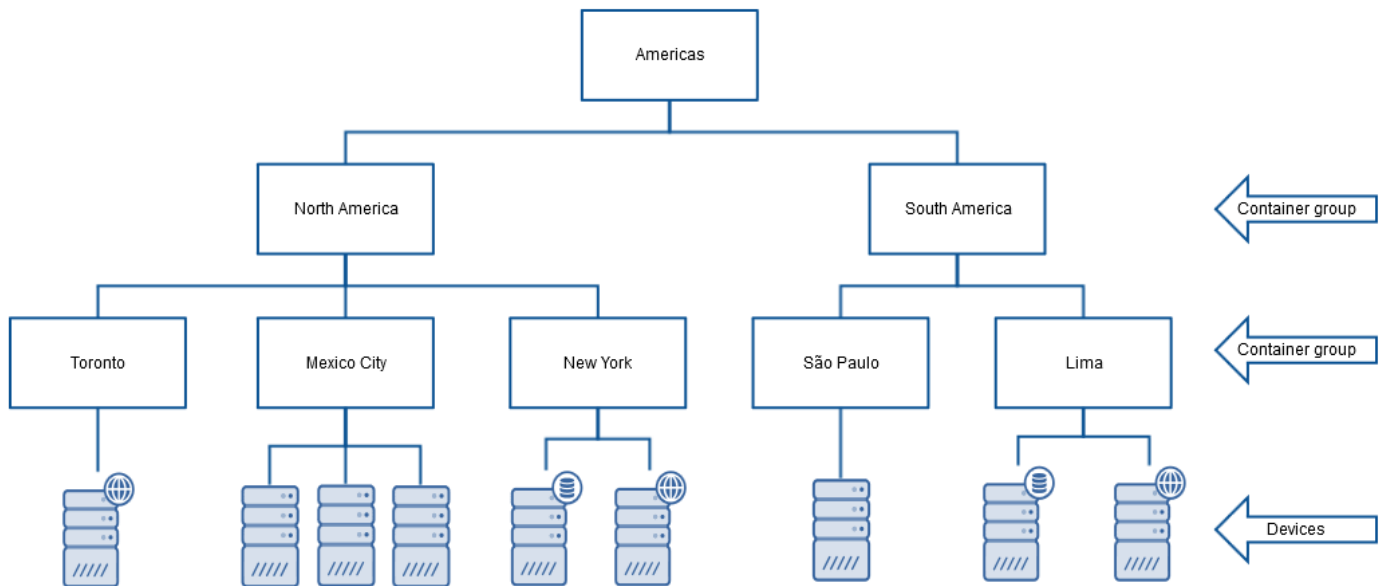
**Figure 22: business group**



**Grouping by Region**

This grouping example shows two levels of container groups. Level 1 is the Americas container group. Level 2 container groups are North America and South America. The level 3 subgroups contain devices that are located in different cities.

**Figure 23: region group**



**View Interface Data**

You can view data about your network interfaces in several locations in OC. These include the Interface Group view and the device interface view. The Interface Group view displays basic metrics for the list of interfaces. The Interface view displays further metrics.

## Contents

### NOTE

Make sure that you have configured the required probes to view interface metrics. See the article [OC Prerequisites](#) for more information.

### The Interface Group View

Click an Interfaces group name in the OC Groups tree view to open the Interface Group View. This view allows you to:

- See a list of all interfaces on a network device, including important attributes and metrics:
  - Utilization % in/out
  - Errors % in/out
  - Discards % in/out
  - MAC address
  - Device Speed
- Sort the interfaces on any column.
- Select an interface and see a detailed view of interface attributes and metrics.

Columns for administrative data in existing interface groups are hidden if they do not contain data. Columns for metrics are displayed whether data is returned or not. All columns are displayed in the dialog for creating a new interface group.

### NOTE

Columns in the Interfaces tab allow for quadruple sorting on metrics. For example:

- Click the **Utilization %** column once to view **Utilization % (In)** in ascending order.
- Click the **Utilization %** column again to sort on **Utilization % (In)** in descending order.
- Click the **Utilization %** column again to change the sorting to **Utilization % (Out)** in ascending order.
- Click the **Utilization %** column again to change the sorting to **Utilization % (Out)** in descending order.

### NOTE

Interface report graphs distinguish between alarms that return no data, alarms that return metric values of 0, and alarms that return metric values of less than 1. A gray cell after the interface name indicates that no metrics are available; an empty (white) cell indicates that the returned metric value is 0; and a graph that occupies at least one pixel indicates that there is returned data, however small. Hovering over a cell displays the values for that metric.

To view information about an interface in the table, sort on the column of interest and select an interface. The **Interface** view opens and displays information and tabs to view alarms and select further metrics.

### NOTE

The **Interface** view can also be opened from the OC Groups tree view and from the **Interfaces** tab in a device view. Information in the **Device Interfaces** view is identical to the information in the **Interface Group** view.

### The Device Interfaces View

To view information on interfaces in the context of a device, open a Device View and select the **Interfaces** tab.

#### Follow these steps:

1. Expand a group in the OC Groups tree view.
2. Select a computer system.
3. Click the **Interfaces** tab at the top of the window.

Information in the **Device Interfaces** view is identical to the information in the **Interfaces Group** view table. Columns for administrative data are hidden if they do not contain data. Columns for metrics are displayed whether data is returned or not.

### **The Interface View**

The Interface view is available when you select an interface from an interfaces table or the OC Groups tree view. The view contains information available in the table views and tabs to view further metrics.

#### **Follow these steps:**

1. Expand a group in the OC Groups tree view.
2. Select a computer system.
3. Navigate to the **Interface** tab using one of the following methods:
  - Click the **Interface** tab at the top of the **Device View** screen. A list of available interfaces for the device appears. Select an interface from the table.
  - Select an interface from the Groups view left navigation tree. Interfaces are indicated with the interface icon.
4. Click the interface that you want to view.

The Details and Metrics tabs display line charts with intervalized data to the right. If there are multiple data samples for an interval, the values are averaged. Minimum and maximum values for the sampled data is displayed as a shaded area below and above the averaged value. To view another interval or change chart display properties, hover over the upper right area of a chart and select the pop out; this loads the chart into another browser window as a Performance Report.

### **The Metrics Tab**

The **Metrics** tab allows you to display metrics that have been configured for the interface.

#### **Follow these steps:**

1. Expand the metrics menu.
2. Select a metric or set of metrics.

The metrics are displayed in the pane to the right.

Data charts in the Metrics view are the same as for the interface details view.

### **The Advanced Tab**

The **Advanced** tab displays graphs for the following SNMPcollector probe metrics:

- Utilization In (%)
- Utilization Out (%)

#### **NOTE**

Interface utilization percentage takes into account the overridden speed configured in SNMPcollector (for example: 50 Mbps Down/10 Mbps UP).

#### **NOTE**

Contents of the **Advanced** view changes based on configured metrics. For example, if CA Network Flow Analysis (NFA) has been integrated with UIM, NFA data is displayed in this view with a link to the NFA diagnostic view for the interface. Refer to system configuration details for metrics available to this view.

## **Manage Alarms**

This article describes the alarm view for devices and interfaces and how to manage the alarms and to change the view to display the information that you need.

## **Overview**

UIM monitors the system for system availability and operating parameters. If configured operating thresholds are exceeded, UIM generates an error message called an alarm. Alarms represent changes in device performance levels or complete device failures: for instance, high system loads or a loss of access. Knowing when specific system elements need attention, you can correct performance problems before they affect system availability.

The Alarms view in Operator Console displays a list of active alarms that are returned by the system along with the Alarm by Severity, Alarm by Probes charts, Top Alarming devices, with a history toggle button to view the history, and include/hide invisible toggle to include the invisible alarms or hide them. You can view details for individual alarms and can identify the devices that created them. You can distinguish between critical and non-critical alarms to prioritize alarm resolution. Also, you can easily access dashboards that display performance metrics over time to address patterns in low system performance.

## **The Alarm Lifecycle**

UIM collects metrics on all monitored devices. If an operating parameter exceeds the threshold, UIM:

1. Generates an alarm.
2. Assigns the alarm an associated severity.

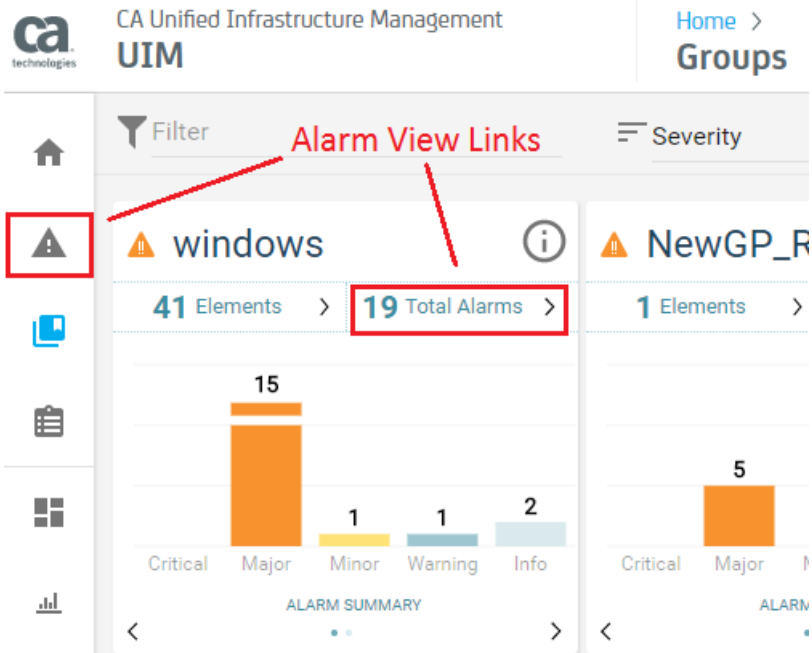
Alarms that meet default parameters for severity are automatically sent to the email account configured in the emailgw probe.

If the alarm condition persists, the time of the latest event is maintained internally. The calculated duration of the alarm represents the persistence of the alarm condition.

If the alarm level changes (another alarm threshold is exceeded or the current threshold is no longer met), the alarm view displays the new severity. When the alarm condition is corrected, the alarm condition is cleared and the alarm is removed from the alarm display.

## **How the Alarms View Works**

The Alarms view gives you a list of current alarms and details on those alarms. To open the Alarms view, click on Alarms in the left of the Home view or the alarm count in the navigation card in the Home view for a displayed group or inventory.



The view is context-sensitive. If you open the Alarms view without navigating to a specific group in the Home view, the Alarms view displays all system alarms. If you navigate to a group within the Home view, the Alarms view displays alarms for all devices in the group. If you navigate within the Home view to a specific device within a group, the Alarms view displays alarms for the selected device.

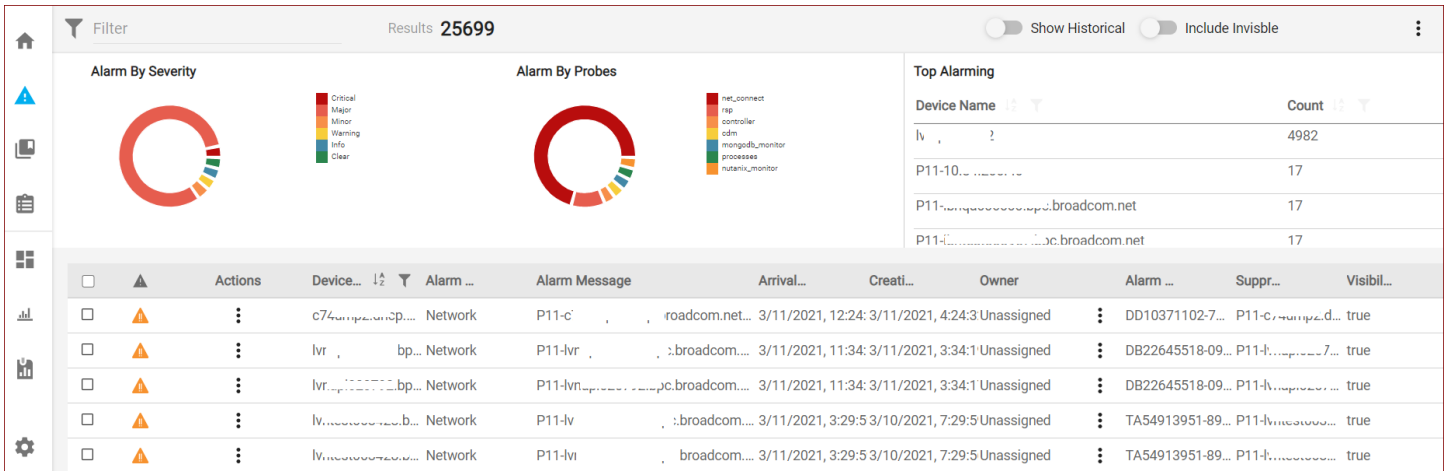
The alarm view is dynamic: On opening, the alarm list is automatically updated to show the latest alarms. Alarms that are cleared by the system are removed from the view.

An alarm is displayed so long as its device is operating outside of operating parameters. A condition that persists over time is represented by a single alarm, and the view displays the duration of the first instance of the alarm. Subsequent identical alarms are suppressed from the view. Any change in an alarm other than severity (for example, an alarm message revision) generates a new alarm.

All the alarms are displayed in the table but the Alarm count is based on the visibility set for alarms. The alarms for which visibility is set to false are not included in the count of alarms.

The Alarms view opens as a list. Some of the columns in the view are (for example):

- Severity icons (!)
- Actions
- Device Name
- Alarm Type
- Alarm Message
- Alarm ID
- Arrival Date
- Duration



Icons represent the alarm severity that you defined in the monitoring configuration.



- Critical



- Major



- Minor



- Warning



- Info

The number of alarms in the list is displayed at the top of the Alarm charts. When no filter is applied, the view displays the number of alarms for the view context. When a filter is applied, the view displays the number of alarms in the filtered list.

### Alarm Table

The alarm table displays information about alarms in a table format for the selected group or device and is displayed with the alarms by severity, alarms by probes charts, and top alarming as a default view. You can view table information by selecting various elements within the table.

#### Follow these steps:


- Click the Edit Columns in the Global **Actions** menu



at the top right of the Alarms view to add or remove columns in the display. Only options in the menu that apply to the display are active.

- Click the checkbox next to an alarm to select the alarm. If at least one alarm is selected, the **Actions** menu is activated. You can also select *select all* and clear selected alarms.

**NOTE**

A menu of actions for an individual alarm can also be displayed from the **Actions** icon (  ) in the table.

- Click on the **Alarm** record in the table to display the overview.  
To return to the alarm list, close the overview.
- Click a column header to sort the table data by that column.

You can change the columns that are displayed in the table by choosing **Edit Columns** from the Global **Actions** menu and select the columns that you want to display.

**NOTE**

You can set values for the columns **Custom 1** through **Custom 5** by selecting one or more alarms and choosing **Set Custom** from the **Actions** menu.

**View Alarm Details**

Click the alarm record to view more information about the alarm in the **Overview, Device Details, Metric, and History** tabs. The details identify device and alarm attributes to help identify performance issues. For example, knowing what probe monitors the device might prompt you to check the probe status and log through the Admin Console view. Such details can help you determine whether the issue is in the device or in the probe.

- The Overview tab displays alarm details.
- Device Details displays the details about the device.
- The History tab displays the history of the alarms that are created for the device.
- The Metric tab displays performance metrics for the device. This tab only exists when an alarm is based on a metric.

The details view remains open for any selected alarm on the page but displays the details that are related to another alarm when another alarm is selected. You can close the details view and return to the list of alarms by clicking the **X** at the upper-right corner of the view. Multiple alarms can be selected in the Operator Console and can be performed with different actions like closing the alarms on the selected alarms.

**View Device Metrics**

You can view performance metrics for devices through the Alarms view. Metrics let you see the performance of the device for the last 24 hours. Device metrics are available in two places: under the Metrics tab in the Alarms view and in the dashboard for the device, accessible through the dashboards view. The Metrics tab is only available for alarms that are associated with metrics. Alarms for some conditions, such as an expired license, do not produce metrics, and no Metrics tab is generated. A link in the device name under the Device Details tab opens the dashboard view for the device. The dashboard view provides additional information about the device details. You can also open this view through the Dashboards view by drilling down through the group cards to the device.



The screenshot displays the UIM interface with several components:

- Alarm By Severity:** A donut chart showing the distribution of alarm severities: Critical (red), Major (orange), Minor (yellow), Warning (green), Info (light green), and Clear (dark green).
- Alarm By Probes:** A donut chart showing the distribution of alarms by probe type: net\_connect, rdp, controller, cdm, mongodb\_monitor, processes, and nutanix\_monitor.
- Top Alarming:** A table listing the top devices by alarm count.
 

| Device Name                | Count |
|----------------------------|-------|
| lvnqa014672                | 4982  |
| P11-1009200-0              | 17    |
| P11-1009200-0-broadcom.net | 17    |
| P11-1009200-0-broadcom.net | 17    |
- Alarm List:** A table showing active alarms with columns for Actions, Device Name, Alarm Name, Alarm Message, Arrival Time, Creation Time, Owner, Alarm ID, Suppression, Visibility, and Customization.
 

| Actions | Dev...      | Alar... | Alarm Message                  | Arri...         | Cre...          | Owner      | Alar...        | Sup...        | Visi... | Cust... |
|---------|-------------|---------|--------------------------------|-----------------|-----------------|------------|----------------|---------------|---------|---------|
| [icon]  | lvnqa014672 | Network | P11-1009200-0-bpc.broad...     | 3/11/2021, 3:29 | 3/10/2021, 7:29 | Unassigned | TA54913951-... | P11-1009200-0 | true    | --      |
| [icon]  | lvnqa014672 | Alarm   | Physical Memory Usage (%) o... | 3/11/2021, 3:26 | 3/10/2021, 7:26 | Unassigned | TA54913951-... | M3009200-0    | true    | --      |
- Alarm Details:** A detailed view for alarm ID TA54913951-77760, showing:
  - Probe: cdm
  - Suppression key: M3690E0027325494F273C4A91D8DBF0A8-STATIC-9-0
  - Alarm Message: Physical Memory Usage (%) on Physical for lvnqa014672 is at 80.85 %.
  - Monitoring host/robot: lvnqa014672
  - Source: lvnqa014672
  - Hub: lvnqa014672\_hub
  - Alarm type: Alarm
  - Created: 19:26 IST Wed 10 Mar 2021
  - Annotation: [empty]
  - Customization: Custom 1, Custom 2, Custom 3, Custom 4

For information about viewing dashboards for groups and devices, see [View Your Dashboards](#).

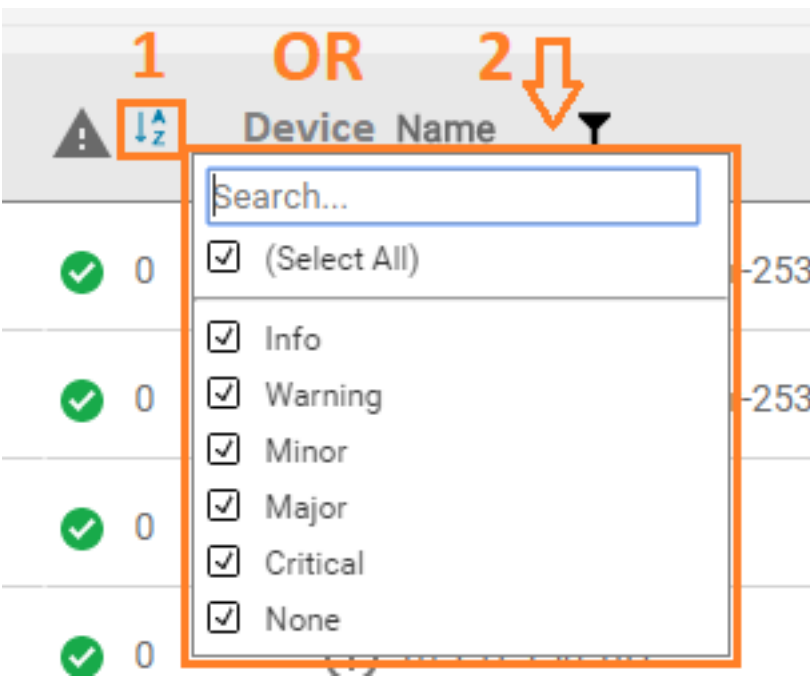
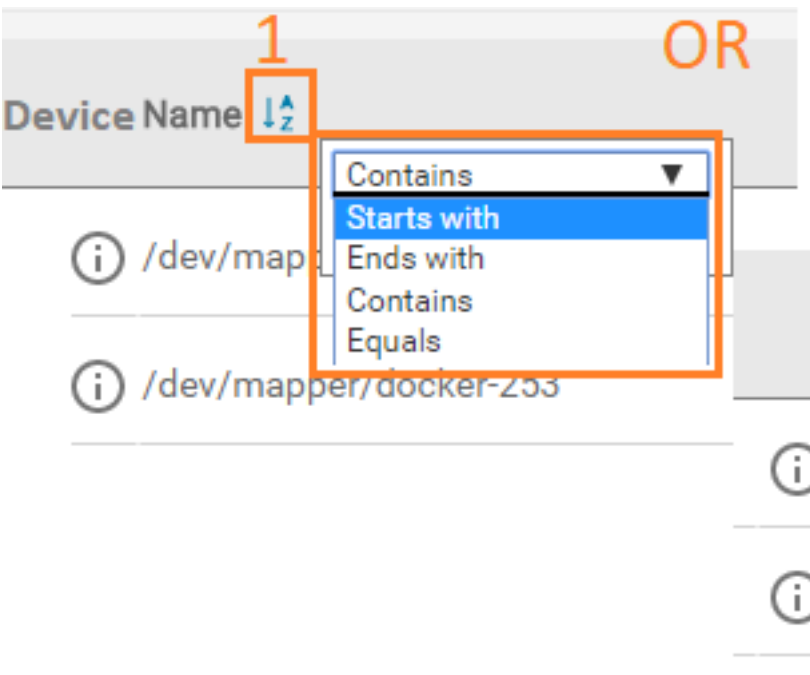
**NOTE**

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

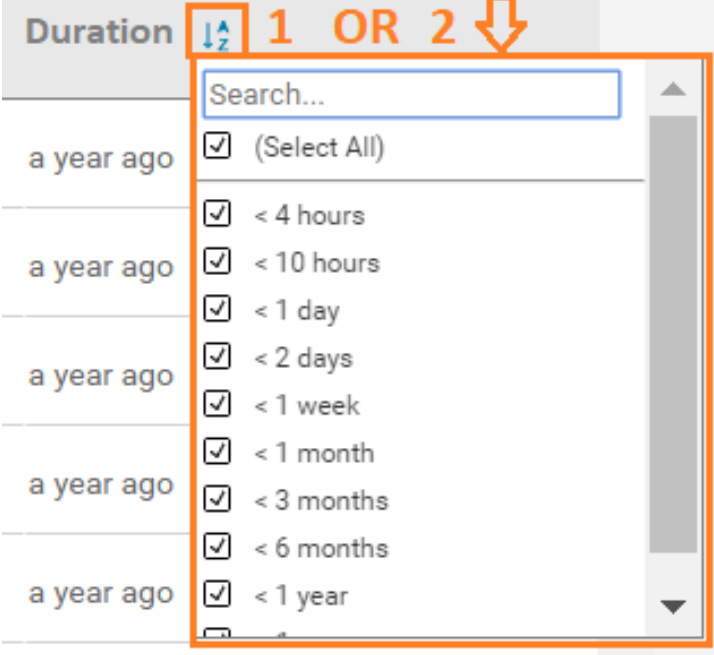
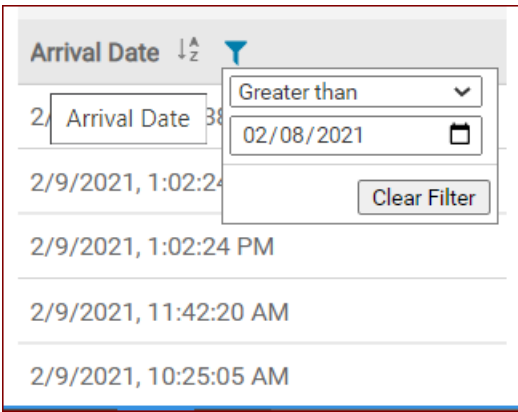
**Alarm Filters**

There are times when all of the data available on alarms is too much information, either for you or for the user. You can filter alarm data either as part of a current analysis or as part of a designed view to filter out data that is not important. For example, data specific to an alarm severity or location or time might be easier to view and analyze when less-important data is removed from the display. You can change views dynamically by selecting different parameters in the current display, or you can create complex filters that can be applied to alarms and alarm views and modified according to want. You can apply filters to custom OC views to emphasize specific content each time the portal is opened and the list of alarms is viewed.

For each column in the Alarms view, you can use the additional filter options to narrow your search. Move the mouse pointer to the column to view the filter options. Some examples are as follows:

| Column Name           | Filter                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Alarm Severity</b> |   | <p>Filter alarms based on the alarm severity:</p> <ul style="list-style-type: none"> <li>View a sorted list based on the alarm severity (shown as 1 in the image). When all alarms are of the same severity, the alarms are displayed in random order and not on the alarm count.</li> <li>Use specific alarm severity to view the related list of alarms (shown as 2 in the image).</li> </ul> |
| <b>Device Name</b>    |  | <p>Filter alarms based on the device name:</p> <ul style="list-style-type: none"> <li>View a sorted list based on the device name (shown as 1 in the image).</li> <li>Use specific device name text to view the filtered list (shown as 2 and 3 in the image).</li> </ul>                                                                                                                       |

| Column Name          | Filter | Description                                                                                                                                                                                                                                                                            |
|----------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Alarm Type</b>    |        | <p>Filter alarms based on the source of the alarm:</p> <ul style="list-style-type: none"> <li>View a sorted alarms list based on the alarm type (shown as 1 in the image).</li> <li>Use specific alarm type text to view the filtered list (shown as 2 and 3 in the image).</li> </ul> |
| <b>Alarm Message</b> |        | <p>Filter alarms based on the alarm message:</p> <ul style="list-style-type: none"> <li>View a sorted alarms list based on the alarm message (shown as 1 in the image).</li> <li>Use specific alarm message text to view the filtered list (shown as 2 and 3 in the image).</li> </ul> |

| Column Name  | Filter                                                                             | Description                                                                                                                                                                                                                                                                                           |
|--------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Duration     |  | Filter alarms based on the time when they were raised: <ul style="list-style-type: none"> <li>View a sorted alarms list based on the duration (shown as 1 in the image).</li> <li>Use specific duration to view the filtered list (shown as 2 in the image).</li> </ul>                               |
| Arrival Date |  | Filter alarms based on the date when they arrived in the system: <ul style="list-style-type: none"> <li>View a sorted alarms list based on the arrival date. Click A-&gt;Z.</li> <li>Use specific duration to view the filtered list. Click the filter icon and enter the required values.</li> </ul> |

The filter item appears above the filter list. Click the filtered item again to clear the filter.

### Alarm Management Actions

Alarm Management actions menu in the Alarms table has the following options.

- **Acknowledge** to acknowledge an alarm.
- **Set invisible** icons to hide an alarm.
- **Launch URL action** to select a URL action, if available.
- **Add Annotation** to add an annotation to an alarm.

### Set Custom Alarm Fields

Authorized users can enter text in five custom fields for selected alarms, and the text is displayed in the alarm list view. You can use these fields to enter information about who to contact when certain alarms occur, instructions on how to

resolve the alarms or general notes about the alarms. Alternately, the UIM alarm\_enrichment probe can be used to add information automatically, such as device information (serial numbers, for example) or contact information to the custom text fields. You must have the **Alarm Management** permission in your Access Control List (ACL) to enter text in the custom alarm fields. By default, in OC these fields are named **Custom 1** through **Custom 5**. Administrators can change the name of these fields in the Raw Configure window for the Alarm Server (nas). The text that you enter in the custom fields is viewed by clicking the **More** button in the alarm list view. Or, you can add the columns for the custom fields to the alarms table view.

#### NOTE

The custom text fields are displayed in the alarms list view only if text has been entered for the field.

Click a custom field to filter alarms by that field. You can also group information in the alarm summary chart by custom fields by choosing a custom field from the pull-down list.

#### Follow these steps:

1. Click the **Alarms** view.  
The alarms are displayed.
2. Select one or more alarms by clicking the checkbox next to the alarms or by choosing **Select All** from the Alarms table.
3. Choose **Set Custom** from the Global **Actions** menu.  
The **Set Custom** dialog is displayed.
4. Select the fields that you want to enter a value for, then enter the desired text.

#### NOTE

Existing text for custom fields is not displayed in the Set Custom dialog. Text that you enter overwrites any existing text.

5. Click **OK**.
6. In the alarms table view, select **Edit Columns** from the Global **Actions** menu and select one or more custom fields  
The custom fields that you entered text for are now displayed.

#### Change Names of Custom Fields

The default names for the custom text fields for alarms are **Custom 1** through **Custom 5** in OC. Administrators can change the name of these fields in the Raw Configure window for the Alarm Server (nas).

#### Follow these steps:

1. Use Infrastructure Manager to open the **Raw Configure** window for the nas probe:
  - a. Select the nas probe.
  - b. Press the **Ctrl** key and right-click on the nas probe.
  - c. Choose **Raw Configure**.
2. Add the **setup > custom\_headers** folder, then open the folder.
3. Click **New Key**.  
The New Key dialog is displayed.
4. Enter the following values:
  - Key name = **custom\_1** through **custom\_5**
  - Value = The name you want as the label for the field
5. Click **OK**, then click **OK** again to close the Raw Configure window.
6. Restart the OC webapp in the wasp probe:
  - a. In Infrastructure Manager, double-click on the wasp probe to launch its configuration GUI.
  - b. Click the **webapps** tab.
  - c. Right-click **OC**.
  - d. Click **Stop**.

- e. Click **Start**.

### **Delete Text from Custom Fields**

You can delete text from a custom alarm field.

#### **Follow these steps:**

1. In the **Alarms** tab, select one or more alarms by clicking the checkbox next to the alarms or by choosing **Select All** from the **Actions** menu.
2. Choose **Set Custom** from the **Actions** menu.  
The Set Custom dialog is displayed.
3. Select the fields where you want to remove text.
4. Delete the text.

#### **NOTE**

Existing text is not displayed in the Set Custom dialog. Leaving it blank removes any existing text.

5. Click **OK**.
6. In the Alarms list view, click **More** for one of the alarms you selected.  
The custom fields that you removed the text for are no longer displayed.

### **Sort Alarms**

You can change the sorting of alarm data in the alarm list and alarm table. To change the sorting of data in the alarm list or alarm table, select an item from the pull-down menu in the toolbar above the alarm list or table. The sorting you select is retained when you switch between the alarm list and alarm table.

#### **Follow this step:**

- In the Table view, click a column header to sort by that column.  
This updates the **Sort by** pull-down menu and also sorts the list.
- In the List view, pull down the Sort button and click on an item in the alarm description.

#### **NOTE**

Clicking on the same sorting criteria for the third time removes the applied sorting and displays the results without sorting.

### **Change Alarm States**

You can accept, assign, unassign, or acknowledge (clear) alarms in the OC **Alarms** table.

#### **NOTE**

You must have the **Acknowledge**, **Accept**, **Assign**, or **Unassign** permissions set in the Access Control List (ACL) to take those actions on alarms.

#### **Follow these steps:**

1. Click an alarm in the **Alarms** table.
2. In the table view, do the following:
  - Click the checkbox to select one or more alarms, then select **Accept**, **Assign**, **Unassign**, or **Acknowledge** from the table **Actions** menu and the Owner column actions.

### **Configure Invisible Alarms**

Administrators can set whether an alarm is visible to other users. You might want to set some alarms to invisible to hide them if they are not relevant to other users. You can quickly set a single alarm to invisible (or visible) by clicking the

appropriate **Set invisible** or **Set visible**, or you can select multiple alarms and can set them to invisible (or visible) by choosing a menu item.

**NOTE**

You must have the **Invisible Alarms** permission to set alarms as invisible and to view invisible alarms.

**Set a Single Alarm to Invisible**

You can quickly set whether a single alarm is visible by clicking an icon in the alarms list view.

**NOTE**

You must have the **Invisible Alarms** permission to set alarms as invisible and to view invisible alarms.

**Follow these steps:**

1. Click the **Alarms** view.  
The alarms information is displayed.
2. Select an alarm.
3. Click the **Set invisible** or **Set visible** from the table, Actions menu to set whether an alarm is hidden for users who do not have the **Invisible Alarms** permission.

**Set Multiple Alarms to Invisible**

Administrators can filter or sort to find certain types of alarms and then set multiple alarms to invisible (or visible).

**NOTE**

You must have the **Invisible Alarms** permission to set alarms as invisible and to view invisible alarms.

To see what other users (who do not have the **Invisible Alarms** permission) will see, select **Hide Invisible**. All invisible alarms are hidden. Choose **Include Invisible** to include the invisible alarms in the list. In the Table view, you can add the Visibility column to the table (select **Edit Columns** from the **Actions** menu). As with all columns in the table, click the **Visibility** header to sort the table by that column.

**Follow these steps:**


1. Click the **Alarms** view.  
The alarms information is displayed.
2. Select the alarms you want to set to invisible. You can do this by:
  - Clicking checkboxes next to the alarms
  - Choosing **Select All** from the **Actions** menu
3. Choose **Set Invisible** from the **Actions** menu.

**NOTE**

To view the visible and invisible data in the Alarms table, you must add the Visibility column from Edit Columns in the Actions Menu. You can select true or false in the Visibility column filter to view the visible and invisible alarms.

**Add Annotations**

Annotations can only be added; previous annotations cannot be edited or deleted. Each entry in the Alarm Annotations editor is time-stamped and tagged for the user. HTTP or HTTPS addresses become active links when the annotation is saved. Annotations are automatically added when alarm ownership changes. The added annotation is visible in the Overview tab of the selected alarm:


windowstemplate

OVERVIEW
DEVICE DETAILS
HISTORY

---

Alarm ID **ZM15922341-76526**

Alarm Message **Connection to windowstemplate gin refused**

Alarm type **Host**

Created **08:01 IST Tue 9 Feb 2021**

Annotation **Test**

**failed or lo**

**NOTE**

Any notes that are attached to alarms using the nas API are displayed as annotations in OC.

**Use Alarm ID or Host Name to Directly Access Alarms**

You can use an alarm ID as a filter to directly access the associated alarm. Similarly, you can use a host name as a filter to access only those alarms that are related to that host.

- **Use Alarm ID**  
To use an alarm ID as a filter, enter the alarm ID value in the URL: `http://<OC_server>/operatorconsole_portlet/uim-alarms?alarmId=<value>`
- **Use Host Name**  
To use a host name as a filter, enter the host name value in the URL: `http://<OC_server>/operatorconsole_portlet/uim-alarms?hostname=<value>`

**Create a Custom URL Action**

A custom URL action provides a shortcut from an alarm to a third-party application by launching the URL in a new browser tab. You can use parameters in the syntax of the URL action so that alarm attributes are substituted in the URL. For example, you can use the parameter **\${MESSAGE}** to include alarm messages in the URL that can be consumed by a third-party service desk application. As another example, you can use a custom URL action to launch a Remote Desktop session to a system that is generating an alarm, using the format **rdp://\${SOURCE}**.

**NOTE**


More configuration steps are required on the system where Remote Desktop is launched.

To create or edit custom URL actions, you must have the *Edit URL Actions* permission set in the ACL. To launch a custom URL action, you must have the *Launch URL Actions* permission set in the ACL. With this permission, you can select an alarm, then launch an alarm action from the **Actions** menu.

**Follow these steps:**


1. Select **Alarms** View in the left Navigation of the Operator Console (OC).
2. Select **Edit URL Actions** from the **Actions** menu  
The **Edit URL Actions** dialog opens.
3. Select **New URL action**.
4. Specify a name and a valid URL.



5. (Optional) Click the **argument** () button and select an argument from the list. Repeat this step to add more arguments if desired.
6. Make a selection from the **Visibility** menu.

**NOTE**

The **Public** option makes the URL action available to both bus users and account contact users. Select **account > No Account** to restrict the URL action to bus users only.

7. (Optional) Click **New variable** to define a POST variable. If desired, click the **argument** () button to use parameters in the POST variable.
8. Click **Save** to exit the dialog.

**Export Alarms to Excel**

You can export a list of current alarms to a .csv file from the alarms table of a selected group or device. You can also export specific alarms to a .csv file. To export a list of alarms, click on the Global **Actions** menu above the list or table, and select **Export to Excel**. To export only selected alarms, click the box next to the alarm in the table, click on the **Actions** menu, and select **Export to Excel**.

**Historical Alarms**

You can view the historical data of the alarms in the Alarms table, by clicking the toggle for the historical data located on the top of the Alarms view page. This displays all the alarms for the devices till date including the cleared alarms.


The following items are common questions and their answers.

**What happens to the view when a new alarm occurs?**

The list of alarms is "paused" by default: that is, new alarms are held apart from the list. Pausing keeps the alarms list static while you view the current alarm data. When a new alarm is logged or an alarm is cleared, a message appears in the header of the view. You can update the alarm list by clicking the update message to view the new alarms and drop the cleared or expired alarms. The page contents change accordingly but keep a currently selected alarm visible.

**Can I sort the alarms list? Can I filter alarms?**

You can sort the view by any column by clicking the column title and then the sort icon for ascending or descending sort order. Strings are sorted alphabetically. If no alarm is selected, the sort opens to the first page of results. You can filter

alarms. Click next to the Filter icon () at the upper left of the list to enter a quick filter. The alarm list is filtered on device names. Filters are case-sensitive.

**How do I view alarm details, such as device information?**


Select an alarm to open the alarm details pane below the list. If the monitoring probe collects metrics, the details pane contains alarm, device, and metric details. Opening the details pane automatically adjusts the length of the list to accommodate the pane.

**What happens to the list when an alarm condition is corrected?**

Alarms are displayed until the monitoring probe clears the condition. The alarm condition is cleared when the next monitoring interval no longer reports the condition. Each probe has its own monitoring interval, so different types of alarms can take different amounts of time to clear.

## Clear Alarms

UIM clears alarms when you correct the condition that created the event or the alarm expires due to inactivity. After you correct an alarm condition, the monitoring probe will clear the alarm at the next monitoring interval and UIM removes the alarm from the Alarms view. If an alarm is not updated for 72 hours, UIM clears the alarm automatically and removes the alarm from the Alarms view. Refer to the following displays to identify possible causes of an alarm. Be aware that an alarm condition for one device—for instance, a power supply—can cause dependent devices to register alarm conditions too. Be selective about the priority of alarms to restore system operation quickly.



- View the metrics for the alarm in by clicking the Metrics tab and viewing the metrics graph to identify any pattern in device performance that might result in an out-of-range condition. The graph displays the last 24 hours of device operation. The graph might indicate an hourly or daily pattern of heavy use.
- View the alarm metrics for the device in the **Dashboard** () view for the same information in the context of the device. In the dashboard, you can change the displayed period to view metrics patterns to days or weeks. Changing the display period can be useful if periods of high use occur on specific days of the week or month.

### NOTE

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies view page. Custom and Out-of-the-Box dashboards and reports are still rendered using CABI; that is, they have a dependency on CABI. However, the native OC screens (generic dashboards) are no longer dependent on CABI (Jaspersoft) and are rendered using HTML5.

- If a minimum value is required for normal operation and no metrics are being returned, the monitoring probe may not be active. Check the status of the monitoring probe through the **Admin Console** to verify that the monitoring probe is running. If the probe status shows that it is inactive, restart the probe. For instructions, see [Activate, Deactivate, or Restart a Probe](#).
- If an alarm is being returned for otherwise an acceptable operating condition, alarm threshold settings may be set too low.

### Follow these steps:

- a. Select the group for the device in the Home () view.
  - b. Click the Monitoring Config () icon at the upper right of the window to view the group monitoring profile.
  - c. Check for an alarm threshold value that should be raised or a metric that should be turned off.
- Review the monitoring probe log file for the device through the **Admin Console** to identify potential sources of the alarm condition. The alarm condition may be a one-time occurrence or a pattern of performance problems. If a configuration parameter (for example, a memory partition or the number of CPUs available) causes the condition, you might must reconfigure or replace the device. Refer to internal troubleshooting procedures to proceed. For instructions on viewing the log file, see [View a Probe Log File](#).

Consult with your IT administrator for troubleshooting steps and configuration changes that are must correct the alarm condition.

## Troubleshooting

**Symptom:** There may be instances where the alarms are not generated though alarm policy is active.

**Solution:** Alarm policy works only for enhanced templates. Ensure that the template that generates the metrics is an enhanced template.

## View Your Dashboards

After you have configured your monitoring, you can view your metric and alarm data in dashboards.

### Contents

## Accessing Your Dashboards

To access your dashboards, click the **Dashboards** icon



in the left navigation of the Operator Console (OC).

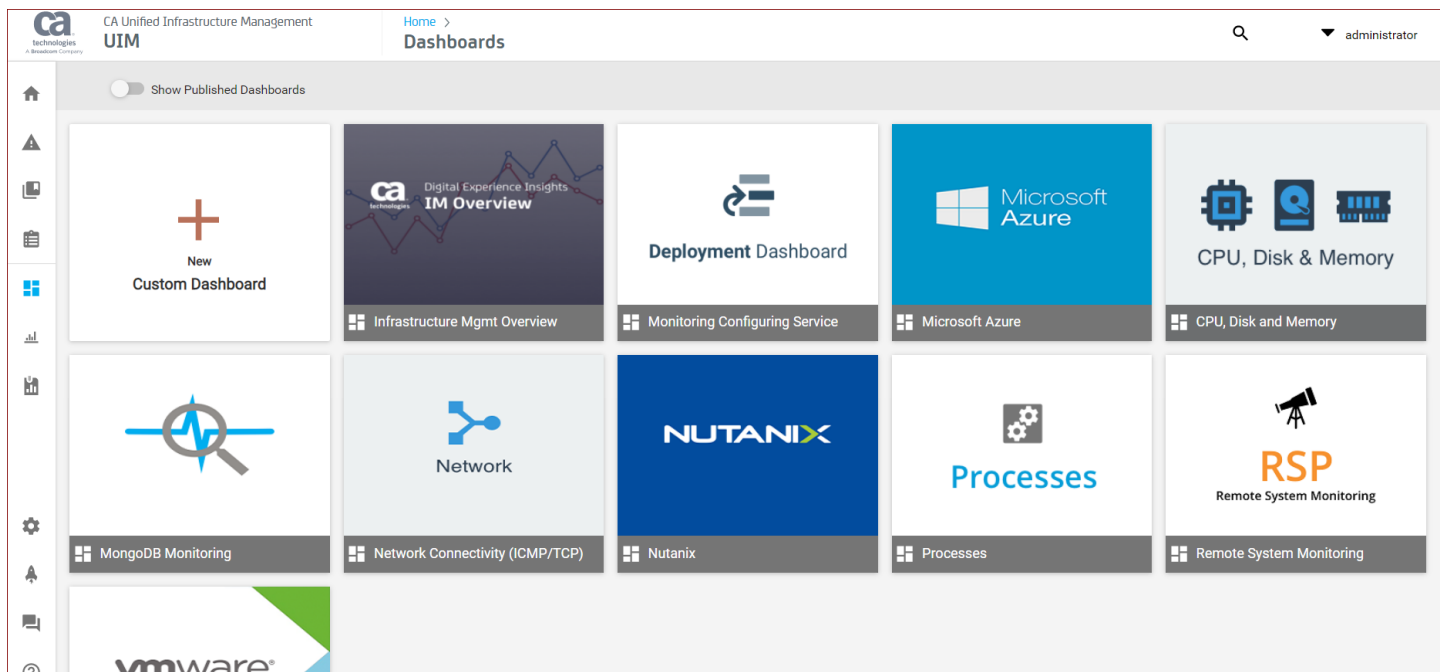
### TIP

- UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.
- To view an overview dashboard for a specific group, navigate to the group and click the **Dashboards** icon

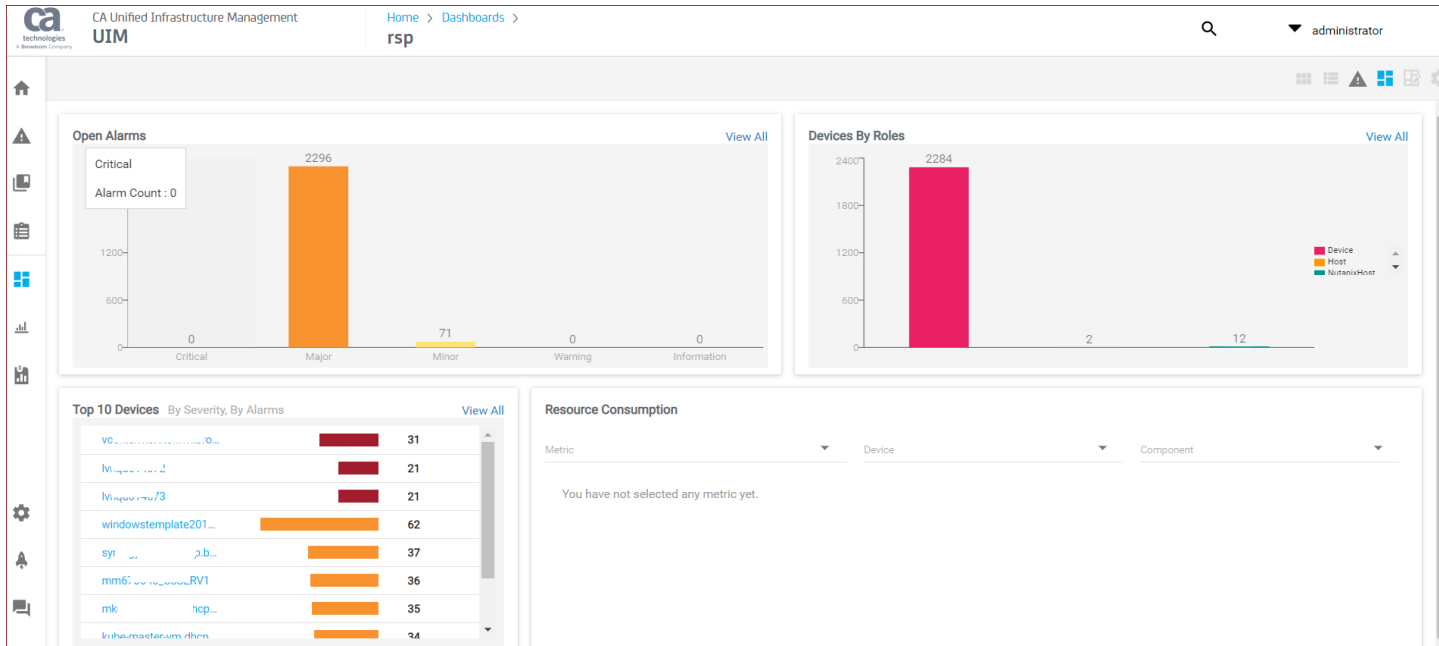


in the upper-right corner of the screen.

In UIM 20.3.3, the main Dashboard page is displayed as follows when accessed using the Dashboard link in the left navigation view:



Additionally, in UIM 20.3.3, the dashboard pages for the monitoring technologies like processes, rsp, cdm, net\_connect, and so on are rendered by using HTML5, not CABI. Therefore, when you click a tile on the main Dashboards page, the dashboard pages for such probes are rendered by using HTML5. The following screenshot shows an example of the cdm dashboard page in UIM 20.3.3:



### Dashboard Time Ranges

Some dashboards allow you to select a time range for viewing metric data. If the dashboard you are viewing supports time ranges, a time range list appears in the upper-left corner of the screen.

### Managing Dashboard Report Content

The following actions might be available to manage the contents of a report:

- Click an item in a report legend to add or remove the data from a report.
- Click a table column heading to format, filter, or sort table content.

### Dashboard Basics for Monitoring

This section provides some general guidelines on how to monitor your environment effectively. The predefined dashboards are designed to help you quickly identify the source of an alarm and make your monitoring more effective and meaningful over time. When an alarm is generated, consider the following items:

- Identify alarm information - Alarms identify changes in your environment that require some form of intervention. The intervention might need to occur immediately or at some point in the future depending on the type or severity of the alarm. The quickest way to view all open alarms in your environment is from the Summary Dashboard.
- Look for groups of related alarms - Alarms can occur within a related group of resources. When groups of alarms occur, identify any shared physical resources and any shared software or services that serve as supporting resources for the group. You can quickly identify groups from the Monitored Technologies report or Top Groups by Alarm report in the Summary Dashboard. Once you identify a problematic group, you can use the links in the report to view more specific information about the group resources.
- Review metrics - Review the metrics of the highest-level resource with an alarm in the group. The metrics allow you to identify what system, instance, devices, components, or services are not performing well. It might be necessary to continue this review process until the true cause of the alarm is identified. For example, virtual machines might generate alarms if their host system runs out of memory. In this example, adding more memory to the host system

should resolve the virtual machine alarms. The summary dashboards for devices, groups, probes, and services contain reports that you can use to view key performance indicator metrics.

- Investigate how to prevent future problems – Once an issue is corrected, evaluate if more adjustments for alarms or more metrics are needed for your dashboards.

## MCS Dashboards

UIM 20.3.0 includes the MCS Dashboards functionality in the Operator Console. This functionality provides an overview of your device and device group monitoring profile configurations for MCS. You can view the information by groups—which contains groups, profiles, and devices summary. You can also view the information by devices—which contains devices and profiles summary. The summary contains information about the percentage of the categories that have been deployed, failed, pending, and not applicable. You can get more detailed information by further drilling down based on the count and percentage.

### NOTE

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

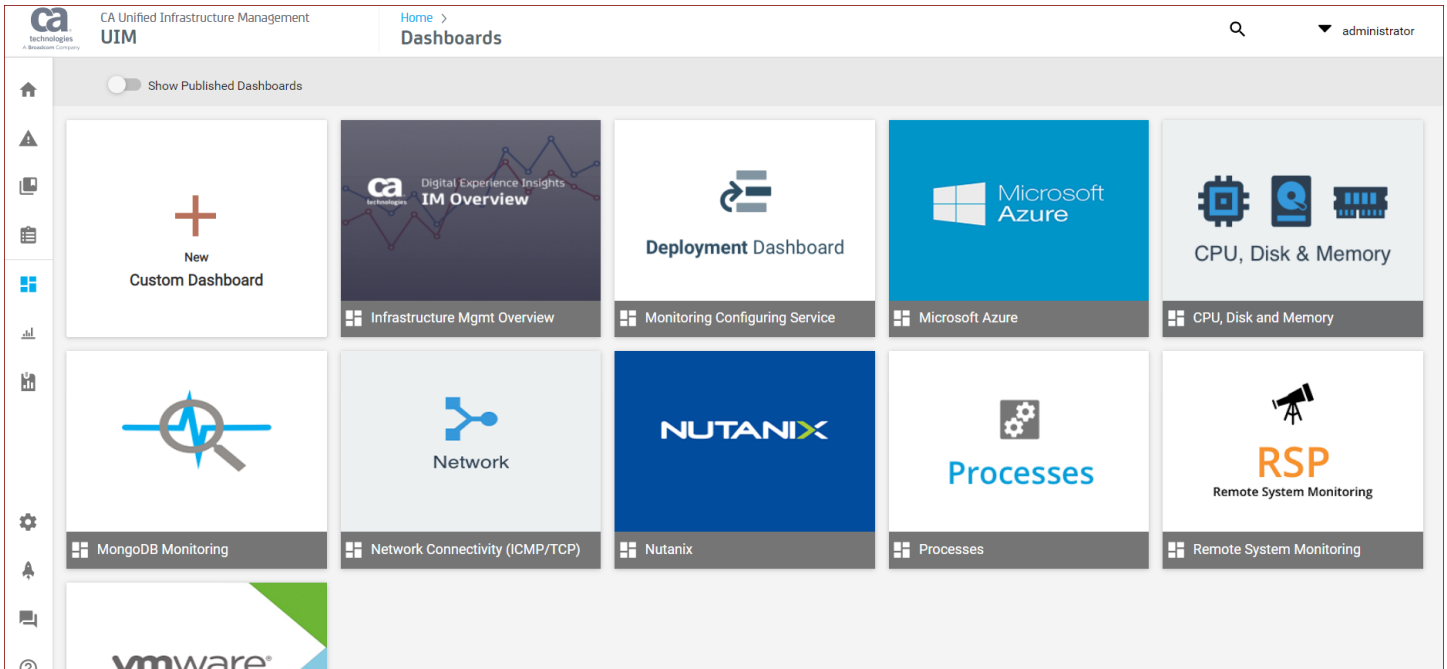
### Packages

The following packages are required for this functionality:

- mon\_config\_service on the UIM server machine.
- mcsuiapp\_portlet and ump\_operatorconsole on the Operator Console system.

### Understanding the Functionality

The MCS Dashboards feature is available in the Operator Console.



In the Dashboards view, a new "Monitoring Configuration Service" is available. There are two top-level tabs—"View By Groups" and "View By Devices".

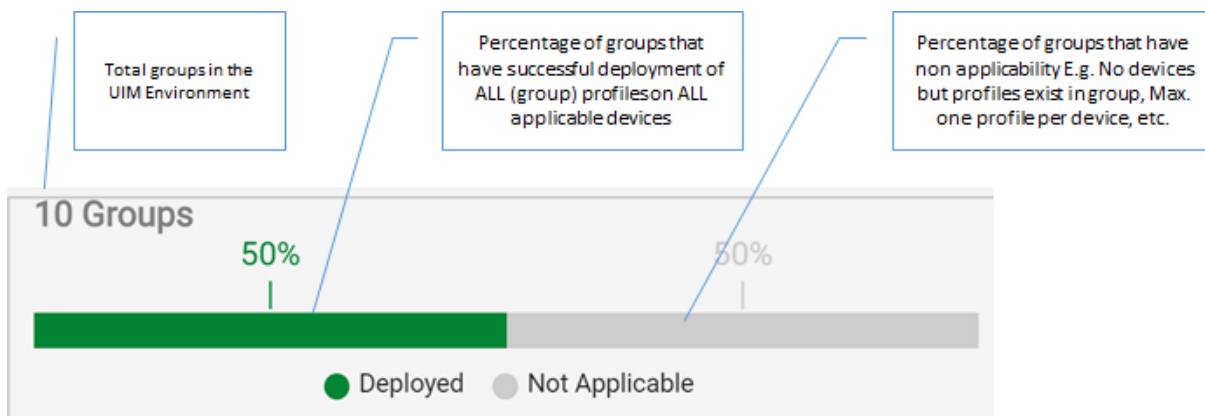
## View By Groups

## View By Devices

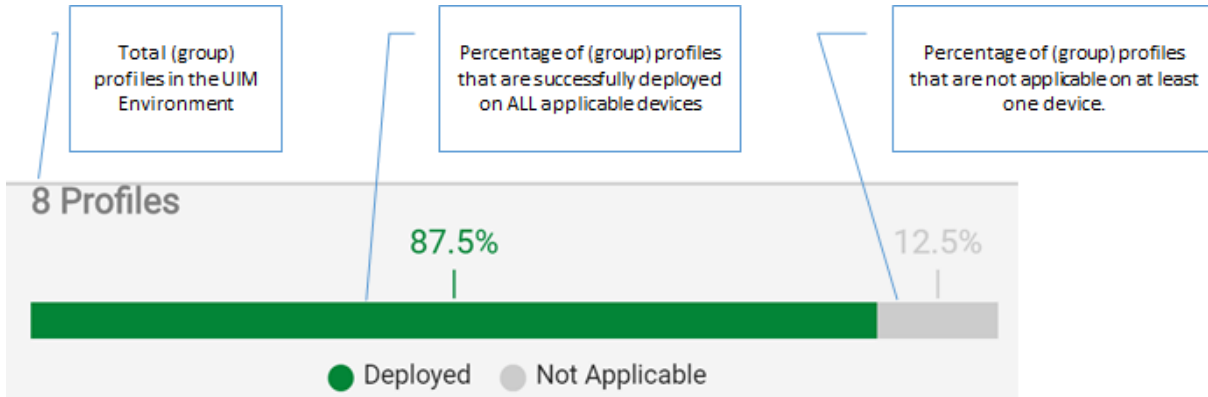
Dashcards are available that provide summarized information. Few examples are as follows:

### View By Groups:

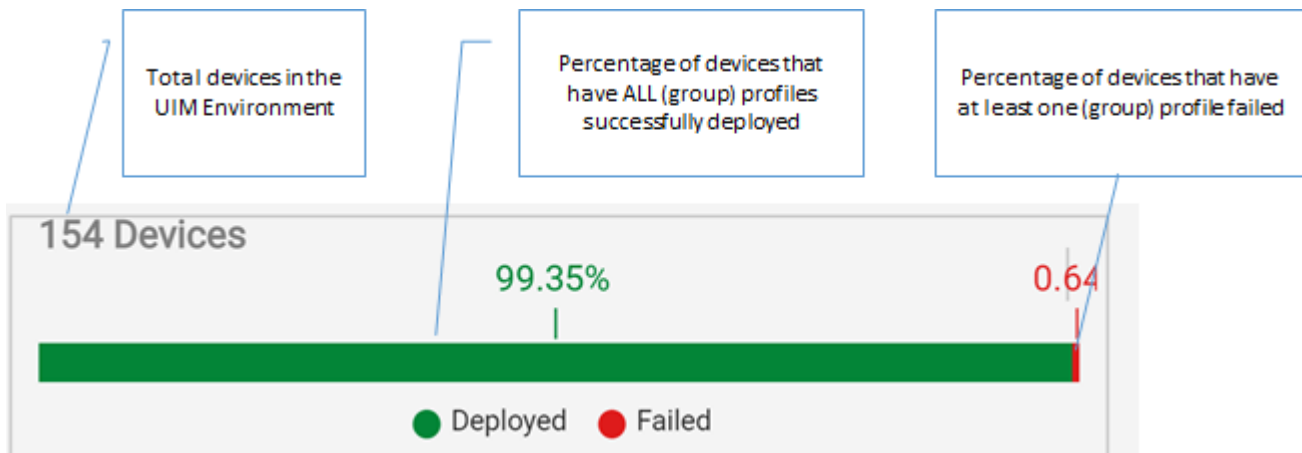
#### Example 1:



#### Example 2:

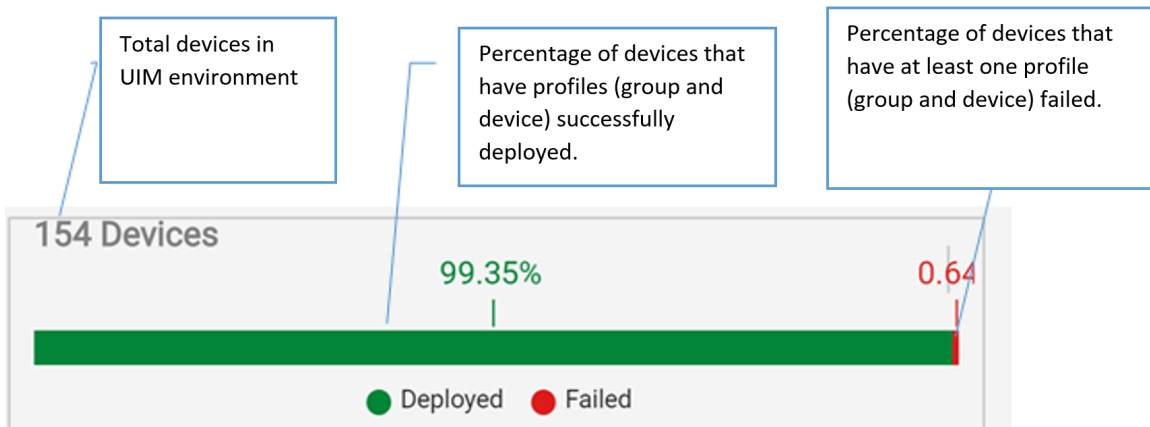


**Example 3:**

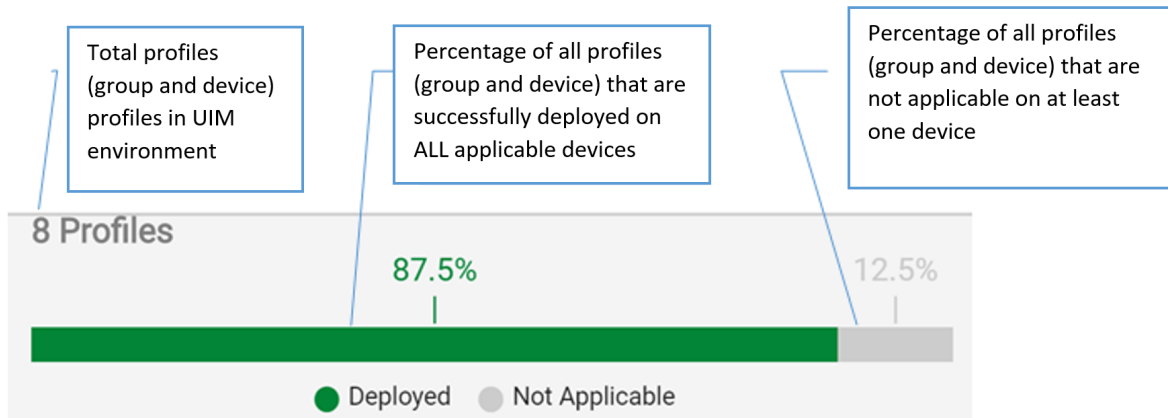


**View By Devices:**

**Example 1:**



**Example 2:**



### View the Information

Summary information in the MCS Dashboards helps you quickly understand the overall deployment scenario.

#### Follow these steps:

1. Access the Operator Console.
2. Click the Dashboards icon in the left pane.
3. Select MCS Dashboards
4. Click dashcards or bars.

All filtered entities of the type Groups, Profiles, and Devices are displayed in the Groups table, Profiles table, and Devices table respectively. This applies to both 'View By Group' and 'View By Device'.

5. Click the 'Clear' link in the dashcard to return to the original view (without filtering).
6. In View By Groups, review the following information:
  - Groups Table
    - Status shows percentage of group profiles that are present in that particular state.
    - Filter is enabled on the 'Name' column. To filter by status, use the dashcard filter (drill down). The filter and sort on the Name column are only on the group name and not on the hierarchical path. See the following example image that displays group names in the ascending order—190, Child Group, and DemoRobot:

Groups

| Name                                    | Profiles | Status                     |
|-----------------------------------------|----------|----------------------------|
| 190 (11 Devices)                        | 1        | ● 100% Deployed 11 Devices |
| parentContainer.Child Group (1 Devices) | 0        | ● NA                       |
| DemoRobot (5 Devices)                   | 3        | ● 10% Failed 5 Devices     |

- The sort on the Status column is on the status. For example, Deployed, Failed, Not Applicable, and Pending.
- Profiles Table
    - Status shows the percentage of the devices that are present in that particular state.
    - Filter is enabled on the Profile Name column. The sort on the Status column is on the status. For example, Deployed, Failed, Not Applicable, and Pending.
  - Devices Table
    - Filter is enabled on all the columns. Filter on 'Last Deployment Status' is on the profile name. Sort on 'Last Deployment Status' is on the last deployed date.
7. In View By Devices



- Devices table: Filter is enabled on all the columns. Filter on 'Last Deployment Status' is on the profile name. Sort on 'Last Deployment Status' is on the last deployed date.
  - Profiles table: Filter is enabled on the Profile Name column. Sort on 'Last Deployment Status' is on the last deployed date
    - Clicking any row displays the profile summary page with all the profile properties.
8. Click devices in dashcards or bars in the 'View By Groups' or 'View By Device' views. The device status with respect to the last deployed profile is displayed.
  9. Click the 'export' button. All the filtered entities are exported to CSV.
    - Example: In View by Groups, a filter is applied on the Name column of the Groups table and then export is clicked, the exported CSV contains only the entities that are filtered out.
    - In short, the exported CSV contains all the entities that are shown in the table including all pages (complete filtered list).

### **Known Issues/Limitations**

In View By Groups, clicking the devices dashcard restricts further navigation from the device table.

## **Create a New Custom Dashboard View**

UIM 20.3.3 lets you create new custom dashboard views using CA Business Intelligence (CABI) and add them to the OC Dashboards page. This ability helps you address situations where you want to create customized views of your dashboards depending on your needs. Therefore, in UIM 20.3.3, you can create these views in two ways: by using CABI or by using the already existing Dashboard Designer functionality.

### **Follow these steps:**

1. Access the OC UI.
2. Click the Dashboard link in the left pane.
3. Click the **New Custom Dashboard** tile. The **Add Dashboard** dialog opens:

## Add Dashboard

Cabi URL `http://...:80/cabijs`

Dashboard Path\* ▼

---

Default Alarm State  
Open Alarms ▼

---

Default Time Range  
1 Hour ▼

---

Default Minimum Alarm  
Minor ▼

---

Default Top N  
Top 10 ▼

---

Static Filters  
{} ▼

---

Dashcard name\*

---

CREATE    CANCEL

4. Enter the required information:

- **Dashboard Path:** Lets you choose the specific dashboard that you want to use to create the custom dashboard view. Select the required dashboard from the drop-down list, which displays the dashboard name along with its path.

**NOTE**

The default alarm state, default time range, default minimum alarm, and default top N filters are applicable only for the out-of-the-box dashboards.

- **Default Alarm State:** Lets you specify the alarm state that you want to use as the default value in the view. Select Open Alarms, Closed Alarms, or All Alarms from the drop-down list.
- **Default Time Range:** Lets you specify the time range that you want to use as the default range in the view. Select the required duration from the drop-down list.
- **Default Minimum Alarm:** Lets you specify the type of alarm that you want to use as the default value in the view. Select Information, Warning, Minor, Major, or Critical from the drop-down list.
- **Default Top N:** Lets you specify the top N entities in your dashboard that you want to use as the default value in the view. Select the required value from the drop-down list.
- **Static Filters:** A fixed dashboard filter defines the initial input parameters for the dashboard. The format is the filter name and then the array of the filter values. For example:
  - To collect data from the aws and vmware probes in a dashboard, enter `{'prid':['aws','vmware']}`.
  - To collect data in a dashlet for a specific device, enter `{'cs_id':['6']}`.
- **Dashcard Name:** Lets you specify the name that you want to use for the custom dashboard view.
- **Description:** Lets you specify a meaningful description for the dashboard view.

5. Click **Create**.

The new custom dashboard tile is created and is displayed in the UI.

## View Your Reports

After you have configured your monitoring, you can view a library of dynamic reports that provide deeper insight into your monitored infrastructure.


### NOTE

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

### Contents

#### Accessing Your Reports

##### Follow these steps:

1. To access your reports, click the **Reports** icon  in the left navigation tree of the Operator Console (OC).
2. Select the report category and then the report you want to run. You can apply different input options to define the report data as necessary.

#### Run or Schedule Reports

For each report tile, you can run a report immediately (**Run Now**) or schedule it to run at a later date (**Schedule**). When you run a report immediately, it opens a new window to display the report details. When you schedule a report, the CABI UI opens where you can define the schedule details of the selected report.

#### Create Ad-hoc Reports

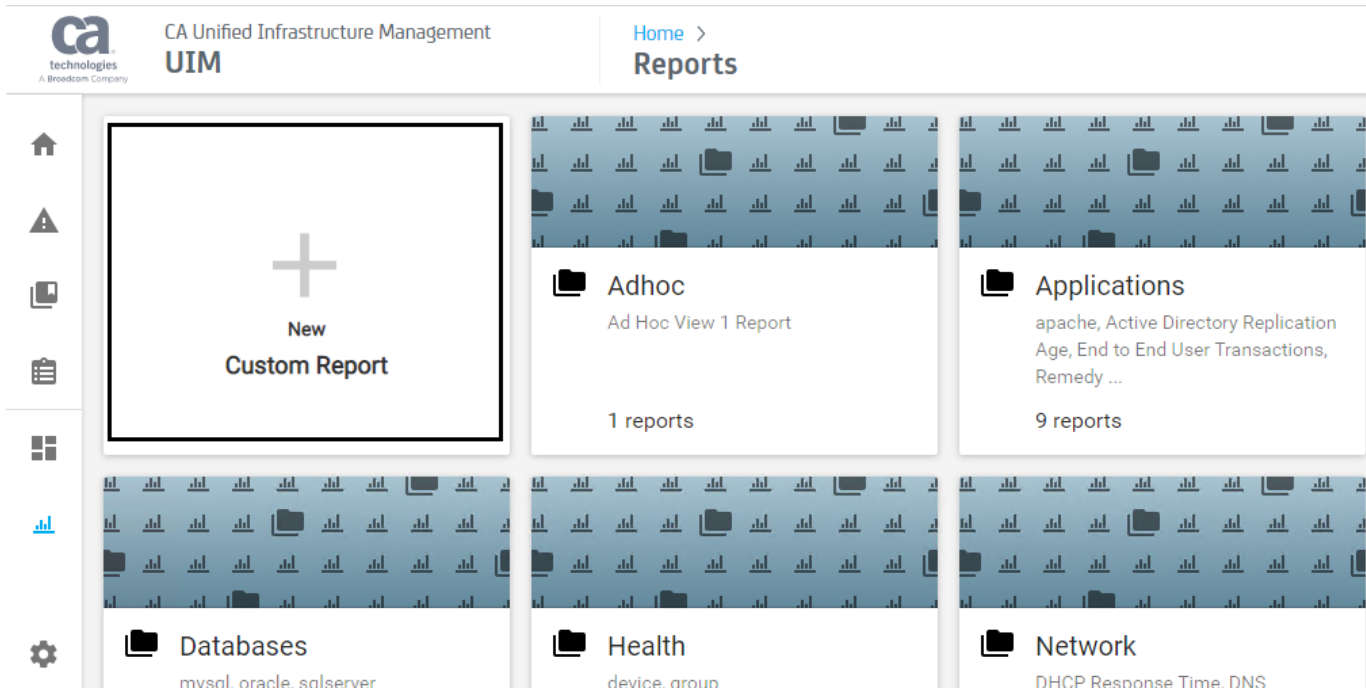
Folders in the Reports view contain many predefined reports (dashlets). If predefined information does not meet your needs, you can create a custom report using the Custom Report option. When you click on the Custom Report option, the CABI UI opens where you can define further details. For more information, see the [TIBCO JasperReports Server User Guide](#).

##### Follow these steps:

1. In the Reports view, click **New Custom Report**.  
The CABI Reports UI opens.
2. Create an Ad Hoc view to create a report.
  - To create a view for alarms, devices, or groups, select **UIM Domain**.
  - To create a view for a single metric, select **UIM Single QoS Topic**.
  - To create a view with data from multiple metrics and devices, select **UIM Metric Topic**.
3. Create a report from the Ad Hoc view.  
All custom reports appear in the custom folder in the Reports view.

## Create User/Account-Specific Report Views

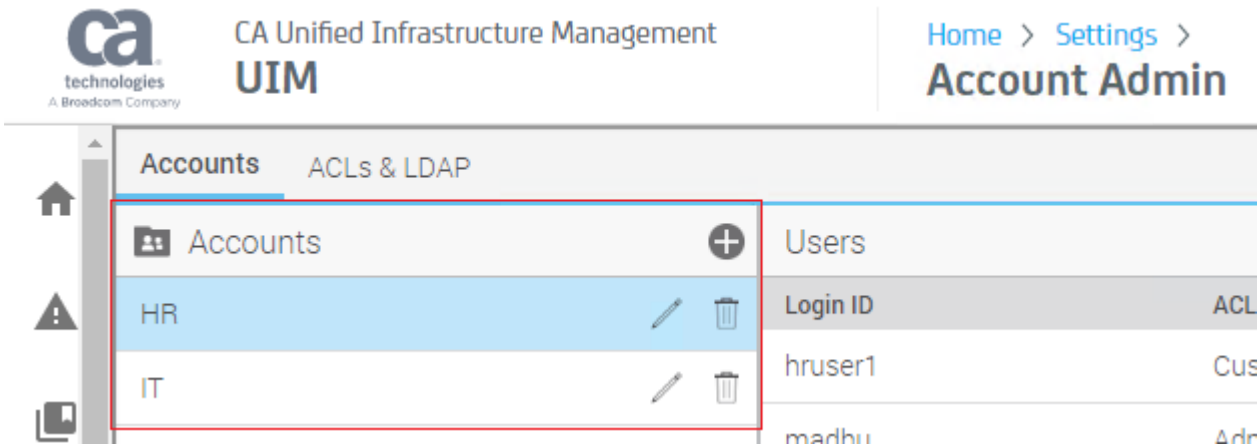
All the CABI reports saved under the `/public/ca/uim/reports/library` folder (or subfolder) of CABI are visible to all the users of OC.



However, some organizations want to restrict these custom views so that only authorized users can access the reports. Other users must not be allowed to access them. When users create a custom report, they get the option to select the folder to save their reports. Superusers can provide the user/account-level access so that the users can save their custom reports under those folders to which they have access. After creating the custom reports under those folders, when they log in to OC, they can view those reports that they have saved. This way, one user cannot view the custom reports created by another user.

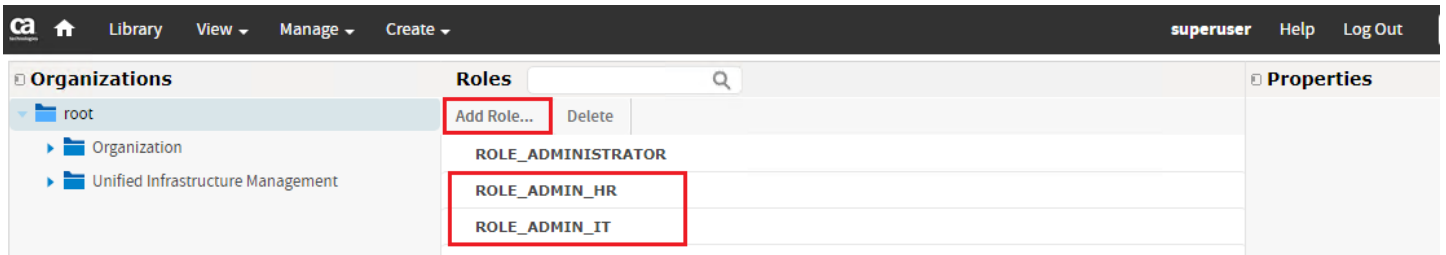
### Follow these steps:

1. Log in to OC.
2. Navigate to **Settings, Account Admin**.
3. Verify all the accounts. The following screenshot shows the two accounts HR and IT:

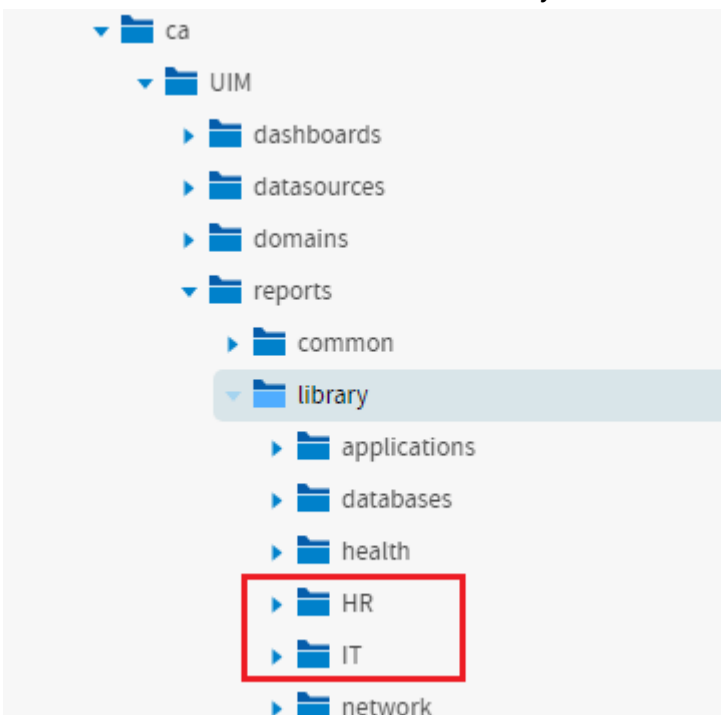


4. Log in to Jasper Server with superuser credentials.

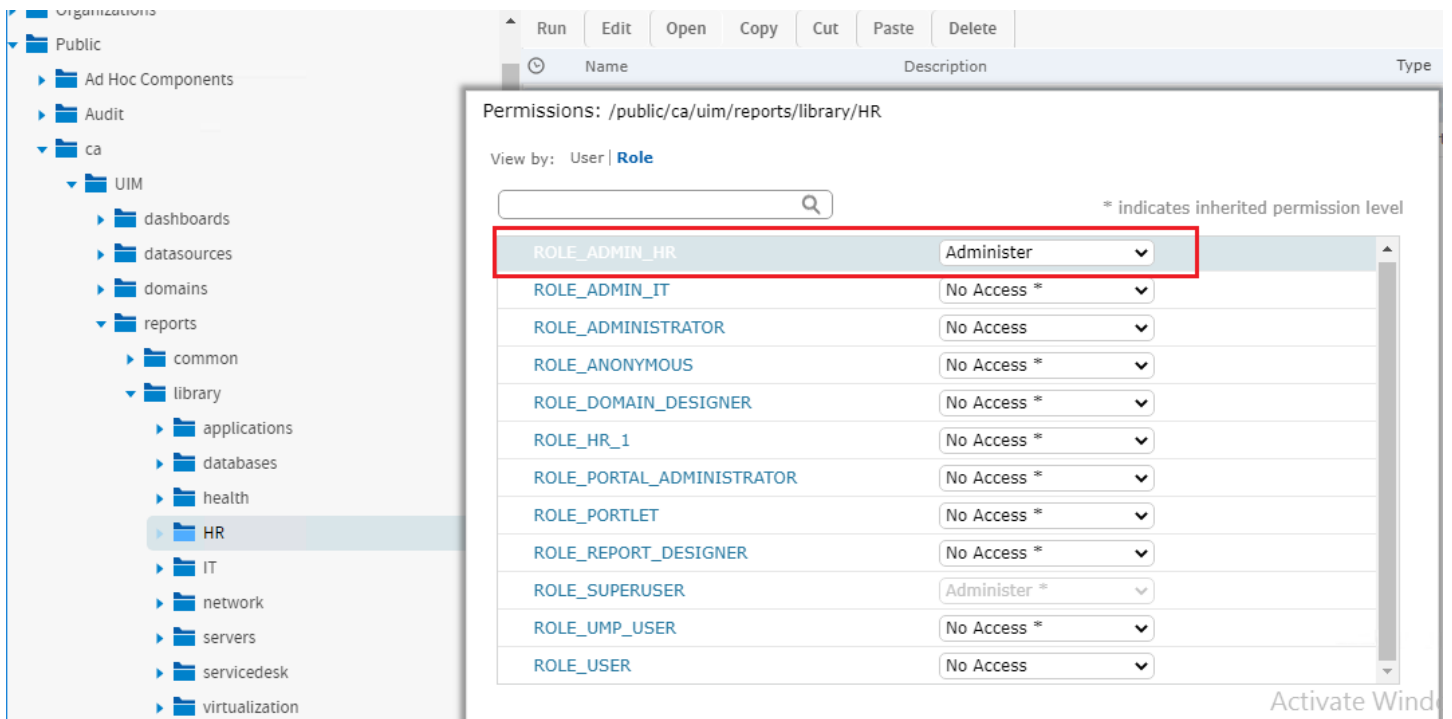
5. Click **Manage, Roles**.
6. Add a new role for each account. The following screenshot shows that the two new roles, ROLE\_ADMIN\_HR and ROLE\_ADMIN\_IT, are added:



7. Click **View, Repository**.
8. Navigate to the `/public/ca/uim/reports/library` path.
9. Create subfolders for different accounts under the `library` folder. The following screenshot shows that the two new folders HR and IT are created under the `library` folder.



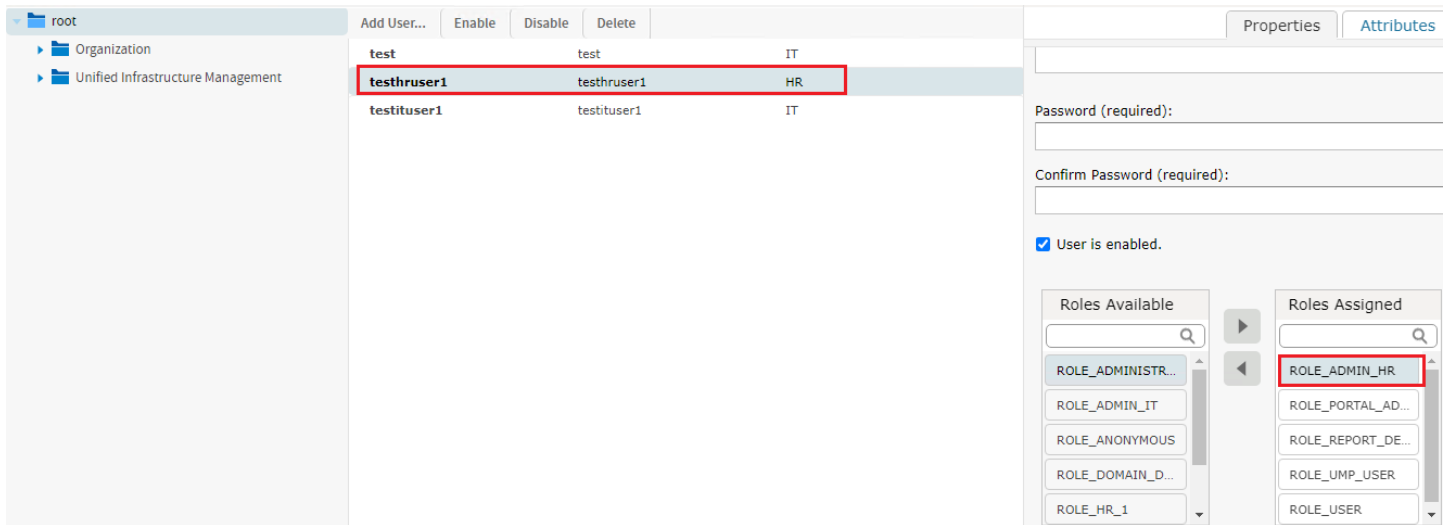
10. Select the account name folder (for example, HR).
11. Right-click, select the permissions option, and give the **Administer** permission to the HR role (ROLE\_ADMIN\_HR), which was added in one of the previous steps.
12. Remove the permission of the other roles and users. The following screenshot shows the required information:



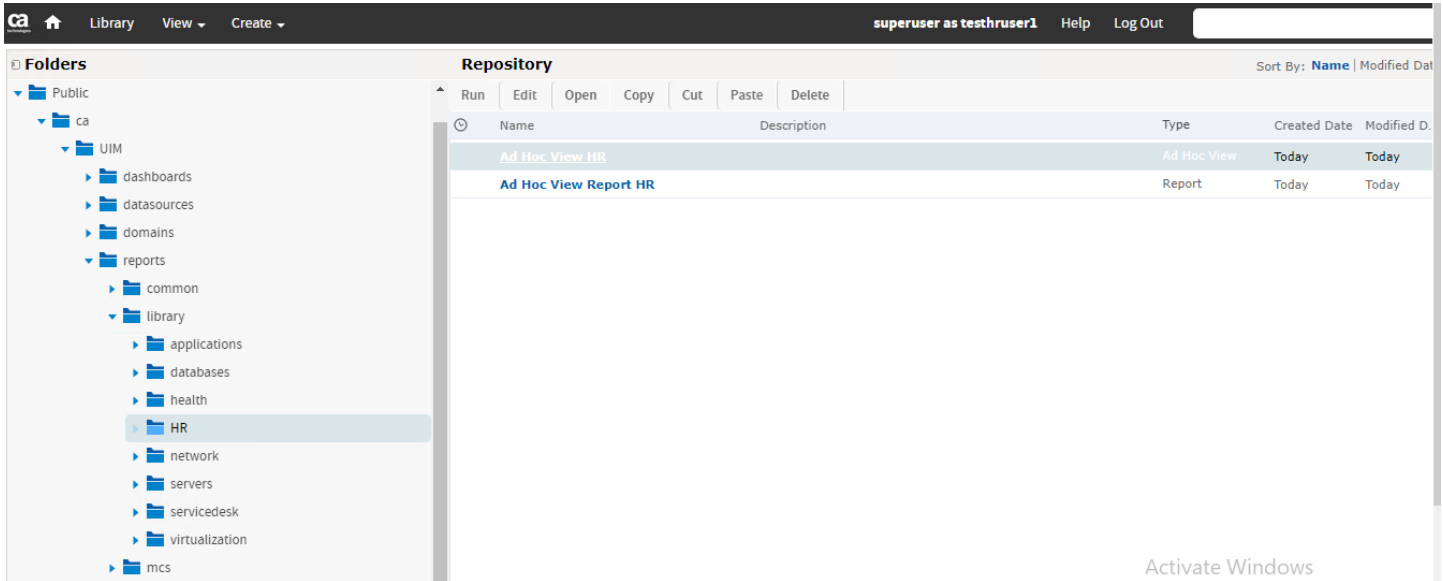
13. Follow the same steps for the other account folders.

14. Click **Manage, Users**.

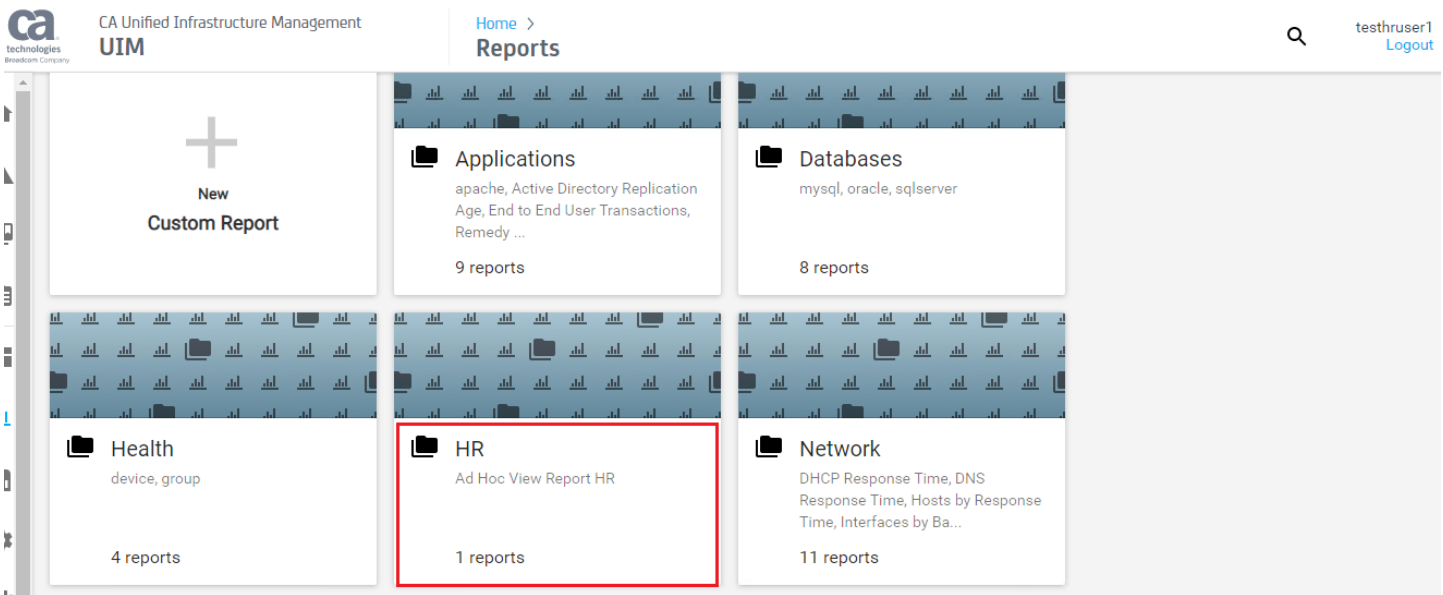
15. Assign the account-specific role to all the users of that account. These are those users to whom you want to provide access to the account-specific reports. The following screenshot shows that the testhruser1 user is assigned the ROLE\_ADMIN\_HR role:



16. Log in as an account user (for example, testhruser1), create views and reports, and save the reports under the account (HR) folder. The following screenshot shows the required information:



17. Log in to OC with the same user credentials and see the reports. These are the same reports that are created under the account-specific (HR) folder. The following screenshot shows that the HR report view is now available for the testhruser1 user:



You have successfully created user/account-specific views.

**NOTE**

When you log in with a different account user, you see the same report view until you restart the wasp probe.

**Available Reports**

For a list of available reports, refer to the topic [List of Reports](#).

# View Your Inventory

## The Inventory view



the left navigation of the Operator Console allows you to view computers and devices that have been discovered on your managed environment. The Inventory section of the tree contains discovery agents, with network scopes under each discovery agent. The tree also has an Automatic and an External node.

You can see alarm counts, the monitoring technologies applied, and the role for each device. The robot column indicates which devices are monitored locally by a monitoring agent (referred to as a robot) or remotely from a monitoring host.

## Tree View Navigation for the Inventory

Along with the List view, Tree view structure is supported for the navigation for inventory and devices with the alarms, roles and hierarchy are displayed.

Click on the button on the right will open the tree view structure.

Click a node in the tree to view associated systems and their properties in the table.

The screenshot shows the UIM interface with the 'Inventory' view selected. The main table displays a list of devices with columns for Name, Device Type, Operating system, and IP address. An 'Inventory Tree' sidebar is open on the right, showing a hierarchical view of the inventory structure.

| Name                      | Device Type    | Operating syst...        | IP address       |
|---------------------------|----------------|--------------------------|------------------|
| lvndev003682.bpc.broa...  | Device         |                          | 10.74.113.13     |
| lvntest017288.bpc.broa... | Host           | WindowsServer-2019 (1... | 10.74.128.42     |
| lvntest012408             | Host           | WindowsServer-2016       | 10.74.90.147     |
| asdasd                    | Device         |                          |                  |
| 10.112.65.77              | Device         |                          | 10.112.65.77     |
| 1.2.3.95                  | Device         |                          | 1.2.3.95         |
| mycomputer.mycompan...    | DatabaseServer | WindowsServer-2008 (6... | 2.2.2.2, 1.2.3.2 |
| lvndev005251.bpc.broa...  | Device         |                          | 10.74.128.212    |
| lvndev005253.bpc.broa...  | Device         |                          | 10.74.128.213    |

The Inventory Tree sidebar shows a hierarchy starting with 'Inventory (679)', followed by several nodes under 'lvnqa012407\_domain' and 'lvnqa012407\_domain/lvndev012409 (52)'.

## Generated Alarms

Click an alarm count



in the first column to access details about the alarms that are generated for a specific device.



## View Summary Data or a Device Dashboard

Click the Information



icon that is next to a device name to view information, alarms, or maintenance schedule of a specific device.

## View Maintenance Schedule for Devices

You can view the maintenance schedule for devices at a single location. When you select a device through the Inventory view, you can view all the maintenance schedules that include the selected device.

### Follow these steps:

1. Click the Information icon (Name column) for the selected device.
2. Select the **Maintenance** tab.

| Schedule | Status   | Disassociate |
|----------|----------|--------------|
| SC-1     | Inactive | ⊖            |
| SC2      | Inactive | ⊖            |

3. Review the following information:
  - Name of the maintenance schedule that contains the device.
  - Status (Active or Inactive) of the maintenance schedule that contains the device.
  - An option to remove the device from the maintenance schedule. When you click the minus icon (Disassociate column), the device is removed from the maintenance schedule. The corresponding row is also removed from the table.

## Sort Data

Click a column title to sort the content in a column.

## Filter Data

The quick filter at the upper-left selects items in any of the text columns (**Name** through **Monitored by**) for display. The **Monitored by** column lists only those probes that have generated alarms or metrics for a monitored device.

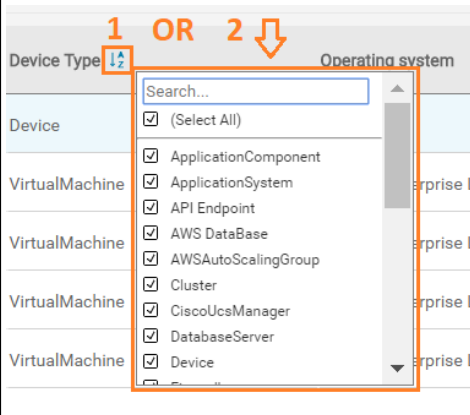
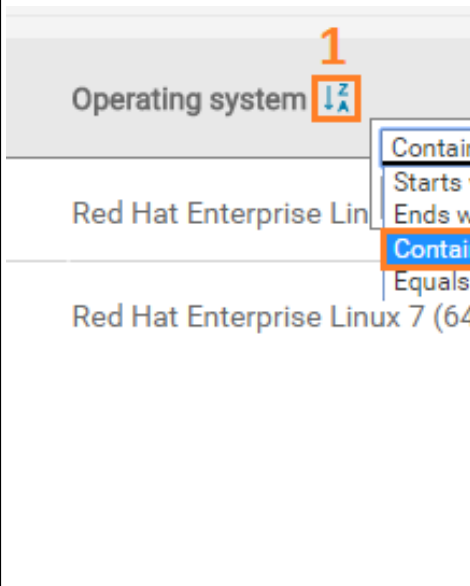
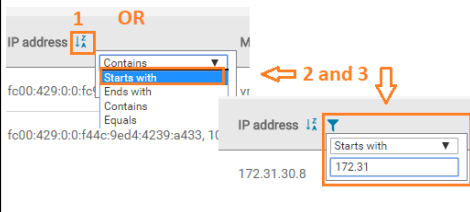
### NOTE

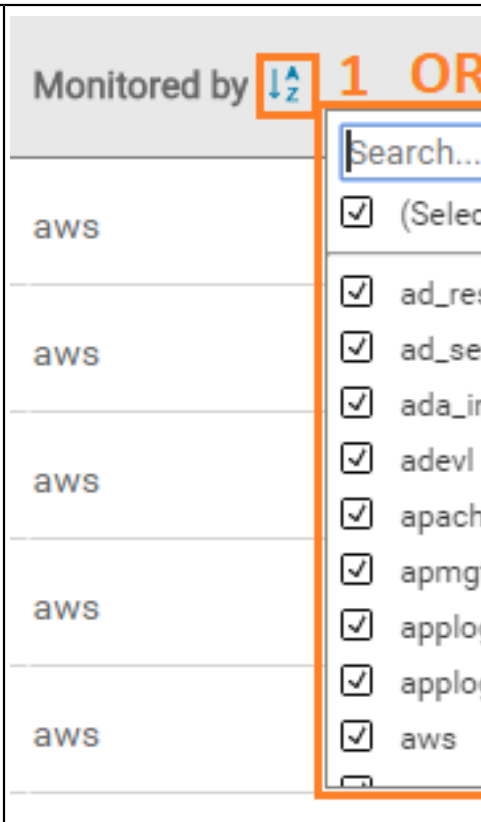
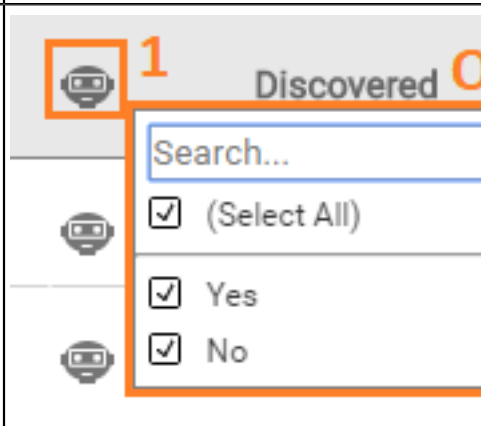
If a filter criteria appears in more than one column, such as an operating system name that also appears in the device name, all rows containing the filter text are displayed.

### Additional Column Filters

For each column in the inventory view, you can apply additional filter options to narrow your search. Move the mouse pointer to the column to view the filter options.

| Column Name           | Filter | Description                                                                                                                                                                                                                                                          |
|-----------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Alarm Severity</b> |        | <p>Filter alarms based on alarm severity:</p> <ul style="list-style-type: none"> <li>View a sorted list based on the alarm count (shown as 1 in the image).</li> <li>Use specific alarm severity to view the related (shown as 2 in the image).</li> </ul>           |
| <b>Name</b>           |        | <p>Filter devices based on the device name:</p> <ul style="list-style-type: none"> <li>View a sorted list based on the device name (shown as 1 in the image).</li> <li>Use specific device name to view the related list (shown as 2 and 3 in the image).</li> </ul> |

|                                |                                                                                      |                                                                                                                                                                                                                                                                                            |
|--------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Device Type</b></p>      |    | <p>Filter devices based on the device type:</p> <ul style="list-style-type: none"> <li>View a sorted list based on the device type (shown as 1 in the image).</li> <li>Use specific device type to view the related list (shown as 2 in the image).</li> </ul>                             |
| <p><b>Operating System</b></p> |   | <p>Filter devices based on operating system:</p> <ul style="list-style-type: none"> <li>View a sorted list of devices based on the operating system (shown as 1 in the image).</li> <li>Use specific operating system to view the related list (shown as 2 and 3 in the image).</li> </ul> |
| <p><b>IP Address</b></p>       |  | <p>Filter devices based on IP address:</p> <ul style="list-style-type: none"> <li>View a sorted list of devices based on the IP address (shown as 1 in the image).</li> <li>Use specific IP address to view the related list (shown as 2 and 3 in the image).</li> </ul>                   |

|                            |                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Monitored By</b></p> |   | <p>Filter devices based on the technologies that are monitoring them:</p> <ul style="list-style-type: none"> <li>• View a sorted list of devices based on the monitoring technology (shown as 1 in the image).</li> <li>• Use specific monitoring technology to view the related list (shown as 2 in the image).</li> </ul>                                                                     |
| <p><b>Has Robot</b></p>    |  | <p>Filter devices based on whether a robot is deployed on the device:</p> <ul style="list-style-type: none"> <li>• View a sorted list of devices based on the robot deployment or non-deployment (shown as 1 in the image).</li> <li>• View a list of devices that have robot deployed on them, not deployed on them, or both (deployed and not deployed) (shown as 2 in the image).</li> </ul> |

**Discovered**

Discovered **1 OR 2**

Search...

(Select All)

< 4 hours

< 10 hours

< 1 day

< 2 days

< 1 week

< 1 month

< 3 months

< 6 months


< 1 year

Filter devices based on the time when those were discovered:

- View a sorted list of devices based on the time interval (shown as 1 in the image).
- View a list of devices filter based on any specific time interval (shown as 2 in the image).

### Actions Menu

Click the Actions menu

(  )  
 at the top right of the Inventory view to import the devices, discover the devices and deploy the robots. The menu has the following options:

- **Import** - to import xml file with the device information  
 Import functionality is for importing devices only and not for deploying robots.
- **Discovery Wizard** - to launch devices for discovery.
- **Robot Deployment** - to deploy robots using OC.

CA Unified Infrastructure Management UIM

Home > Inventory

Filter 684 a few seconds ago

| Name                           | Device Type | Operating system | IP address    | Monitored by | Discovered |
|--------------------------------|-------------|------------------|---------------|--------------|------------|
| 10.10.150.2                    | Device      |                  | 10.10.150.2   |              | 3 days ago |
| 10.150.10.4                    | Device      |                  | 10.150.10.4   |              | 3 days ago |
| 10.10.150.3                    | Device      |                  | 10.10.150.3   |              | 3 days ago |
| 10.10.150.1                    | Device      |                  | 10.10.150.1   |              | 3 days ago |
| 10.105.10.5                    | Device      |                  | 10.105.10.5   |              | 3 days ago |
| 1.23.33.34                     | Device      |                  | 1.23.33.34    |              | 3 days ago |
| lnntest005287.bpc.broadcom.net | Device      |                  | 10.74.128.229 |              | 3 days ago |

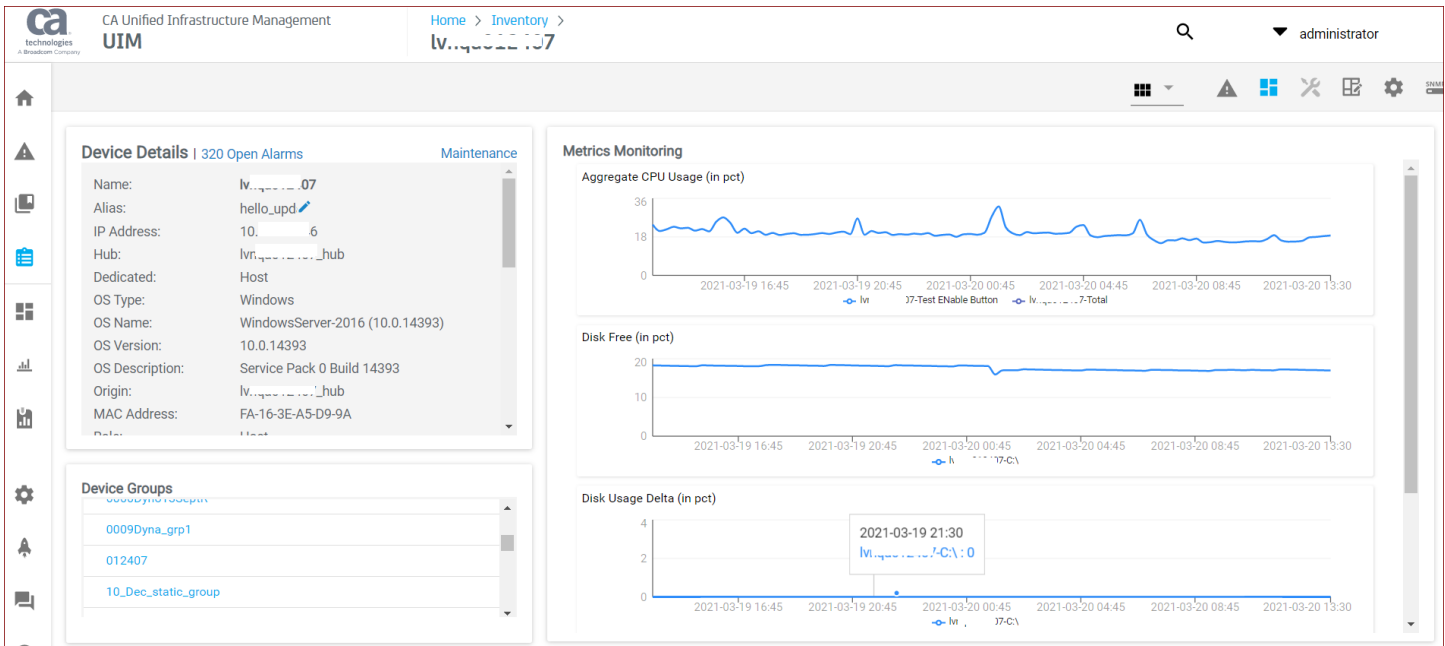
Import  
 Discovery Wizard  
 Robot Deployment

### Device Details (Dashboard) View

After you click a device in the inventory view, you can then access the device details (dashboard) view. The following screenshot shows the device dashboards (details) view (native OC screen) in UIM 20.3.3. This screen is rendered using HTML5; it is no longer dependent on CABI in UIM 20.3.3:

**NOTE**

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article



This view helps you as follows:

- **Device Details**

View the the summary about the details of the device. This includes detailed information; for example, name, IP address, hub, OS, information about the maintenance schedule of the device, and so on.

- **Open Alarms Count**

- View the count of the open alarms for the selected device.
- Click the alarm count link to navigate to the detailed view.

**NOTE**

If the device is in maintenance, the alarms count is not displayed. Instead, the maintenance mode symbol is displayed.

- **In-Context Maintenance Link**

- Put the device in the maintenance schedule by using the in-context Maintenance link in the Device Details tile. Click the Maintenance link and specify the maintenance schedule details. The device is then included in the maintenance schedule. The related maintenance information is then displayed at the bottom of the same Device Details tile.

- **Edit the Device Alias**

- Click the edit icon (pencil) next to Alias, provide the appropriate name in the dialog, and click Apply to save the update.

- **Device Groups**

View the groups associated with the selected device.

- Click the respective group link on the tile to navigate to the related Groups view to find more information.
- **Metrics Monitoring**  
View the metrics monitoring charts (metric views) for the device. Metrics view that is created for the selected device is displayed under Metrics Monitoring. If no metrics view is defined, then the view based on the default metrics (for example, CPU) is displayed by default. If the Metrics Monitoring section is empty, it implies that no monitoring is configured for the device.
- **Properly Created URL**
  - Use the properly created URL to directly access the device dashboard view: `http://<OC_Server>/operatorconsole_portlet/computer_systems/<CI_ID>/dashboard`

**NOTE**

If you try to access this device view by navigating through the Groups path (Groups view -> Group -> Device), then you need to click the Detail view icon to access this view. The Dashboard view icon is disabled in this case.

## Using Setup Wizard

The Setup Wizard allows you to configure Device Discovery or configure the available remote and cloud monitoring technologies as Tiles.

- Configure Device Discovery  
For more information on configuring device discovery, see [Device Discovery](#).
- Configure Remote and Cloud Monitoring Technologies
  - The monitoring technology tiles are arranged under the following categories:
  - Public Cloud
  - Server
  - Response
  - Remote
  - Private Cloud and Virtualization
  - Database
  - Application

The number of monitoring technologies belonging to a specific category is displayed adjacent to the category title. For more information on configuring local monitoring technologies, see [Monitoring Technologies](#).

### **Using the Search on Setup Wizard**

Click **Remote and Cloud** in the **Setup Wizard** and navigate to and search for the required technology in the search box:



You can search based on the following search criteria:

- Technology name, such as Azure, cdm, oracle, and so on.
- Technology category, such as cloud or remote
- Technology type, such as Microsoft

#### **WARNING**

The only local monitoring available from the Setup Wizard is for Linux or Windows devices.



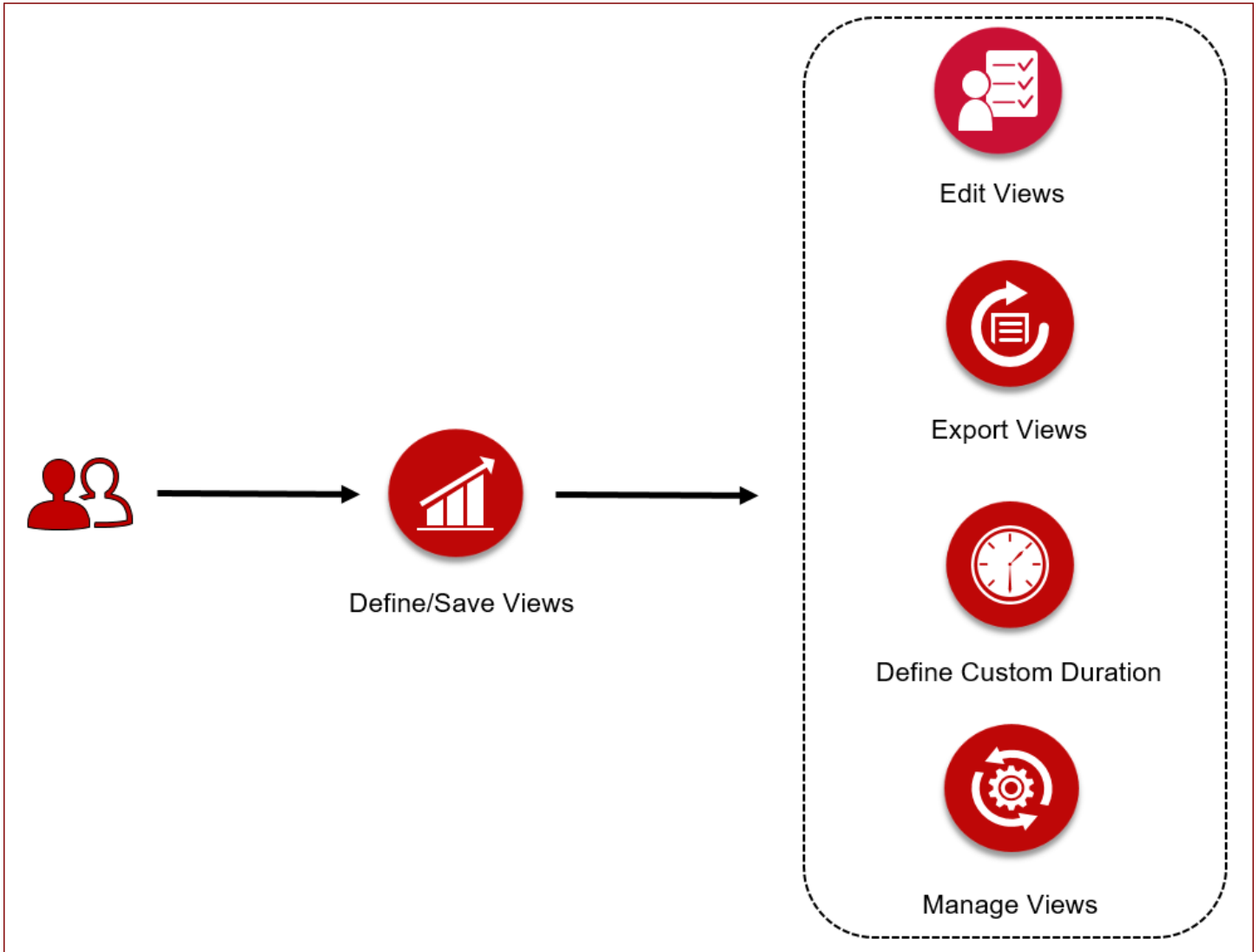
**Example:** Enter Microsoft in the search box. The count and tiles of all the currently supported Microsoft-based monitoring technologies are displayed.

The screenshot displays the CA Unified Infrastructure Management (UIM) interface. At the top left is the CA Technologies UIM logo. The breadcrumb navigation shows 'Home > Setup Wizard > Remote And Cloud'. A notification banner at the top indicates 'Local Monitoring' with a link to 'Read more'. The main content area is titled 'Setup Infrastructure Monitoring' and is divided into two sections: 'SERVER | 1 Technology' and 'RESPONSE | 1 Technology'. The 'SERVER' section features a blue tile for 'Windows' with '+ ADD' and 'CONFIG' buttons and a 'Devices: 6' indicator. The 'RESPONSE' section features a blue tile for 'Active Directory' with a 'Response' button. A vertical sidebar on the left contains various navigation icons. The footer of the interface includes the copyright notice '©2020 CA. All rights reserved.'

#### NOTE

## Working with the Metrics Palette

The **Metrics** palette displays, in a single window, the configured key performance indicators (KPI) based on the role of a device. The KPI metrics quickly provide insight into the operation of a device. For example, if the selected device is a host, the KPI metrics displayed on the device dashboard and the **Metrics** palette could include CPU usage (total), disk usage, and memory usage. These KPI metrics let you know how a device is functioning and whether it needs attention.



The following topics provide the required information:

**NOTE**

The KPIs can vary between probes or device types.

The following illustration helps you quickly understand how you can access and create a metrics view:

| Name                   | Device Type    | Operating system      | Origin          | IP address | Monitored by | Discovered   |
|------------------------|----------------|-----------------------|-----------------|------------|--------------|--------------|
| ss030626_win2012r2_vm1 | Device         |                       | lvnqa014673_hub |            | net_connect  | 16 hours ago |
| tas-tn-w16             | VirtualMachine | WindowsServer-2012    | lvnqa014673_hub |            | vmware       | 19 days ago  |
| TAS-ITC-WIN10          | VirtualMachine | Windows-8             | lvnqa014673_hub |            | vmware       | 19 days ago  |
| TAS-ITC-WIN10          | VirtualMachine | WindowsServer-2008-R2 | lvnqa014673_hub |            | vmware       | 19 days ago  |
| tas-tn-w64b            | VirtualMachine | WindowsServer-2008-R2 | lvnqa014673_hub |            | vmware       | 19 days ago  |
| tas-tnl-co7            | VirtualMachine | Linux-CentOS          | lvnqa014673_hub |            | vmware       | 19 days ago  |
| tas-tn-w12             | VirtualMachine | WindowsServer-2012    | lvnqa014673_hub |            | vmware       | 19 days ago  |
| tas-itcapm-n98         | VirtualMachine | Linux-CentOS          | lvnqa014673_hub |            | vmware       | 19 days ago  |
| tas-itcflid-n3         | VirtualMachine | WindowsServer-2008-R2 | lvnqa014673_hub |            | vmware       | 19 days ago  |
| TAS-F5                 | VirtualMachine | Other (64-bit)        | lvnqa014673_hub |            | vmware       | 19 days ago  |
| tas-itcapm-na1         | VirtualMachine | WindowsServer-2008-R2 | lvnqa014673_hub |            | vmware       | 19 days ago  |
| w2k8itcass03           | VirtualMachine | WindowsServer-2008    | lvnqa014673_hub |            | vmware       | 19 days ago  |

### Overview of Tasks in Metrics Palette

You can perform various operations in the Metrics palette; for example:

- Define and save a metrics view.
- Rename, copy, or delete the views.
- Export the saved views.
- Publish the views at private, account, or public level.
- Set a default view for a given device or group.
- Configure the custom duration.


The subsequent sections in this article explain these tasks.

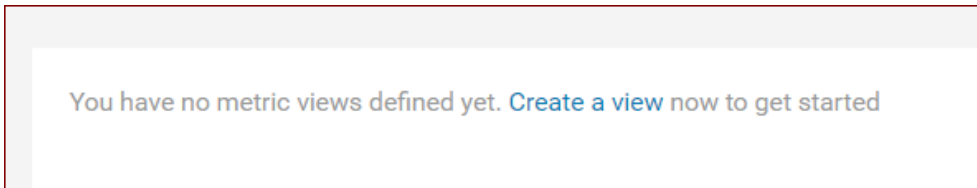
### Define and Save a Metrics View

You can define and save your metrics view for each device/group. The ability to save the views lets you access them at a later stage whenever you need.

#### Follow these steps:

1. Log in to the OC UI.
2. Access the required device or group view.
- 3.

Click the Metrics icon (  ) in the top-right section of the UI. A page with the following message opens:



**NOTE**

If a view is already defined, the above message is not displayed. That is, the **Create a view** option is not available. In that case, you use the **New View** option to create another view. The **Create a view** option is displayed only when no view is defined for that entity.

4. Click the **Create a view** option.  
The **New Metrics View** dialog opens.

| <input type="checkbox"/> | Name               | Type           |
|--------------------------|--------------------|----------------|
| <input type="checkbox"/> | .....dhcp.br...    | VirtualMachine |
| <input type="checkbox"/> | .....dhcp....      | Host           |
| <input type="checkbox"/> | .....bo.dhcp.br... | Host           |
| <input type="checkbox"/> | .....dhcp.broad... | Host           |
| <input type="checkbox"/> | .....dhcp.broa...  | Host           |
| <input type="checkbox"/> | .....dhcp.broad... | VirtualMachine |
| <input type="checkbox"/> | .....dhcp.br...    | Host           |

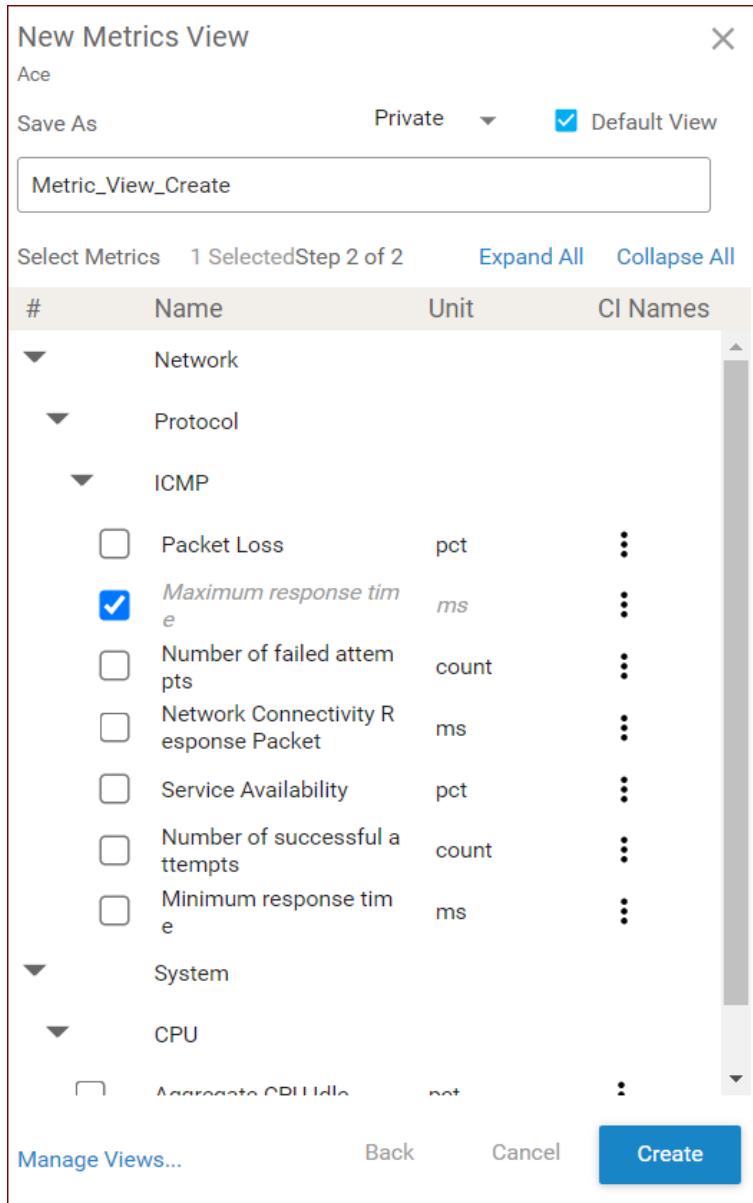
5. Enter an appropriate name for the view in the **Save As** field.
6. Select the access level (private, account, or public) from the drop-down list:
  - **Private** implies that the view is available only for self-use.
  - **Public** implies that the view is accessible to all the UIM users.
  - **Account** implies that the view is saved and shared at the account level. Only users belonging to the same account can access the view.
7. Select the **Default View** option to make the current view as the default view for the given device or group.
8. For groups:
  - a. Select the required devices from the displayed list, and click **Next**.

**NOTE**

You can use the Search field (under Select Devices) to quickly find the device. You can also use the [Advance Filter](#) option to define the filter criteria and then select the required device from the filtered

list. When you click the Advance Filter option, a dialog opens that lets you provide the filter details. Click the Clear Filter option to clear the applied filter.

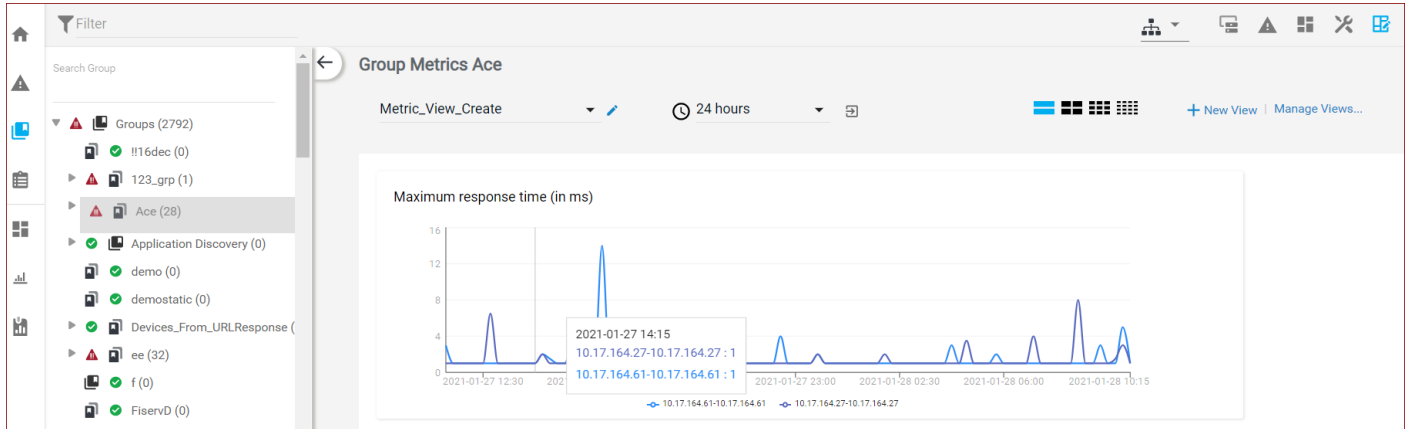
- b. Select the metrics in which you are interested from the displayed list. The following screenshot shows the required information:



9. (For devices) Select the required metrics from the displayed list.

10. Click the **Create** button.

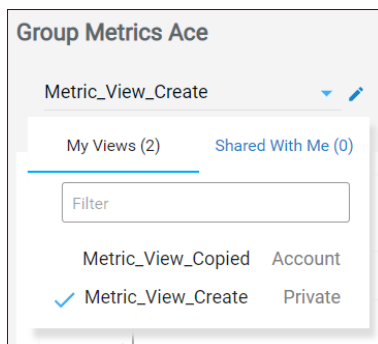
The view is created and displayed in the UI:



You have successfully defined and saved the metrics view.

### Access the Created Metrics View

When a view is saved, it is added to the metrics view drop-down list. You can use this drop-down list to retrieve the saved metrics view. The following screenshot shows the metrics view drop-down list:



When you access this drop-down list, you can verify that the **My Views** option lists the views that you have created. Whereas, the **Shared With Me** option lists the views that are shared with you (for example, public- or account-level views). Also, review that the default view has a tick mark before its name. This helps you quickly identify which view is the default view for a specific device/group. Therefore, whenever you access the metrics view for that device/group, you always see the related default view displayed in the UI.

### Working with Advance Filter for Devices

The Advance Filter option is displayed in the UI when you try to define the views at the group level. You can create the filters and quickly find the devices in a group. You can then select the devices in which you are interested.

#### Follow these steps:

1. Click the **Advance Filter** option while creating the metrics view for a group. The following screenshot shows the advance filter options:

**Match Filters**

All ▾

| ID | Field  | Operator | Value |   |
|----|--------|----------|-------|---|
| 1  | Name ▾ | = ▾      |       | + |

Cancel Apply


2. Select the appropriate field for defining the filter from the **Field** drop-down list.
3. Select the required operator from the **Operator** drop-down list.
4. Enter the appropriate value in the **Value** field.
5. Click the plus (+) icon to add a new row to define additional filter criteria. Repeat this step to add more rows. Similarly, to remove a row, click the minus (-) icon.
6. Select one of the following options from the **Match Filters** drop-down list:
  - **All:** Applies the filter only when all the defined filter conditions are met. For example, if you have defined three rows, then the filter will work only when all the three conditions are met.
  - **Any:** Applies the filter when any one of the defined filter conditions is met. For example, if you have defined three rows, then the filter will work when any of the three conditions is met.
  - **Custom:** Applies the filter based on the criteria that you define in the **Custom Filter** field. For example, if you enter the expression as (1 AND 2) OR (3 AND 4) , the filter evaluates the expression and displays the result. In this case, 1, 2, 3, and 4 represent the row ID, which is displayed in the ID column. The ID 1 represents the criteria defined in the first row, the ID 2 represents the second row, and so on. The expression (1 AND 2) OR (3 AND 4) implies that the filter is applied and the result is displayed only when
    - *condition 1 AND condition 2* are true
    - OR**
    - *condition 3 AND condition 4* are true
7. Click **Apply** to apply the filter.

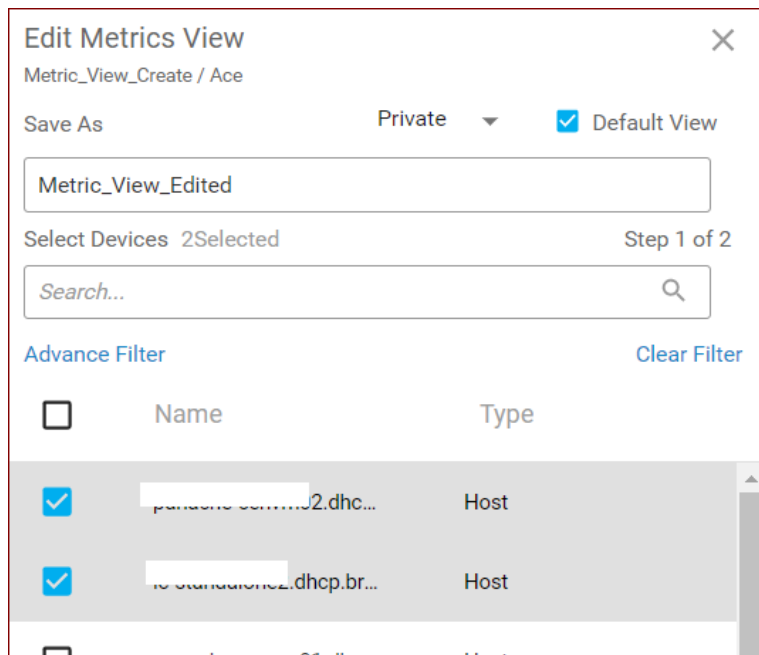
The device list is modified according to the applied filter. To clear the filter, click **Clear Filter**.

### **Edit Views**

If you want to edit the view after creating it, you can do so. You can edit only those views that you have created.

#### **Follow these steps:**

1. Access the required device or group.
2. Click the Metrics icon.
3. Select the view from the drop-down list.
4. Click the Edit View icon (  ) next to the metrics view drop-down list. The **Edit Metrics View** dialog opens.



5. Update the information as appropriate:

- Edit the view name.  
Update the name of the view.
- Change the access level.  
You can change the access level (Public, Private, or Account) of the view based on your requirements. You can change the access level of only those views that you have created. Select the required option.
- Change the default view.  
You can decide whether you want to make the current view as a default view or not. To make the current view as the default view, select the **Default View** option. If the option is already selected and you do not want that view as your default view, clear the selection.
- (For groups) Update the devices and metrics selection, as appropriate.  
You can select a different device and then the corresponding metrics for the device, if desired.
- (For devices) Update the metrics selection, as required.  
You can expand the metrics list and select a different metrics for the device, if desired.

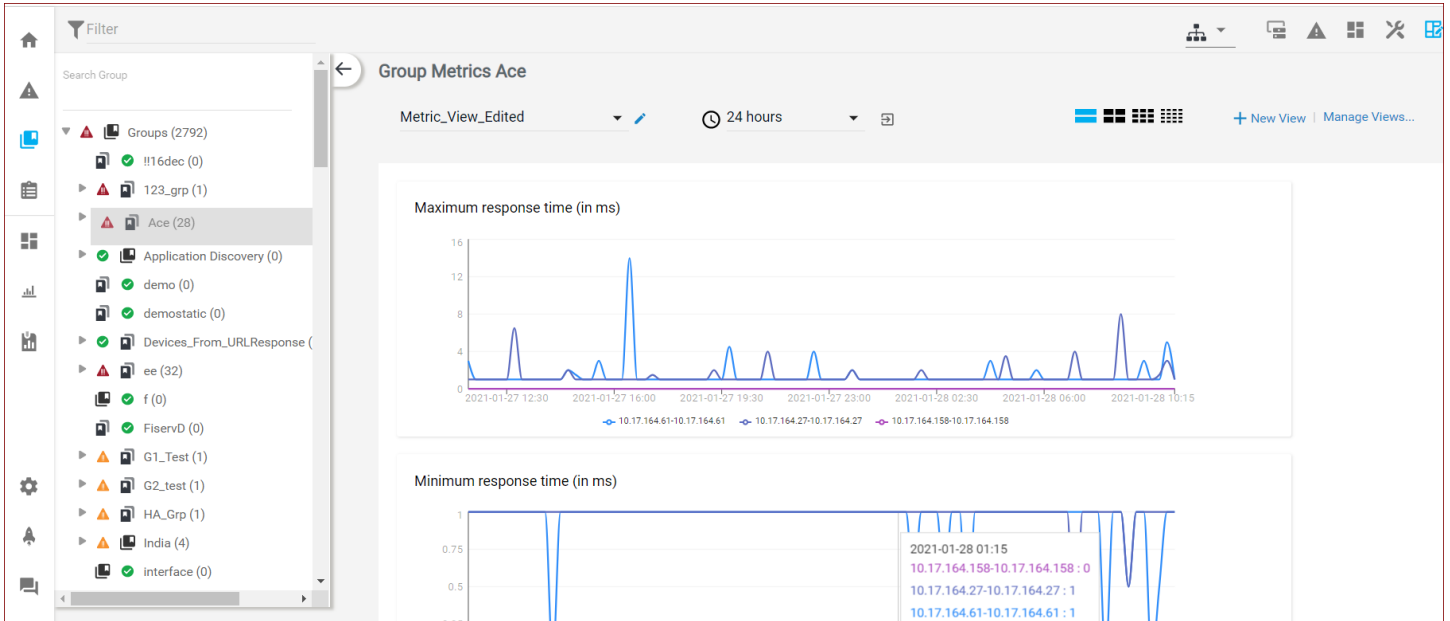
**NOTE**

Graphs can represent average metrics for multiple device components, such as multiple CPUs or disk drives in a single device. If a checkbox is not displayed for a metric, expand a metric to see its components. Select an individual component to display its metric graph.

6. Click the **Edit** button.

The information is saved and the view is updated accordingly. Graphs for the selected metrics are added at the bottom of the page. The following screenshot shows the updated view:



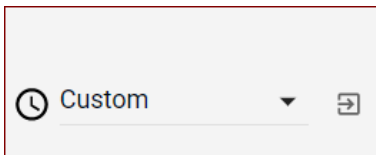


## Export Views

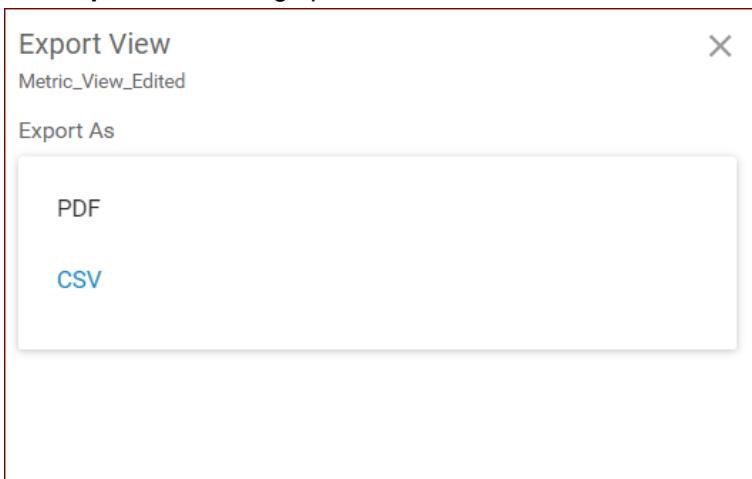
You can export the views as PDF or CSV. This provides an easy way to save and share the views.

### Follow these steps:

1. Navigate to the metrics view that you want to export.
2. Click the Export icon next to the duration drop-down list.



The **Export View** dialog opens.



3. From the **Export As** drop-down list, select the format (PDF or CSV) in which you want to export the view.
4. Click the **Export** button.

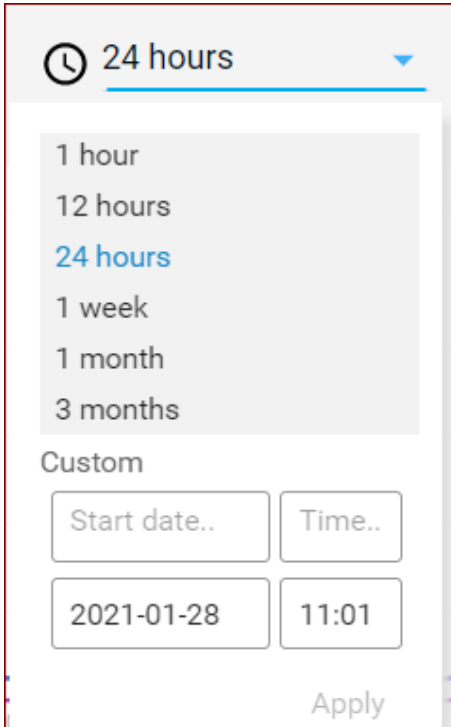
The view is exported successfully.

## Define Custom Time Range

If you do not want to use the predefined duration for your view, you can define your own duration using the custom time period option. This lets you view the historical metrics data based on your defined time range.

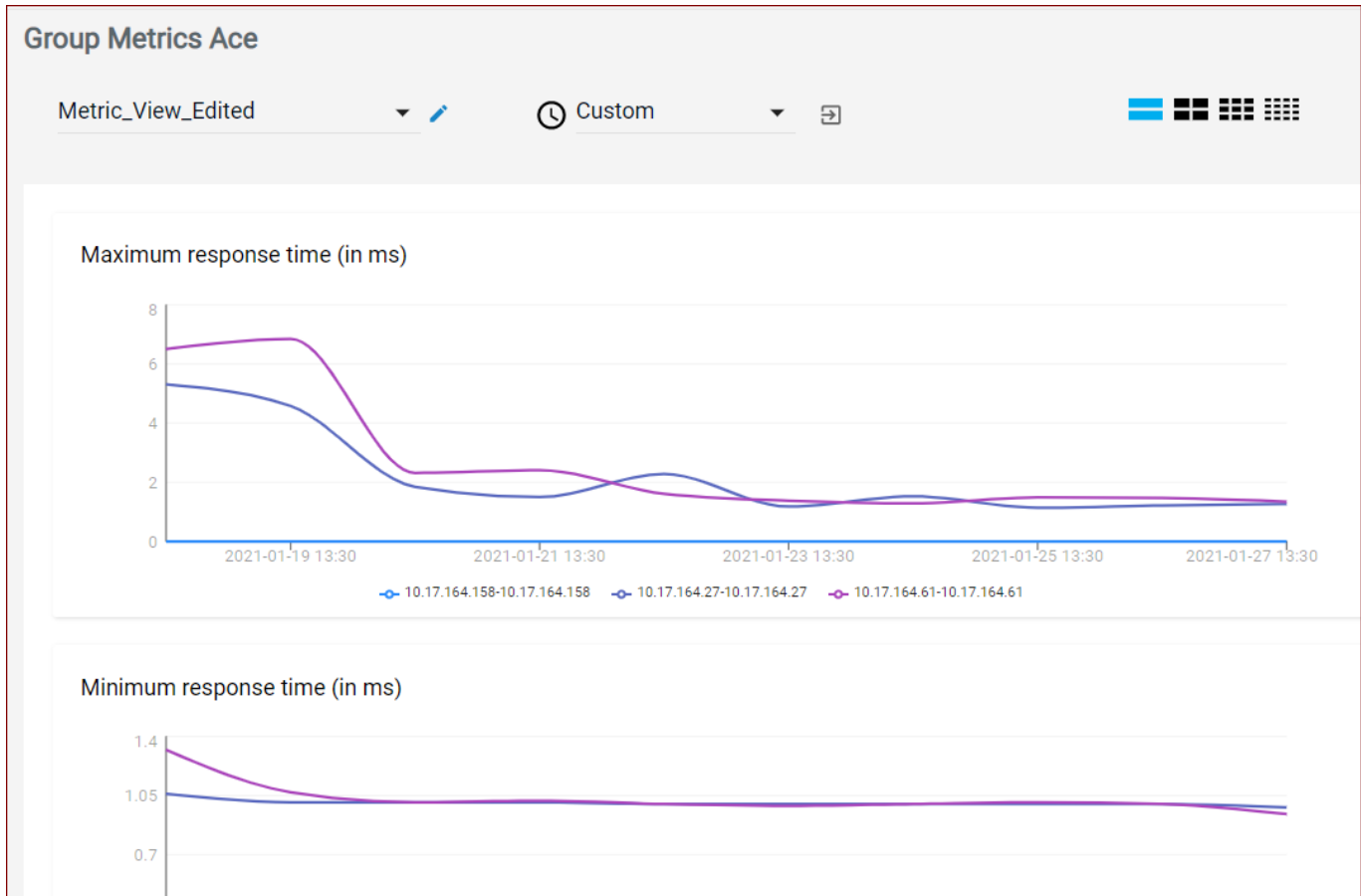
### Follow these steps:

1. Access the Metrics palette for the required view.
2. Click the duration drop-down list.
3. Specify the duration in the Custom section. You can define the custom duration for up to 12 months.



The screenshot shows a duration selection menu. At the top, there is a clock icon followed by "24 hours" and a downward arrow. Below this is a list of predefined durations: "1 hour", "12 hours", "24 hours" (highlighted in blue), "1 week", "1 month", and "3 months". Underneath the list is a "Custom" section. It contains two input fields: "Start date.." and "Time..". Below these fields are two text boxes containing the values "2021-01-28" and "11:01". At the bottom right of the custom section is an "Apply" button.

The historical metrics data for the defined duration is displayed.



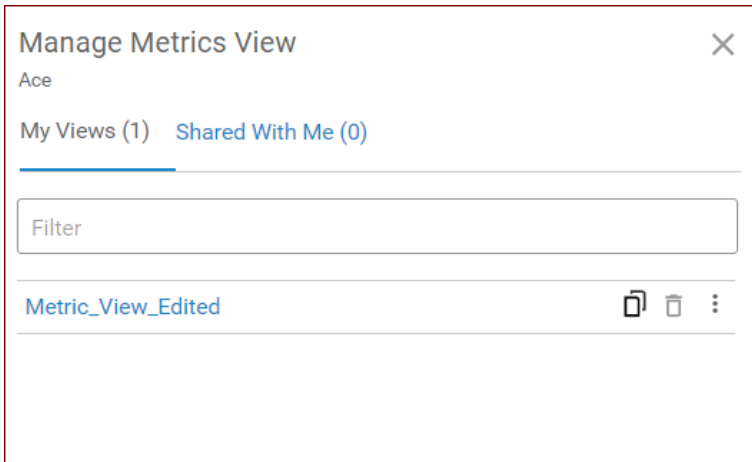
## Manage Views

The Manage Views link provides quick access to some of the actions; for example:

- Copy the view.
- Delete the non-default view.
- Change the default view.
- Change the access level of the view.

### **Follow these steps:**

1. Access the required device or group.
2. Click the Metrics icon.
3. Click the **Manage Views** option in the top-right corner.  
The **Manage Metrics View** dialog opens.



4. Locate the view that you want to update.
5. **Copy the view**  
You can make a copy of an existing view. This is useful if you want to create another view with the similar settings.
  - a. Click the copy icon, enter a name for the view, and click **Apply**. The view is created and is added to the metrics view drop-down list. You can edit the settings of the copy, if required.
6. **Delete the view**  
You can delete the views that you no longer need. You can delete only those views that you have defined. Once a view is deleted, it is removed for all the users.
  - a. Click the Delete icon (trash icon) to delete the view. The view is deleted and is removed from the metrics view drop-down list.
7. **Select or clear the default view**  
You can change the default view, if required.
  - a. Click the three-dot menu and select the **Default View** option if you want to make that view as the default view. If the option is already selected and you do not want that view as your default view, clear the selection.
  - b. Click **Apply**.
8. **Change the access level of the view**  
You can change the access level of the view, if required. You can change the access level of only those views that you have created.
  - a. Click the three-dot menu and select the **Private**, **Account**, or **Public** option.
  - b. Click **Apply**.
9. Review the updates.

The appropriate updates are done successfully.

## Manage Alarms with Centralized Alarm Policies

An alarm policy defines a set of metrics and alarm conditions in a centralized location, so that monitoring administrators can view and manage alarm reporting easily. Administrators can also create alarm policies in response to new conditions and needs. They can manage all aspects of alarm behavior in an alarm policy; for example, manage the alarm thresholds, timing, and messages configured for alarms. The Alarm Policies feature lets you perform the following actions:

- View a list of alarm policies.
- Add alarm policies.
- Add and delete conditions that trigger an alarm.
- Add alarm conditions to monitor individual devices, a group of devices, or a specific monitoring technology (such as Docker).
- Configure Time Over Threshold alarming to reduce alarm noise to an actionable level.
- Customize alarm messages to provide the information you need.

## Contents

### Prerequisites



The following are the prerequisites for creating an alarm policy:

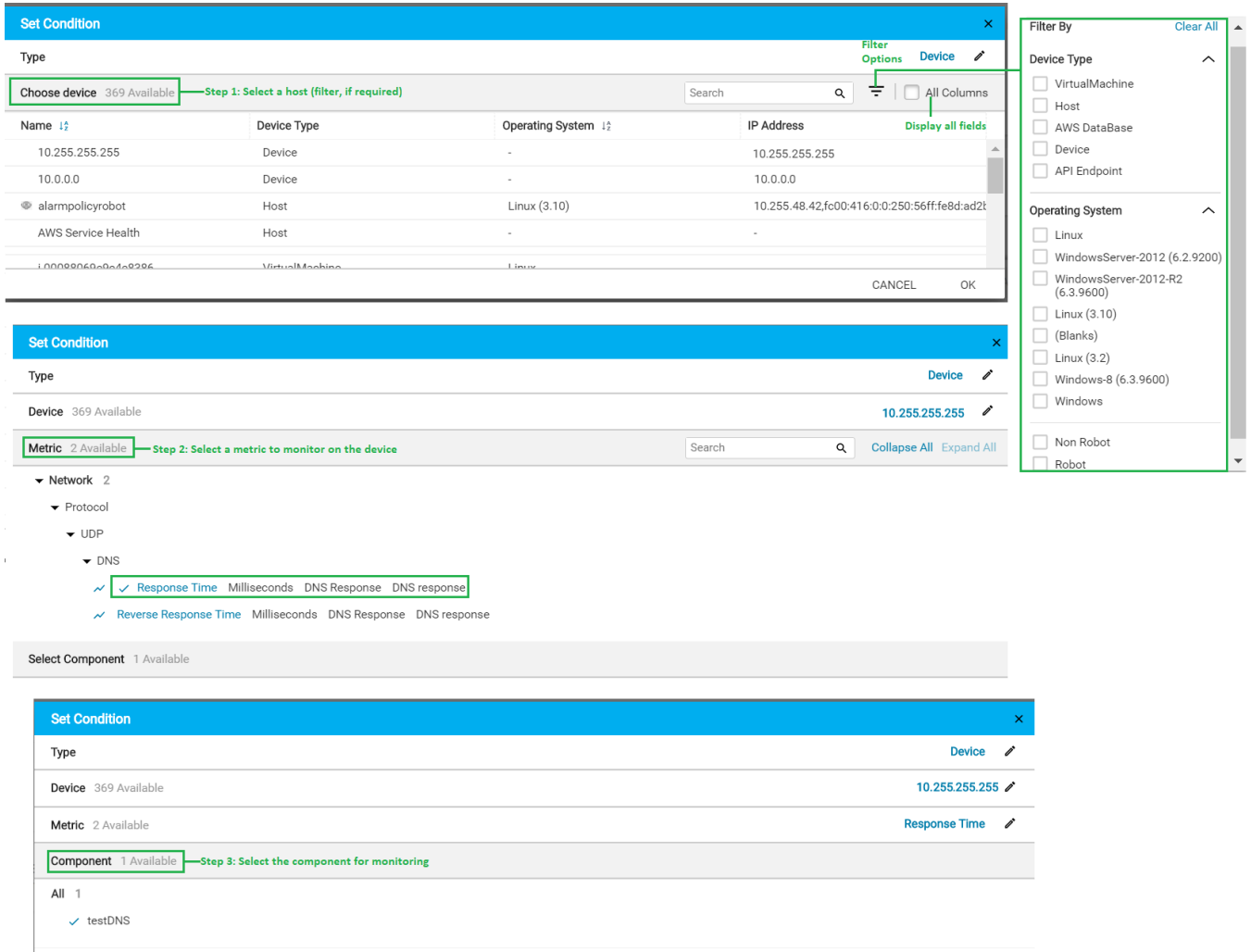
- Ensure that the robot version is 7.96 or later.
  - If your robot version is 9.31 or 9.31S, ensure that the MCS version is also 9.31. If this compatibility is not maintained, MCS profiles and alarm policies will not work.
- Ensure that the profile is an enhanced monitoring profile and it is collecting metrics.
- Ensure that Monitoring Configuration Service (MCS) is already configured.

### Create an Alarm Policy

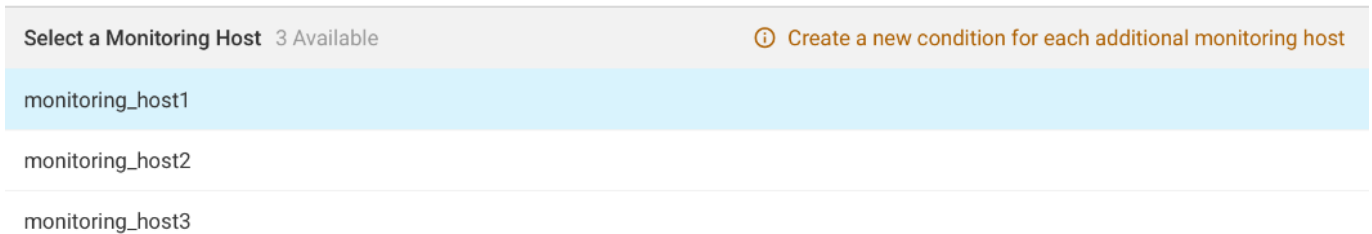
The complete process to create an alarm policy requires you to work in Operator Console. You create an enhanced profile in OC (with metrics collection enabled). Only when the metrics collection starts, you can create an alarm policy in Operator Console.

#### Follow these steps:

1. Log in to OC.
2. Create an enhanced monitoring profile with metrics collection enabled. The following screenshot shows an enhanced monitoring profile in OC
3. In Operator Console, click **Settings** in the left pane.
4. Click the **Alarm Policies** card.  
The **Alarm Policies** page opens.
5. Click the plus icon  at the bottom of the page.
6. Enter a policy name in the **Alarm policy name** field.  
Enter a policy name that helps you distinguish one policy from other policies. If you are creating an alarm policy for a device or group, you can include the device name or IP address or the group name. Include key words in the name to make it easier to search for a specific policy.
7. Click **Add condition** ().  
The **Set Condition** dialog opens. This dialog lets you define alarm conditions.  
An alarm condition defines what is monitored. You can set alarm conditions for a group (device and container), a specific device, or a monitoring technology.
8. Select the type of alarm condition on the **Set Condition** dialog:
  - **Device**  
Monitors the state or performance metrics for a device component.  
To configure an alarm condition for a device, select a device name, the metric, and the component that you want to monitor. The following example screenshot shows the settings for the Device type:



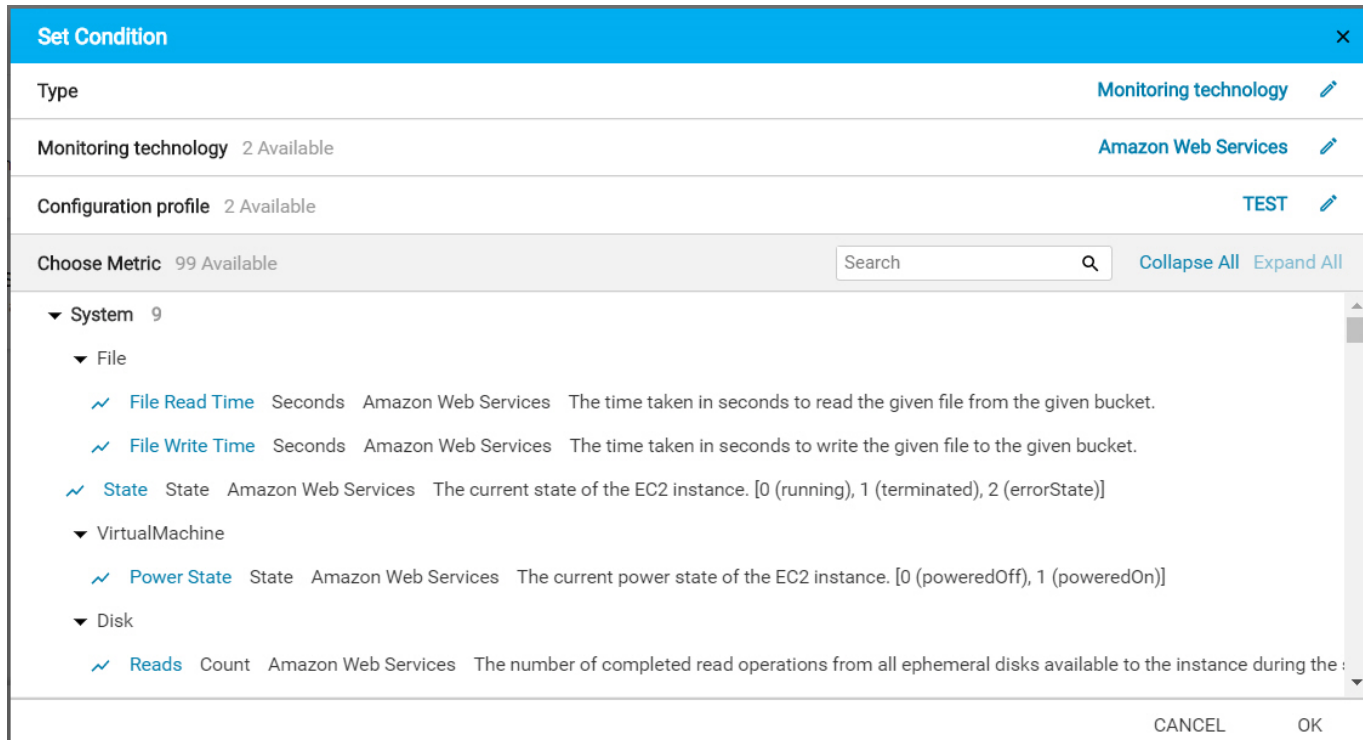
When there are multiple hosts that collect the same metric, the list of monitoring hosts also displays in the **Set Condition** page. You can select only one host at a time to create alarm condition. Create another condition to collect metric on the other host. The following example screenshot shows the **Select a Monitoring Host** section that appears when there are multiple hosts that collect the same metric:



– **Monitoring technology**

Monitors metrics associated with a specific monitoring technology.

To configure an alarm condition for a monitoring technology, select a monitoring technology, a configuration profile, and a metric. The following example screenshot shows the settings for the Monitoring Technology type:



## – Group

Monitors the state or performance metrics for a group (container or device). Add alarm conditions that apply to all devices in a group. Groups are displayed as a navigation tree; container groups followed by subgroups. Expand a container group to select a subgroup. When you create the condition at the container group, all subgroups (child container groups and device groups) in that container group inherit it. Support for container group is helpful in scenarios where you want a single threshold for each metric on a device. That threshold policy can be rolled down from the container group to the device group and then to the device.

### NOTE

To enable the alarm policy functionality for container groups, use the MCS raw configuration to set the value of the `enable_container_support_for_alarm_policy` parameter in the `timed` section to `true`. By default, the value is `false`.

To configure an alarm condition for a group, select the group name and the metric that you want to monitor on all devices in a group. You can also specify whether you want to generate alarms on all the components or for some specific components. By default, alarms are generated on all the components. To generate alarms on specific components, use a regular expression to filter the components. Select one of the following options depending on your requirements:

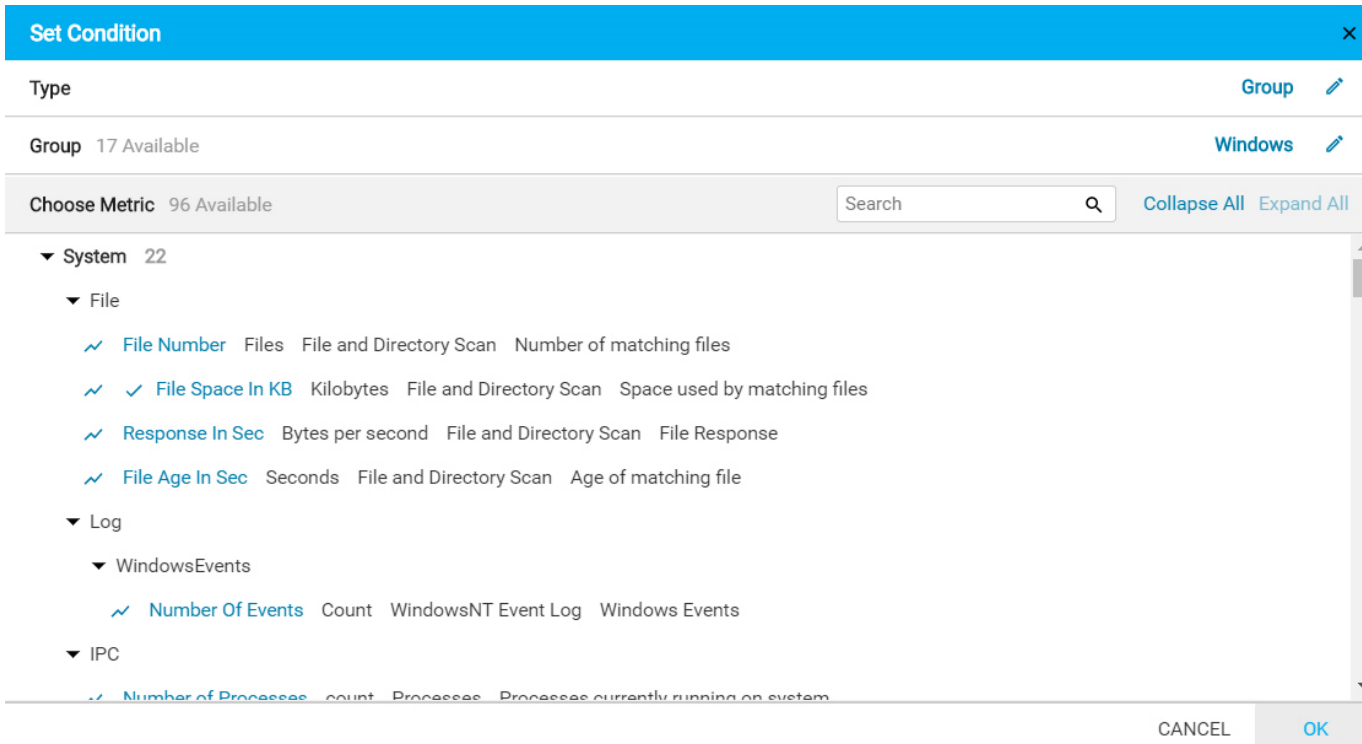
- **All Components**

Lets you generate alarms on all the components of all devices in a group.

- **RegEx**

Lets you filter the components based on a regular expression, which enables you to generate alarms only on the filtered components. Use meta characters such as `*` and `?` to construct a regular expression and pattern matching. RegEx supports regular expressions written in [PERL](#). For example, if you want to generate alarms on the CPU Usage of the CPUs—CPU-11, CPU-12, and CPU-13—of all the devices in a group, you can define the regular expression as: `CPU-1 [1-3]`. You can also use simple text with wild card operators for matching the target string. For example, the `CPU*` expression matches all the CPUs on the system (CPU-0, CPU-1 and so on till CPU-15). There are certain limitations on how you can define specific regular expressions.

The following screenshot shows settings for the Group type:



9. Click **OK** to save the condition information.
10. Specify an appropriate priority in the **Priority** field to evaluate the metric condition for the alarm policy at the group level. The condition that has the highest priority is used for generating alarms on the device. The range of the priority value is from 0 through 10000. You can specify the priority value only for the alarm policy at the group level, not at the device level or monitoring technology level. At the device level, the priority of the condition is set to the highest value and it takes precedence over other condition priorities for the same metric on that device. At the monitoring technology level, though the UI does not show the condition priority, CA UIM internally sets the value to 100, which cannot be changed. The default priority value is 100 at the group level and monitoring technology level. For more information about specific use cases, see the related section. The following screenshot shows the priority of a condition for a device-level alarm policy. Note that the priority is set to Highest and the value cannot be changed:

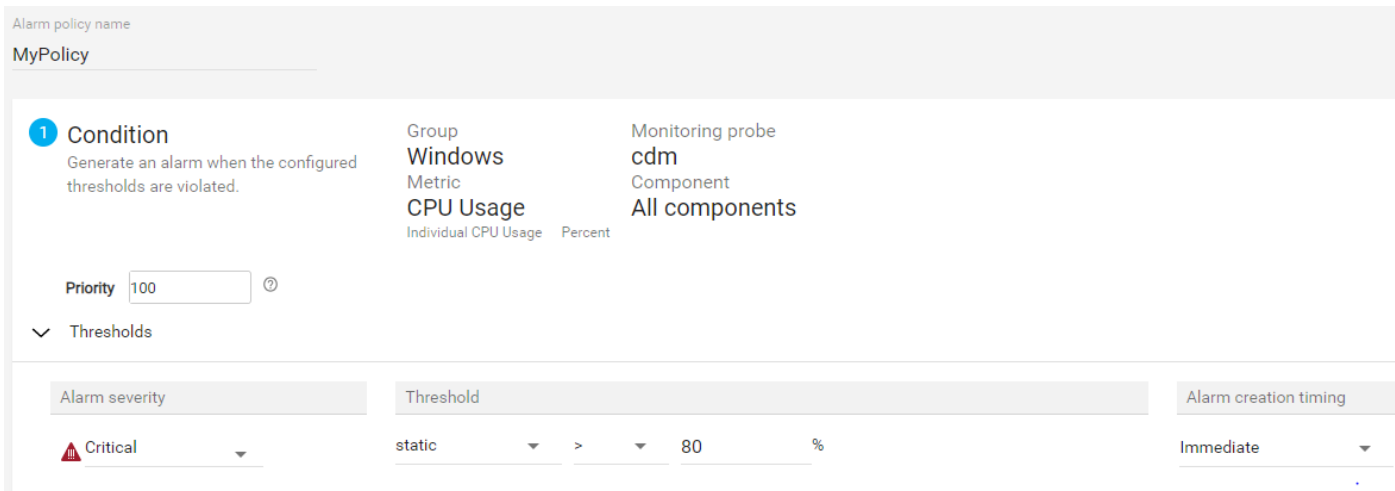


The following screenshot shows the priority of a condition for a group-level alarm policy. Note that the priority field shows the default priority of 100; you can change the value in this case:





- Set the alarm threshold by entering the alarm severity, threshold type (static or dynamic), operator, threshold value, and alarm timing (Immediate or Time over Threshold), as needed.  
 If you select *Time over threshold*, enter the number of minutes, hours, or days the metric needs to violate the threshold value. For example, when the *Time over threshold* is three hours in 4 hours, Infrastructure Management generates an alarm when there is a consecutive threshold violation for three hours within a four-hour time period.  
 The following screenshot shows the alarm condition with condition priority as 100 (default value), alarm severity as Critical, threshold type as static, operator as greater than, threshold value as 80, and alarm creation timing as Immediate:



- Click the arrow next to the **Alarm messages** section to review the default alarm messages. You can also customize the alarm messages to contain additional information.
- Click **Save** (in the lower right corner) to create an alarm policy with one or more alarm conditions.  
 This alarm policy generates alarms with the default alarm messages when the configured thresholds are violated.

The following example screenshot shows a created alarm policy:

| Monitor              | Alarm policy | Metric name(s)                                | Applies to...           | Creator                     |
|----------------------|--------------|-----------------------------------------------|-------------------------|-----------------------------|
| CPU, Disk and Memory | SamePriority | Processor Queue Length, Processor Queue Le... | ITPark-Amaravathi Group | administrator<br>12-26-2018 |

**NOTE**

When you create an enhanced profile in OC and the probe template includes default threshold values, then a default alarm policy is created in the Operator Console for this enhanced profile. The creator of the default alarm policy is displayed as *CA default policy* in the Operator Console. Additionally, when you convert your non-enhanced profile to an enhanced profile, a corresponding alarm policy is created in the Operator Console for the converted profile. Creation of this alarm policy adds threshold values that are present in the non-enhanced profile to the spooler metric ([plugin\\_metric](#)) section. The creator of this alarm policy is displayed as *CA profile migration* in the Operator Console.

**Export/Import Alarm Policies**

With UIM 20.3.0, the policy management API is enhanced to support export and import of alarm policies from one domain to another. To perform these operations, you must have the Policy Management ACL permission.

You can export the alarm policies based on the following:

- Alarm policy identifiers
- Group identifier
- Device identifier
- Technology – probe name

The supported export formats are XML and JSON.

To import alarm policies, map the groups, devices, and profiles to the GROUP, DEVICE, and TECHNOLOGY target types respectively.

Sample file format is as below:

```
[{ "sourcePolicyTargetId": 0, "sourcePolicyTargetType": "DEVICE", "targetPolicyTargetId": 0 }]
```

### **Newly Added APIs**

#### **POST /v0/policy/export**

Input parameters:

- **policyIds**
  - List of identifiers of the alarm policies to export.
- **groupId**
  - Identifier of the group to retrieve alarm policies.
- **deviceId**
  - Identifier of the device to retrieve alarm policies.
- **probe**
  - Technology to retrieve alarm policies.
- **policyFileType**
  - JSON(default), XML

Returns the XML/JSON alarm policies file to be imported.

The exported alarm policies can be downloaded in swagger by clicking on the link in the response body.

#### Response Body

[Download export?deviceId=1&policyFileType=JSON](#)

#### Response Code

200

#### **POST /v0/policy/import**

- **targetMappingFile**
  - Policy target map in JSON format that is used to map the device, group or technology in the source file and the corresponding attributes in the target environment while importing alarm policies.

Example:

```
[{ "sourcePolicyTargetId": 0, "sourcePolicyTargetType": "DEVICE", "targetPolicyTargetId": 0 }]
```

- **policiesFile**
  - File used to import alarm policy.

Returns the list of alarm policies imported.

## Policy Management in High Availability Mode

When the `policy_management_ws` probe is deployed on multiple wasp nodes, you must ensure that all probes do not start processing the policies. That is, there should always be only one processing node. You can do this by manually doing the configuration or by running the `policy_management_ws` probe in the High Availability (HA) mode. Perform the following configuration on the `adminconsoleapp` that is running on the primary hub (under the `<adminconsole>` tag).

Follow the below steps to run `policy_management_ws` probe in the High Availability (HA) mode:

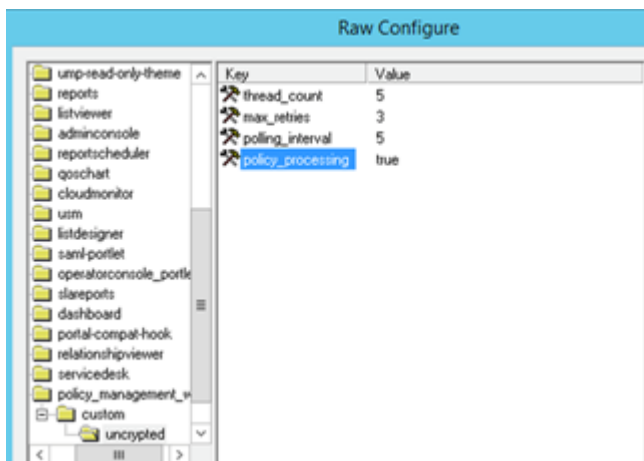
1. In `wasp.cfg`, go to the folder: `webapps/adminconsoleapp/custom/uncrypted`
2. Update the attribute `ha_mode`.  
Allowed values are: HA or MANUAL (default).
  - When set to HA, all the policy management nodes work in co-ordination with the `adminconsoleapp` running on the primary hub. The controller component running as part of `adminconsoleapp` controls which node to process and makes sure that only one node processes at a time.
  - When not set or set to MANUAL, all nodes read the `policy_processing` flag from `wasp.cfg` file of the respective node and process the policies if the value is set to true.
3. Update the additional attributes `heartbeat_interval_min` and `no_failed_attempts`.
  - `heartbeat_interval_min` : Defines the time interval that specifies how often the `policy_management_ws` nodes send the heartbeat to the controller running as part of `adminconsoleapp`. The default value is 5 minutes.
  - `no_failed_attempts` : Defines the number of failed attempts to send heartbeat before stopping the policy processing. The default value is 3. With the default configuration, the policy processing on a node stops in 15 minutes in case of communication issues between the controller and the node. After 20 minutes, a new node becomes the policy processing node.
4. Click Save.

## Manual Configuration

If `ha_mode` is configured to MANUAL, the policy management works in the manual mode. However, administrators can manually choose the failover node in case of any failure on the primary node.

### For enabling this option:

1. Deploy the `policy_management_ws` probe on all the OC servers and set “`policy_processing`” to true in one of the nodes (primary node) as shown in the following screenshot:



### NOTE

`policy_processing = true` is not present by default. You must add it to the `wasp.cfg` file on the OC server for which you want to process the alarm policies.

## Centralized Threshold Management for Technologies Monitored Remotely

(From UIM 20.3.1) The alarm policy functionality provides a centralized threshold management for technologies that are monitored remotely. For remote probes, alarm policies are not tied with the robot, which implies that the same policies are not applied to all the devices that a remote probe manages. This ability lets you define separate thresholds for different devices or groups that are monitored through the same remote probe.

Therefore, for devices or groups that a remote probe manages, alarm policies are now applied only to those devices for which they are created. This ensures that alarms are generated only for the relevant devices, allowing you to manage your policies and alarms in a more efficient manner.

### NOTE

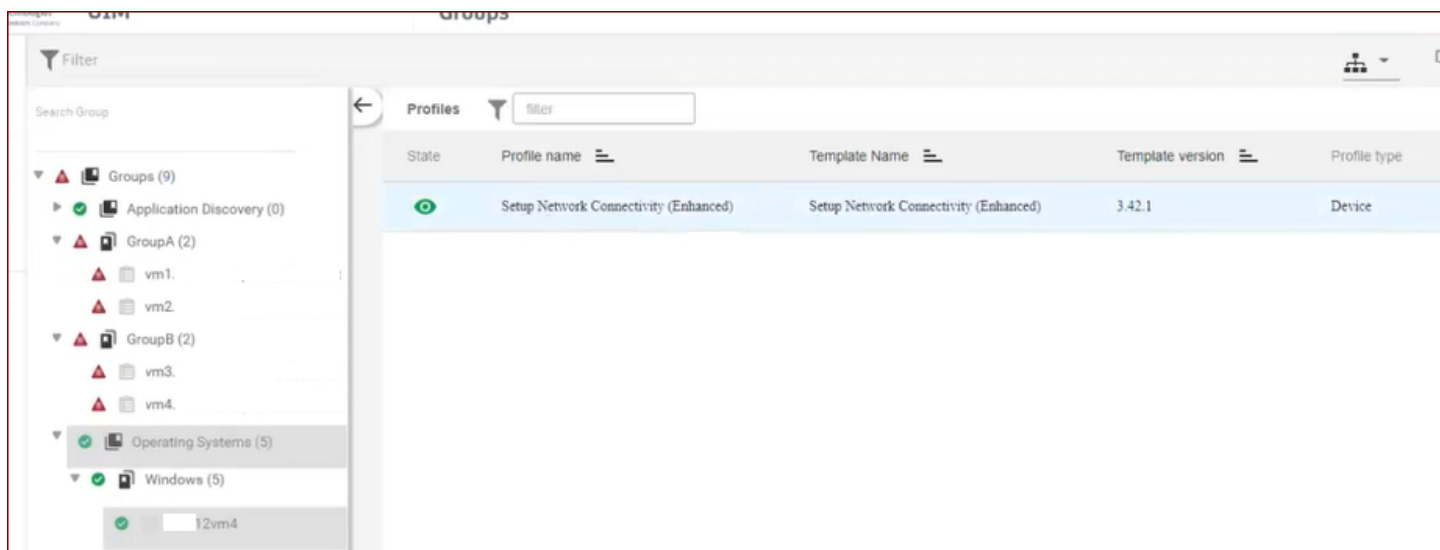
This functionality is applicable only for those remote policies that are created after you upgrade to UIM 20.3.1. Note that UIM 20.3.1 is a patch release. The UIM 20.3.1 patch does not include any upgrade installer for the UIM Server. The patch includes separate standalone artifacts that you can use to upgrade the respective components. For more information about the artifacts that are available as a part of the UIM 20.3.1 patch release, see the [UIM 20.3.1](#) article

Review the following example to understand how the enhanced functionality works.

### Example

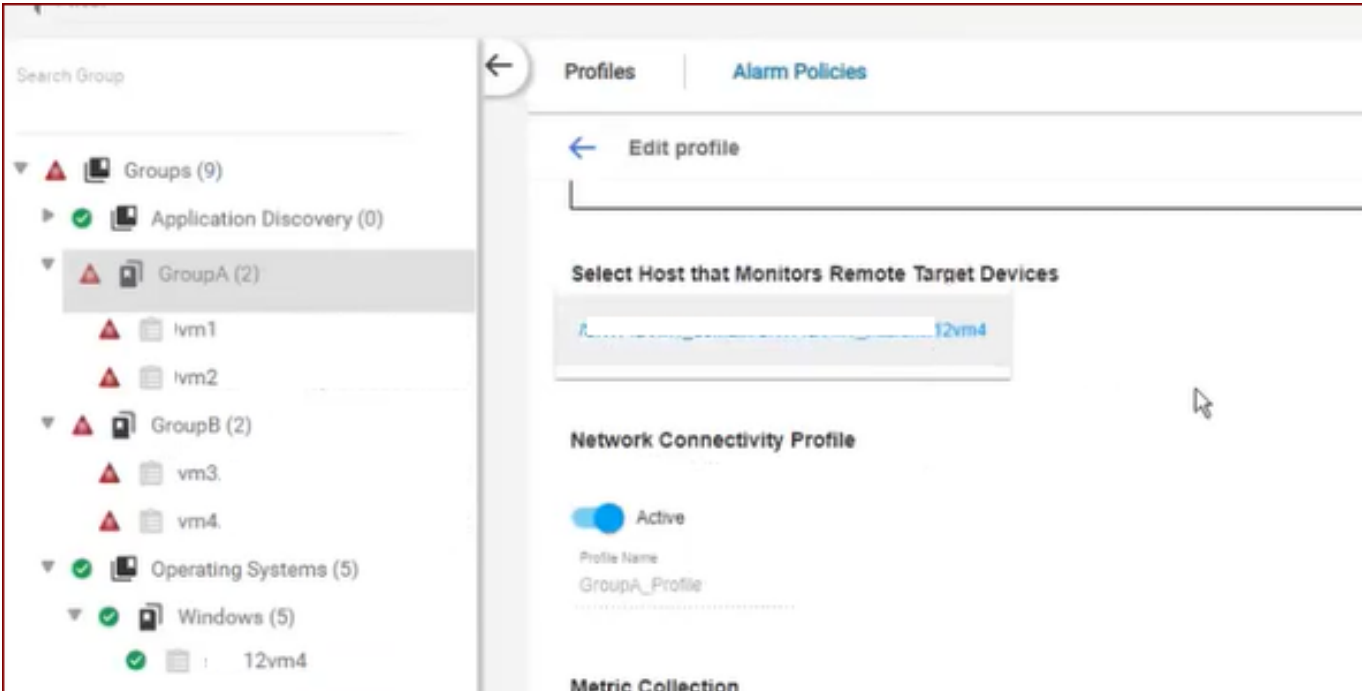
The example setup contains two groups: Group A and Group B. The first group includes two devices: vm1 and vm2. The second group also includes two devices: vm3 and vm4. The computer 12vm4 is acting as a monitoring host and is managing both the groups. The Network Connectivity MCS profile (net\_connect probe) is created on this monitoring host.

The following screenshot shows the target devices under Group A and Group B, monitoring host (12vm4), and the MCS profile:



GroupA\_Profile is the profile deployed on Group A (VM1 and VM2). This profile uses 12vm4 as its monitoring host in the profile configuration. Additionally, Ping Response Time is the metrics that this profile is supposed to collect. Similarly, Group B has the same configuration, where GroupB\_Profile is the profile with snw12vm4 as its monitoring host and Ping Response Time as the metrics.

The following screenshot shows the configuration for Group A:



The alarm policy GroupA\_AP is created on Group A, and the other alarm policy GroupB\_AP is created on Group B. The following screenshot shows the two alarm policies:

| Monitor                         | Alarm policy | Metric name(s) | Applies to... | Profile name | Creator                     |
|---------------------------------|--------------|----------------|---------------|--------------|-----------------------------|
| Network Connectivity (ICMP/TCP) | GroupB_AP    | Response Time  | GroupB Group  |              | administrator<br>10-27-2020 |
| Network Connectivity (ICMP/TCP) | GroupA_AP    | Response Time  | GroupA Group  |              | administrator<br>10-28-2020 |

Now, if you check the alarms, you find that the respective policies are creating alarms only on those devices on which they are created. The following screenshot shows that the GroupA\_AP policy is creating alarms on Group A (vm1 and vm2). Similarly, the GroupB\_AP is creating alarms on Group B (vm3 and vm4):

Filter
Results 0
Show Historical

Alarm By Severity

Alarm By Probes

Top Alarming

| Host           | Count |
|----------------|-------|
| 12vm4. ....net | 4     |

| Device Name    | Actions | Alarm Type | Owner      | Alarm Message                                               | Duration |
|----------------|---------|------------|------------|-------------------------------------------------------------|----------|
| 12vm4. ....net | ⋮       | Network    | Unassigned | GroupA_AP GroupA_Profile-vm1. ....net:ping - Ping Respon... | 2 hours  |
| 12vm4. ....net | ⋮       | Network    | Unassigned | GroupA_AP GroupA_Profile-vm2. ....net:ping - Ping Respon... | 2 hours  |
| 12vm4. ....net | ⋮       | Network    | Unassigned | GroupB_AP GroupB_Profile-vm3. ....net:ping - Ping Respon... | 16 hours |
| 12vm4. ....net | ⋮       | Network    | Unassigned | GroupB_AP GroupB_Profile-vm4. ....net:ping - Ping Respon... | 16 hours |




In this example scenario, prior to 20.3.1, the behavior was that if a policy was created on Group A, the same policy was getting applied to Group B devices also. Now, with this enhanced functionality, alarm policies are not applied to both the group devices; they are applied only to their associated group devices.

## FAQs

This section provides more information on some specific areas related to alarm policy.


### How do I create a new alarm policy in disabled state?

When you create an alarm policy in disabled state, the alarm policy is created successfully but it is not enforced by default. This ability gives you the option to evaluate your alarm policy before you enable it to receive alarms. **Follow these steps:**

1. Click **Settings** () .
2. Select the **Alarm Policies** card.  
A list of existing alarm policies appears.
3. Click the plus icon () at the bottom of the page.  
The new policy screen appears.
4. Enter a name in the **Alarm Policy Name** field.
5. Click **Add condition** () .
6. Select the type of alarm condition on the **Set conditions** dialog.
7. Select options that apply to the type of alarm condition.
8. Click **OK** to save the condition information.
9. Set the alarm threshold. Modify the alarm severity, threshold type (static or dynamic), and alarm timing, as needed.
10. Click the **Save and Disable** button.  
The alarm policy is created in the disabled state and the status tag for the newly created alarm policy displays **Disabled**, in the alarm policies page.

### How do I disable (or enable) an existing alarm policy?

If you want to disable (or enable) an existing alarm policy, you can do so. By disabling the existing alarm policy, you no longer receive any alarms for that policy. This allows you to temporarily disable the alarm policy without the need to delete it. And, when you want to receive alarms from the same disabled alarm policy, you can simply enable it. You are not required to create a new alarm policy. **Follow these steps:**

1. Click **Settings** () .
2. Select the **Alarm Policies** card.  
A list of existing alarm policies appears.
3. Click the required alarm policy.
4. Toggle the option in the lower left corner to **Disabled (or Enabled)**.  
The alarm policy is disabled (or enabled) and a relevant confirmation message is displayed. For example, the policy status displays the

**DISABLED**

tag

against the disabled alarm policy, when you look at the list of policies in the Alarm Policies page.  
The following screenshot shows an example where an existing alarm policy is disabled:

🔔 **Policy Disabled** | This policy has been disabled.

Alarm policy name  
**TLContainer**

---

**1 Condition**  
Generate an alarm when the configured thresholds are violated.

Priority  ?

^ Thresholds

Group  
**TL**

Metric  
**Processor Queue Length**

Processor Queue Length Processes

Monitoring probe  
**cdm**

Component  
**All components**

---

**2 Condition**  
Generate an alarm when the configured thresholds are violated.

Priority  ?

^ Thresholds

Group  
**TL**

Metric  
**Processor Queue Length**

Processor Queue Length Processes

Monitoring probe  
**cdm**

Component  
**All components**

DELETE

ENABLED

•


**NOTE**

Click the **Delete** button (in the lower left corner) to delete an existing alarm policy.

**How do I disable an alarm condition?**

You can disable a specific alarm condition in an alarm policy. In case of multiple conditions in an alarm policy, disabling one condition does not affect other existing conditions. Doing this will stop generating alarms for disabled alarm conditions from an alarm policy, while other alarms from conditions that are still enabled will continue to be generated. For example, you have created an alarm policy for a device that the File and Directory Scan (dirscan) probe monitors. For the same

metric, you have created two separate conditions with different threshold values. You now want to disable one of the conditions. **Follow these steps:**

1. Click **Settings** (  ).
2. Select the **Alarm Policies** card.  
A list of existing alarm policies appears.
3. Click the required alarm policy.
4. Scroll to the alarm condition that you want to disable.
5. Select the **Inline Menu**

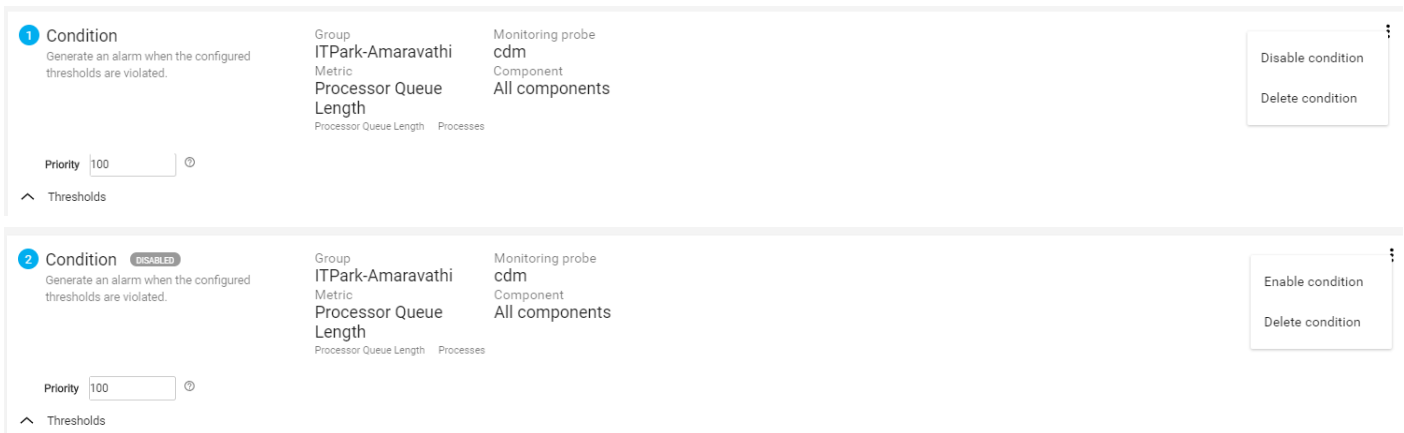


(  ) and then select **Disable condition**.

6. Select **Save**.  
The condition is disabled and alarms are no longer generated for the disabled alarm condition. The status of the condition

(  )

is displayed next to it. The following screenshot shows an example:



**NOTE**

To enable the condition, select **Enable condition**, and click **Save**. The status of the condition is changed and the Disabled tag no longer appears.

**What are the limitations for regular expressions usage?**

The following regular expressions cannot filter components for a group:

- Incorrect regular expression: CPU-(0|1) Workaround:  
Use the regular expression: CPU-[0-1]  
Matches the components: CPU-0 and CPU-1
- Incorrect regular expression: CPU.11  
Workaround:  
Use the regular expression: /CPU.11/  
Matches the component: CPU-11
- Incorrect regular expression: total/i  
Workaround:  
Use the regular expression: /[tT][oO][tT][aA][lL]/  
Matches all occurrences of the string total irrespective of the case. That is, the expression matches total , Total , toTal , TotAl ,TOTAL , and so on.



The following regular expression has limitations on how it searches for the components:

- `tmp1|tmp2` : Matches all the directories starting with `tmp1` ( such as `tmp1` , `tmp11` , `tmp14` , `tmp156` , `tmp1.x` ) and only `tmp 2` .

### **Which configuration file includes alarm policy-related information?**

When an alarm policy is created, all alarm policy-related information is written in the `plugin_metric` configuration file ( `.. \Nimsoft\plugins\plugin_metric\plugin_metric.cfg` ). MCS deploys the alarm policy to spooler. Spooler reads the configuration and generates alarms based on the condition. `plugin_metric.cfg` is the central place for all the alarm policies related to all the probes of a robot. The following `plugin_metric.cfg` snippet shows the information about an alarm policy for the `dirscan` probe:

```

plugin_metric.cfg
1 <spooler-metrics>
2 <policy_27>
3 <dirscan>
4 <metric_1078>
5 metric_type_id = 1.10:1
6 policy_id = 27
7 publish_baseline = false
8 qos_name = QOS_DIR_NUMBER
9 alarm = true
10 qos_source = ~.*
11 publish_qos = true
12 metric_precedence = 0
13 qos_target = ~.*
14 <alarms>
15 <threshold_1108>
16 tot_slider_units = _ hours
17 threshold = 1.0
18 custom_message = Demo_Alarm.#{metric_name}
19 thresh_type = static
20 operator = G
21 ttt = false
22 tot = false
23 severity = 5
24 custom_clear_message =
25 tot_time_frame_units = hours
26 </threshold_1108>
27 </alarms>
28 </metric_1078>
29 </dirscan>
30 </policy_27>

```

Alarm policy logs are available under `.. \Nimsoft\probes\service\wasp` . The name of the log file is `policy_management.log` .

### **How do I correct the plugin\_metric file?**

When you create an alarm policy or an enhanced profile, its configuration information is written in the `plugin_metric` file. In robot versions prior to the secure versions, sometimes, this information is not written properly in the `plugin_metric` file. For example, you create an alarm policy, but that alarm policy configuration is not deployed properly. In this case, the

corresponding information is not updated correctly in the `plugin_metric` file and this creates issues. Similarly, when you delete a child profile from the OC UI, the same information is not deleted from the `plugin_metric` file. This issue has been fixed in the robot version released after CA UIM 9.2.0 releases. To resolve such issues in your environment, you can use the `plugin_metric_correction` callback that is available for the `mon_config_service` probe. This callback re-deploys enhanced profiles and alarm policies based on your input.

#### Follow these steps:

1. Ensure that you do not create any MCS profiles or alarm policies when you are performing this operation.
2. (Optional) Open the `mon_config_service` raw configuration and increase the thread count to 10 in the `timed` section for each parameter:
  - `device_processing_threads`
  - `config_deployment_threads`

We recommend that you increase the thread count so that the process completes quickly. After you complete the process, change the settings back to the original values.
3. Access the probe utility (pu) for the `mon_config_service` probe.
4. Locate and select the `plugin_metric_correction` callback from the drop-down list.
5. Enter the appropriate information for the following parameters, as required:
  - `process_all_devices_flag`  
Enter the value as true if you want to re-deploy enhanced profiles or alarm policies on all the devices. If you select this parameter, all the remaining parameters are not required.
  - `robot_names`  
Enter the specific robot name on which you want to re-deploy the enhanced profiles or alarm policies. If you want to use more than one entry, enter a comma-separated list.
  - `computer_system_ids`  
Enter the specific computer system ID (`cs_id`) on which you want to re-deploy the enhanced profiles or alarm policies. If you want to use more than one entry, enter a comma-separated list.
  - `cm_group_ids`  
Enter the specific group ID on which you want to re-deploy the enhanced profiles or alarm policies. All the devices that are part of that group are considered for re-deployment. If you want to use more than one entry, enter a comma-separated list.

**Note:** You can use any combination of `robot_names`, `computer_system_ids`, and `cm_group_ids`.
6. Run the callback.  
A message appears in the right pane stating that the process has started for the devices. However, note that no completion message is displayed. The process completes all related tasks in the background. If you want to check the status, you need to verify the database.
7. Verify the status by running the following queries:
  - `select * from ssrv2policytargetstatus where cs_id in (<ID>);`
  - `select * from ssrv2profile where cs_id in (<ID>);`

The status OK means that the re-deployment has occurred without any issue.
8. Similarly, to find whether any error has occurred, run the following query:
  - `select * from ssrv2audittrail where userid like 'plugin_correction%';`

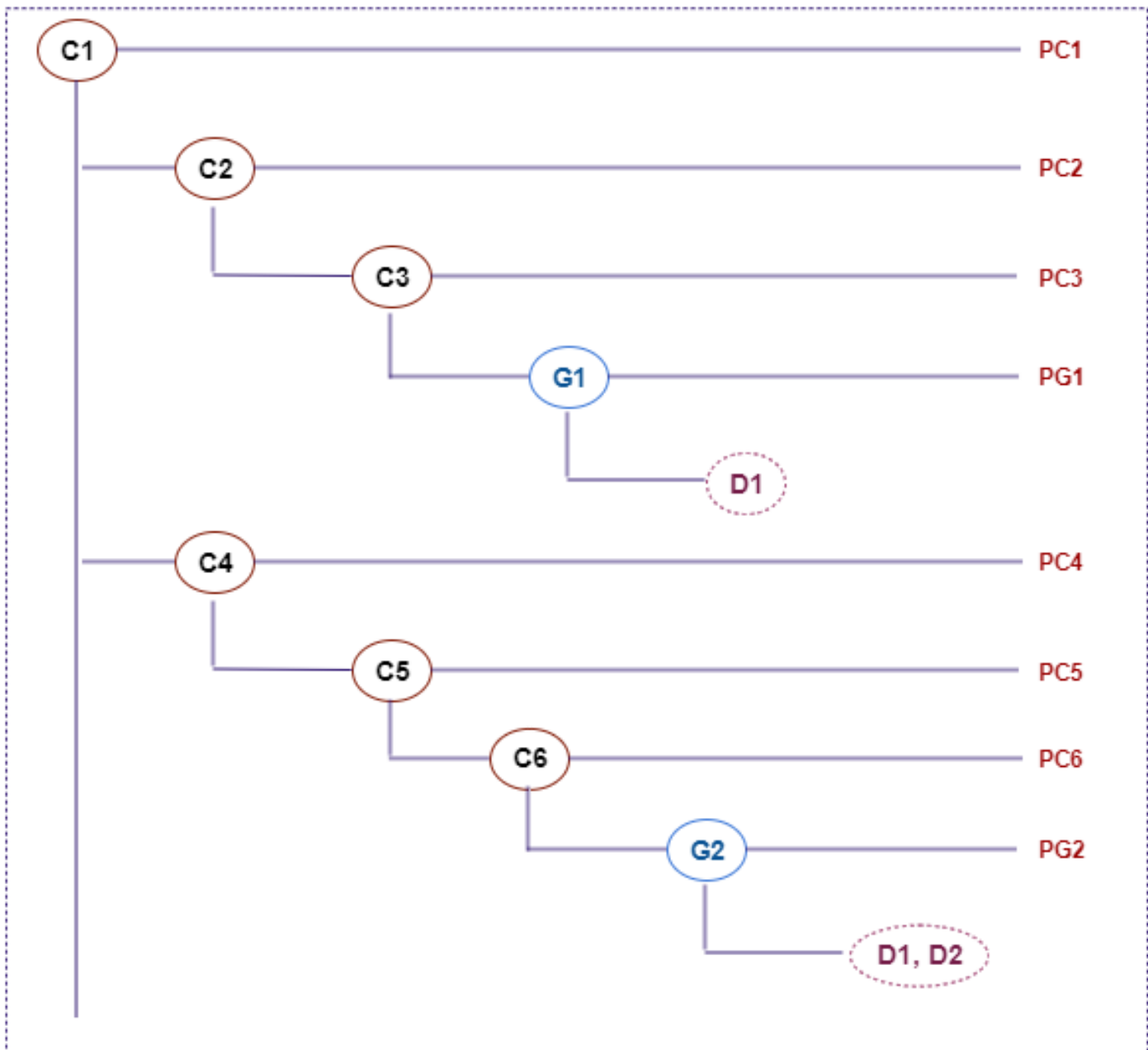
From the result of this query, note down the object IDs (failed computer system IDs), review the error messages, resolve them, and then again run the callback for these failed devices.

You have successfully repaired the `plugin_metric` file.

#### **What are the *condition priority*-related scenarios for alarm policies?**

Consider the following sample hierarchy to understand various scenarios:

Figure 24: Priority Condition for Alarm Policy



- This sample hierarchy includes a root container group (C1).
- The root container group includes child container groups (C2, C3, C4, C5, and C6).
- Two child container groups (C3 and C6) contain device groups (G1 in C3 and G2 in C6).
- These device groups include certain devices (D1 in G1 and D1, D2 in G2). The device D1 is part of the two device groups G1 and G2.
- An alarm policy condition (PC1, PC2, PC3, PG1, PC4, PC5, PC6, and PG2) is created for each group. The alarm policy conditions PG1 and PG2 are for device groups; all other alarm policy conditions are for container groups.

For applying alarm policies to the device D1 in context of the above hierarchy, the following use cases are applicable:

**Use Case 1: Alarm policy with the condition having the same metric and the same priority** If a device is part of multiple groups where conditions have the same metric and the same priority, then all the conditions are applied to the device. For example, if the metrics and priorities are as follows, then all alarm policy conditions PC1, PC2, PC3, PG1, PC4, PC5, PC6, and PG2 are applied and corresponding alarms are generated. In this example, the metric M1 is present in all conditions, and all conditions have the same priority of 100. Therefore, eight alarms are generated in this case.

- **PC1**  
Metric: M1, Priority: 100
- **PC2**  
Metric: M1, Priority: 100
- **PC3**  
Metric: M1, Priority: 100
- **PG1**  
Metric: M1, Priority: 100
- **PC4**  
Metric: M1, Priority: 100
- **PC5**  
Metric: M1, Priority: 100
- **PC6**  
Metric: M1, Priority: 100
- **PG2**  
Metric: M1, Priority: 100

**Use Case 2: Alarm policy with the condition having the same metric and different priorities** If a device is part of multiple groups where conditions have the same metric and different priorities, then the highest priority is taken into consideration to decide which alarm is generated. CA UIM verifies whether all the conditions for the device contain different priorities for the same metric. If so, the highest priority is taken into consideration. For example, if the metrics and priorities are as follows, then PC2 and PC4 have the highest priority of 200 for the same metric M1. In this case, only two alarms are generated for these conditions (PC2 and PC4), because they have the highest priority out of all other conditions:

- **PC1**  
Metric: M1, Priority: 100
- **PC2**  
Metric: M1, Priority: 200
- **PC3**  
Metric: M1, Priority: 100
- **PG1**  
Metric: M1, Priority: 100
- **PC4**  
Metric: M1, Priority: 200
- **PC5**  
Metric: M1, Priority: 100
- **PC6**  
Metric: M1, Priority: 100
- **PG2**  
Metric: M1, Priority: 100

**Use Case 3: Alarm policy with the condition having multiple metrics and the same priority** If a device is part of multiple groups where conditions have multiple metrics and the same priority, then all the metrics will be applied to the device. For example, if the metrics and priorities are as follows, then two alarms are generated for the metric M1, two for M2, one for M3, one for M4, one for M5, and one for M6:

- **PC1**  
Metric: M1, Priority: 100
- **PC2**  
Metric: M1, Priority: 100
- **PC3**  
Metric: M2, Priority: 100
- **PG1**  
Metric: M3, Priority: 100
- **PC4**  
Metric: M4, Priority: 100
- **PC5**  
Metric: M5, Priority: 100
- **PC6**  
Metric: M6, Priority: 100
- **PG2**  
Metric: M2, Priority: 100

**Use Case 4: Alarm policy with the condition having multiple metrics and different priorities** If a device is part of multiple groups where conditions have multiple metrics and different priorities, then the highest priority is taken into consideration and the corresponding metrics is applied. For example, if the metrics and priorities are as follows, then two alarms are generated for the metric M1 because PC2 and PC4 have the highest priority (200):

- **PC1**  
Metric: M1, Priority: 100
- **PC2**  
Metric: M1, Priority: 200
- **PC3**  
Metric: M2, Priority: 100
- **PG1**  
Metric: M5, Priority: 100
- **PC4**  
Metric: M1, Priority: 200
- **PC5**  
Metric: M1, Priority: 100
- **PC6**  
Metric: M3, Priority: 100
- **PG2**  
Metric: M2, Priority: 100


**Upgrade/Migrate Scenarios** While upgrading/migrating from a previous version to 9.2.0, the following scenarios are considered:

- When you upgrade an existing alarm policy (created in 9.0.2) to 9.2.0, the priority of the condition for the upgraded alarm policy is set to 100 at the group level and monitoring technology level and to the highest value at the device level. The behavior of the upgraded alarm policy is the same as explained in the above-mentioned use cases (Use Case 1, Use Case 2, Use Case 3, and Use Case 4).
- When you migrate a device-level legacy profile to an enhanced profile, the priority of the condition for the device-level alarm policy always gets the highest priority.
- When you migrate a group-level legacy profile to an enhanced profile, the priority of the condition for the group-level alarm policy takes the same priority as that of the profile.

**Additional Considerations** Review the following considerations:


- The `metric_precedence` parameter in the `plugin_metric.cfg` file is updated with the condition priority.
- When a new container is added to the hierarchy or an existing one is deleted from the hierarchy, the alarm policy is applied based on the new hierarchy. And, if the condition priority is the same, all the alarm policies in the hierarchy are applied to the device.
- When an alarm policy is deleted from the hierarchy, all related entries are removed from the database and the `plugin_metric.cfg` file.
- For two different alarm policy conditions for the same device and the same metric, alarms are generated from both the conditions as the priority remains the same for both of them.
- If an alarm policy has multiple conditions and you make any update to the alarm policy, the priority of the conditions change accordingly.

### **How do I determine if an alarm policy needs to be updated?**

You should observe the existing alarms in the **Alarms** () view. There may be too many alarms that are generated for a metric, the performance levels you want to monitor are outside the industry norm, or you want to differentiate monitoring for regional and global locations to account for localized issues. Once you develop a monitoring strategy, you can change alarm behavior by opening the alarm policy that generates the alarms and updating, adding, or deleting the alarm thresholds. See the next topic for information about accessing a specific alarm policy.

### **How do I access alarm policies?**

**Follow these steps:**

1. Click **Settings** () .
2. Select the **Alarm Policies** card.  
A list of existing alarm policies appears.
3. From the **Alarm Policies** view, click a policy name to view the configuration. Use the "Custom filter" field to quickly search for a specific policy. Click the column headings to sort policies alphabetically by technology, policy name, or creator.

The following information is provided in the policy list to help you locate a specific alarm policy.

- **Monitor** - Displays the monitoring technology for an alarm policy.
- **Alarm policy** - Provides the policy name and the metrics that are configured in the policy.  
The alarm policy name is either the name of the monitoring profile from which the alarm policy was generated, or the name you entered when you created the policy. Mouse over the metrics under the policy name to see a complete list of metrics configured in the policy.
- **Applies to** - Shows the device, group, component, combination of components monitored by a policy, and the type of target being monitored.
- **Creator** - Displays the username who created an alarm policy, *or CA default policy* appears if Infrastructure Management generated the alarm policy automatically. The date reflects the policy creation date or the date the policy was last updated.

### **Can I create several alarm conditions for the same metric?**

You can configure several alarm conditions from the same metric. In the same alarm policy, you could configure the same alarm condition for the same metric, but apply the metric thresholds to different groups. This provides consistent monitoring across the devices in various groups. **Example:** A monitoring administrator monitors Windows devices for the San Francisco, Chicago, and Boston business units. The Windows devices are grouped by business unit. Because alarm policies can contain alarm threshold configuration for more than one device, group, or technology, the monitoring administrator creates a single alarm policy to apply to the devices in the three business units individually. One way to

configure the alarm policy is to create an alarm condition for each group, and each metric to be monitored. The following table shows an alarm condition created for the Boston and Chicago groups:

| Condition                                                      | Group   | Metric  | Monitoring probe | Component      | Priority | Thresholds                                    |
|----------------------------------------------------------------|---------|---------|------------------|----------------|----------|-----------------------------------------------|
| Generate an alarm when the configured thresholds are violated. | Boston  | Up time | cdm              | All components | 100      | Critical, static, greater than, 80, Immediate |
| Generate an alarm when the configured thresholds are violated. | Chicago | Up time | cdm              | All components | 100      | Critical, static, greater than, 80, Immediate |

### **Why would I change alarm thresholds?**

Configured alarm thresholds are carried over from a monitoring profile during the one-time alarm policy generation process. You might want to change the threshold settings for the following reasons:

- The alarm severity is too high or low.
- Instead of receiving persistent (*immediate*) alarms, you want to receive alarms only after successive alarm threshold violations have occurred within a configured window of time (*Time over threshold*).
- You want different performance thresholds for regional groups of computers, or for older versus new devices and servers.

### **How do I modify, add, or delete alarm thresholds?**

Generated alarm policies provide alarms based on predefined, best practices monitoring. Update the threshold settings to reflect your monitoring needs. **Follow these steps:**

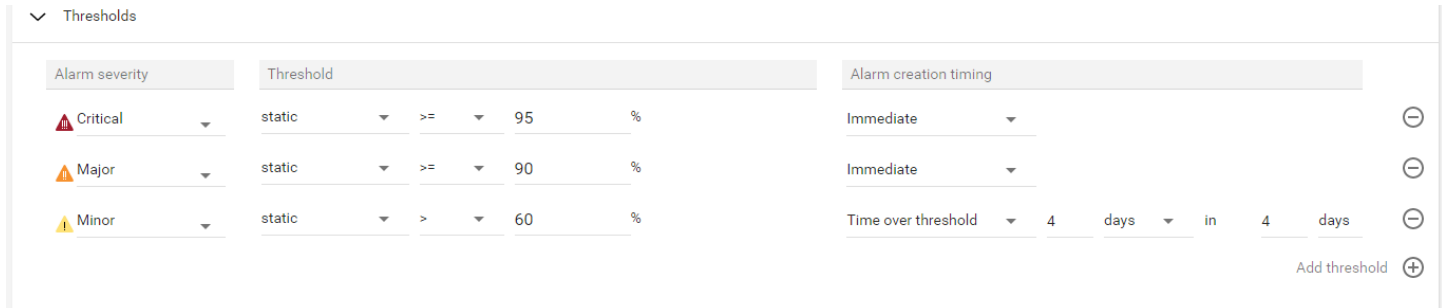
1. In an alarm policy, scroll to the desired alarm condition.
2. Click **Expand** (v) to view the configured thresholds.
3. Modify the configured alarm severity, threshold type (static or dynamic), operator, or threshold value as needed.
4. Modify the configured alarm creation timing.  
If you select *Time over threshold*, enter the number of minutes, hours, or days the metric needs to violate the threshold value. Next, enter the number of minutes, hours, or days to specify the total window of time. For example, when the *Time over threshold* is three hours in 4 hours, Infrastructure Management generates an alarm when there is a consecutive threshold violation for three hours within a four-hour time period.
5. Click **Add** (+) or **Delete** (-) to add or delete thresholds for a metric.
6. Click **Save** (lower right corner) to save your change to the alarm policy.  
**Note:** You cannot save updates to an alarm policy until you have entered the required information for each threshold configured in an alarm condition.  
If you delete a threshold, alarms that were previously generated remain in the system until the close alarm rule time frame is reached.

### **Can I configure more than one threshold for a metric?**

You can configure more than one threshold for a metric to track different severities. The following scenario describes a case in which several thresholds for a metric alerts an administrator to perform different actions to address performance issues. **Use Case** To help you keep track of the user experience or determine when to upgrade equipment, you could configure different thresholds for CPU Usage. For example, you could configure the following three thresholds to generate alarms for different purposes:

- To help you determine when equipment should be updated or replaced, configure a threshold that generates a critical alarm when CPU usage is at 95 percent for 24 hours within a 36-hour window (time over threshold alarming).
- Configure a second threshold to generate a major alarm any time CPU usage exceeds 90 percent (immediate alarm). This alarm could help you track processing jobs that should be scheduled to run after hours.
- Generate a minor alarm when CPU usage is greater than 60 percent for 4 days within a 5-day window of time (time over threshold alarming). This alarm would let you know that users are experiencing data processing delays.

The following screenshot shows several thresholds that are configured for a single metric.



### How do I edit an alarm condition?

For any alarm condition, you can modify what is being monitored, the selected metric, and the threshold. You can also monitor the same metric for a device or group, or configure an alarm condition for a technology. When you configure alarm conditions for a technology, the alarm condition is applied to any device with that technology in your environment. **Follow these steps:**

1. Within an alarm policy, scroll to the **Condition** that you want to change.
2. Click **Edit**.
3. Modify any option on the **Set condition** dialog.
  - a. Expand (v) Type, Device, Metric, Component, Monitoring technology, or Group.
  - b. Select the desired setting.
  - c. If you change the type of condition, ensure that all the options are configured.
  - d. Click **OK** to save your updates.
4. Expand (v) **Thresholds**.
5. Modify existing alarm thresholds, if needed.
6. Click **Add threshold** (+) to configure another threshold.
  - a. Select an alarm severity, the type of threshold, an operator, and enter a threshold value.
  - b. Next, select the timing for an alarm.
7. Click **Remove threshold** (−) to delete a configured threshold.
8. **Save** (lower right corner) the updates to the alarm policy.

### How do I delete an alarm condition?

When you delete an alarm condition from a policy, alarms are no longer generated for the metric. If the metric is enabled, CA UIM continues to generate metric data. CA UIM saves the alarm history for the configured period of time.

**Follow these steps:**

1. Scroll to the alarm condition you want to delete.



## 2. Click the **Inline Menu**



and then select **Delete condition**.

Alarms are no longer generated for the deleted alarm condition.

## **How do I customize alarm messages?**

Each alarm policy can have up to three predefined alarm messages: a general message, a Time Over Threshold message, and a close alarm message. These predefined messages provide sufficient information to help you troubleshoot an issue. However, you can customize the alarm messages to contain additional information. For each type of predefined message, there is a list of [supported variables](#) that you can use in a message to indicate the exact device and threshold violation details. A general and close alarm message appears for each alarm policy. The Time over Threshold violation alarm message appears after a Time over Threshold alarm is configured. The default alarm violation messages and variables are:

- **Immediate threshold violation message**

```
 ${metric_name} on ${component_name} for ${device_name} is at ${metric_value} ${metric_unit}.
```

Example: CPU monitor on C:/ for test\_system is at 90percent.

- **Time over Threshold violation message**

```
 ${metric_name} on ${component_name} for ${device_name} is at ${metric_value} ${metric_unit}. It
 has violated the threshold for at least ${tot_slider} ${tot_slider_unit} out of ${tot_time_frame}
 ${tot_time_frame_unit}.
```

Example: CPU monitor on C:/ for test\_system is at 90%. It has violated the threshold for at least 1 minute out of 5 minutes.

- **Close alarm message**

```
 ${metric_name} on ${component_name} for ${device_name} is OK.
```

Example: CPU monitor on C:/ for test\_system is OK.

You can customize any of the default alarm violations messages to provide information that is relevant to your environment. You can enter text that describes a business location, or can add the variables that provide the information you want. For a complete list of supported variables, see the [Alarm Message Variables](#) topic. **Follow these steps:**

1. Within an alarm policy, scroll to the Alarm messages section.
2. Click the **Inline Menu**



for the message you want to change.

The Alarm Messages dialog displays the alarm message and the available variables.

3. Enter text and additional variables to modify the message.
4. At any time, you can click **Reset to Default** to return the modified message to the predefined default settings.
5. Click **Save** to update the message with your changes.

## **What do I need to know about alarm thresholds?**

The alarm threshold settings determine when an alarm is generated. An alarm threshold consists of three elements:

- **Alarm Severity:** The severity of an alarm. Alarms can be critical, major, minor, warning, or informational.
- **Threshold:** Identifies how threshold violations are handled. A threshold is composed of a threshold type (static or dynamic), an operator, and a value.

- **Threshold type:** For static alarms, violations are determined based on an absolute value that is collected for a metric. Dynamic alarms are generated when the calculated average trend is a configured percentage equal to, above, or below the calculated baseline for a metric.
- **Operator and Threshold Value:** Identifies the acceptable state or level of performance.  
An alarm is generated when a sample, collected for a metric at a configured interval, violates the threshold value.
- **Alarm Creation Timing:** Indicates how long after a threshold violation occurs that an alarm is generated. Infrastructure Management can generate an alarm *immediately* after a threshold violation occurs or after a certain number of threshold violations occur within a configured time period (*Time over threshold*).

### **What are alarm thresholds tied to?**

An alarm threshold is tied to a single metric. You can configure alarm thresholds for a device, a monitoring technology, or a group.

### **What is the difference between a static and a dynamic alarm?**

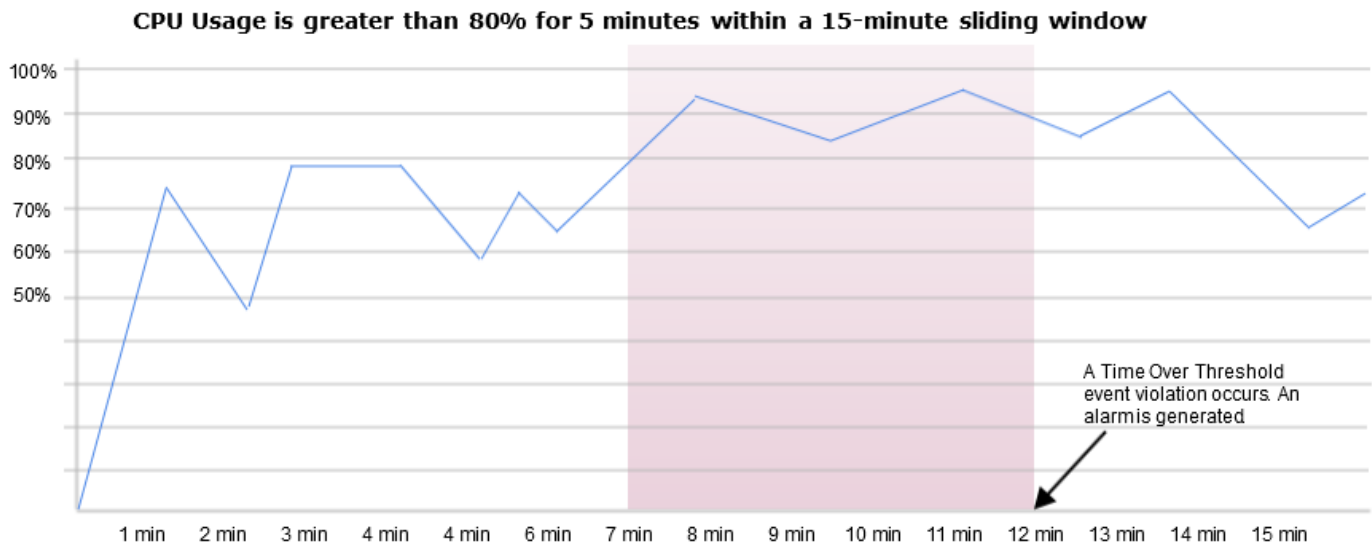
There are two types of alarms: static and dynamic. A static alarm is generated when a metric reaches a configured threshold value. For example, when CPU Usage on a target device reaches 95%, the policy generates a critical alarm. When you are monitoring a device that has persistent issues, consider configuring a static alarm. Dynamic alarms are generated based on the moving average of the baseline data that was collected over the previous 28 days. When you specify a threshold value for a dynamic alarm, an alarm is generated when the calculated average of the data reaches the configured percentage above or below the average trend. The calculated average trend can change over time as the collected baseline data changes. If you enter a dynamic threshold of >10% for CPU Usage, and the average trend of CPU Usage for the last 28 days is 85, an alarm is generated when the CPU Usage goes above 95%. When you are monitoring a healthy, stable device whose resources are used in a consistent manner, configure a dynamic alarm.

### **What is the difference between immediate and time over threshold alarming?**

Infrastructure Management can generate an alarm *immediately* after a threshold violation occurs, or after a certain number of threshold violations occur within a configured time period (*Time over threshold*). The Time Over Threshold is an event processing rule which reduces the number of alarms that are generated when threshold violation events occur. You can use Time Over Threshold to filter out data spikes and monitor problematic metrics over a set period. Instead of sending an alarm immediately after a threshold violation occurs, the Time Over Threshold function:

- Monitors the events that occur during a user-defined sliding time window.
- Tracks the length of time that the metric is at each alarm severity.
- Raises an alarm if the cumulative time the metric is in violation during the sliding window reaches the set Time Over Threshold.

For example, you could configure a static or dynamic alarm that is generated when the threshold has been continuously violated for 5 minutes in a 15-minute sliding time period. The following figure shows when the alarm is generated.

**Figure 25: Time Over Threshold Alarm****Can I change the name of a monitoring profile after a corresponding alarm policy is generated?**

Do not change the name of a monitoring profile after it is used to generate an alarm policy. Alarm policies are dependent on monitoring profiles. If you change the monitoring profile name or the corresponding alarm policy name, CA UIM stops generating alarms for the devices, groups, or technologies monitored by the alarm policy. Other than the lack of alarms, there is no indication or error message that a profile has been deleted.


**Can I change the name of an alarm policy that was generated from a monitoring profile?**

Do not change the name of an alarm policy generated from a monitoring profile. Alarm policies are dependent on monitoring profiles. If you change the monitoring profile name or the corresponding alarm policy name, CA UIM stops generating alarms for the devices, groups, or technologies monitored by the alarm policy. Other than the lack of alarms, there is no indication or error message that a profile has been deleted.

**Can I delete the monitoring profile after the alarm policy is generated?**

Do not delete a monitoring profile associated with an alarm policy. The alarm policies are dependent on monitoring profiles. If you inadvertently delete a monitoring profile, CA UIM stops generating alarms for the devices, groups, or technologies monitored by the associate alarm policy. Other than the lack of alarms, there is no indication or error message that a profile has been deleted.

**How do I search for an alarm policy?**

Click **Settings** (  ), and then select the **Alarm Policies** card. A filtering mechanism is available in the top left corner of the alarm policies list. Enter a technology, an alarm policy name, a metric name, or a creator to search for a specific alarm policy.

**How many alarm thresholds can I configure for a metric?**

For a single metric, you can configure as many thresholds as you need to monitor a target device.

**My alarms are chatty or I'm seeing alarm flapping. What can I do?**

Consider adjusting the alarm threshold setting. If you created a monitoring configuration profile using the predefined threshold settings, these setting might not be appropriate for your environment. If you are seeing alarm flapping—where

an alarm is generated, quickly closed, and generated again within a short time period—consider configuring the Time Over Threshold timing option for an alarm. When you configure the Time Over Threshold (TOT) option, an alarm is generated only when the TOT threshold is reached the configured number of times, during the configured sliding window.

### **How can I reset an alarm message to default settings?**

You can return a customized alarm message to the predefined alarm message at any time. **Follow these steps:**

1. Click **Inline Action**



next to the desired alarm message.

2. On the Alarm message dialog, click **Reset to Default**.

The predefined message appears in the Alarm Messages panel. The next alarm that is generated displays the predefined alarm message.

## **Alarm Message Variables**

You can customize the alarm messages for an alarm policy by using any of the variables that are defined in this topic. If you created custom messages using the older versions of templates, you might have used different variables. Unified Infrastructure Management can resolve these older variables to display the correct data in your customized alarm messages.

### **Examples:**

#### **General Alarm Message**

Major (severity 4) alarm for GuestDisk// on my\_server. Disk Free is > 20%, which is above the configured static threshold of 15. Contact Bob at x1234 to order a new disk.

```
${alarm_severity} (severity ${alarm_level}) alarm for ${component_name} on
${device_name}. ${metric_name} is ${threshold_operator} ${metric_value}${metric_unit},
which is above the configured ${threshold_type} threshold of ${threshold_value}.
Contact Bob at x1234 to order a new disk.
```

#### **Time Over Threshold Message**

Critical (severity 5) Alarm - Send email notification to Bob at bob@CompanyA.com or call x1234 - Immediate response requested. Taking more than 3000 ms to handle server-page requests on my\_apache\_server. HTTP response time has been > 2000 ms for 12 mins in a 15 mins window.

```
${alarm_severity} (severity ${alarm_level}) Alarm - Send email notification to Bob at bob@CompanyA.com or call
x1234 - Immediate response requested. Taking more than ${metric_value} ${metric_unit} to handle server-page
requests on ${device_name}. ${metric_name} has been ${threshold_operator} ${threshold_value} ${metric_unit}
for ${tot_time_window} ${tot_time_window_unit} in a ${tot_sliding_window} ${tot_sliding_window_unit} window.
```

#### **Close Alarm**

HTTP response time on my\_apache\_server is at or faster than 2000 ms for 12 mins in a 15 mins window. Critical (severity 5) alarm cleared.

```
${metric_name} on ${device_name} is at or faster than ${threshold_value} ${metric_unit}
for ${tot_time_window} ${tot_time_window_unit} in a ${tot_sliding_window}
${tot_sliding_window_unit} window. ${alarm_severity} (severity ${alarm_level}) alarm
cleared.
```

## Supported Variables

For a complete list of supported variables, see the "Supported Alarm Policy Message Variables" section in the [plugin\\_metric](#) article.

### NOTE

More information:

- [Manage Alarms with Centralized Alarm Policies](#)

## Alarm Policy Troubleshooting

This article includes troubleshooting topics related to alarm policies.

### Collected Metrics Not Showing During Alarm Policy Creation

This issue indicates that the metric type definitions are not present in the database.

To troubleshoot this issue:

1. Query the `s_qos_data` table with the probe name to verify that the metrics are populated in the table:  
`Select * from s_qos_data where probe='<probename>'`
2. Query the `cm_configuration_item_metric_definition` table to ensure that the given metric type exists in it:  
`Select * from cm_configuration_item_metric_definition where met_type='<met_type>'`
3. If the above step does not work, get the required definition pack and update `ci_definition_pack` in the environment:  
`Select * from cm_configuration_item_metric where ci_metric_id in (select ci_metric_id from s_qos_data where probe='<probename>')`

### Creation/Update of Alarm Policies Failing

This issue indicates that the associated alarm policy management webapp has stopped responding or has some error communicating with the database.

To troubleshoot the issue:

- Verify the `policy_management.log` file in the `<Drive>\Nimsoft\probes\service\wasp` folder for any error. If the error is because of the database connection issues, restart `wasp`.

### Alarm Policy Not Deploying on Devices

This issue indicates that the robot version is not supported or the `policy_mode_enabled` parameter is set to `false`.

To troubleshoot this issue:

- Verify that the robot on which you are creating the alarm policy is 7.96 or later.
- Verify that the `policy_mode_enabled` parameter is set to `true` in the MCS configuration file (`mon_config_service.cfg`) available in the `<Drive>\Nimsoft\probes\service\mon_config_service` folder.

### Policy Details Present in `plugin_metric.cfg` But No Alarms Are Generating

This issue indicates that the collection interval has not reached yet or dynamic alarms are configured with the baseline enabled.

To troubleshoot this issue:

- View the dashboard to verify whether any metric has been collected after defining the alarm policy and it has breached the threshold.
- If dynamic alarms are configured, the baseline calculations are done every hour. So these alarms take time to be generated based on the creation time. For more information, see the [KB Article](#).
- Verify the spooler logs with the log level 4\5 on the robot computer where you have created the alarm policy.
- Increase the log level of spooler to 4 or 5.
- Restart spooler.
- Verify spooler.log to review the threshold calculation and reasons for alarms not getting generated.

### **Understanding Messages in the ssrv2audittrail Table**

Review the `objectvalue` column in the table to understand and troubleshoot the messages:

- `Nametoip`  
This implies that the robot is not reachable. Verify whether there are any issues with the robot in the controller.log file.
- `Session error`  
This implies issues with a client session on the robot computer.
- `Error deploying profile`  
This implies that the alarm policy deployment has failed. Verify the robot availability for the alarm policy.
- `Entity not found`  
This implies that the required device or group is missing.
- `runtime_error\unknown_error`  
This implies that the alarm policy creation has failed because of some unknown exception. Review the MCS logs for more details.

### **Device Added to Dynamic Group But Group Alarm Policy Not Getting Enforced**

This issue can happen when the link between a device and a group is not proper or when the MCS fails to process the device.

To troubleshoot this issue:

1. Collect the group ID from the `cm_group` table and `ssrv2devicegroup` table.
2. Ensure that the device is a member of the group (`cm_group_member` table).
3. Query the `ssrv2policytargetstatus` table with `policyID`, `groupID`, and `ssrv2devicegroup` (device ID).
4. If no entry exists, the MCS has failed to process this device as part of the group.
5. Verify the status in the `ssrv2devicegroup` table for the device ID. If it is `modified`, you can wait for it to be picked up. If it is `OK`, there is some issue. Collect `mon_config_service.log` from the `mcs probe` folder and update the device state to `modified` for a workaround.
6. If an entry exists and is in the new state, the device is yet to be processed.
7. If an entry exists and is in the error state, review the `ssrv2audittrail` table with the policy ID for error details.

### **No Alarm Generation and No Alarm Policy Information in plugin\_metric.cfg**

This issue can happen because of various reasons.

Reason: The template is not an enhanced template or the templates are not set to true for production.

To troubleshoot:

1. Query the `ssrv2template` table:  

```
select * from ssrv2template where probe='<probename>' and type='policy'
```
2. Ensure you have templates of the type `policy` and the production flag is set to 1.

Reason: If the template is proper, check whether the template is set to work for proper OS and nimbus types.

To troubleshoot:

1. Query the `ssrv2packagetemplate` table (template, nimbus\_type, os\_type) by template ID. `select * from ssrv2packagetemplate where template in (select templateId from ssrv2template where probe='<probename>')`
2. Verify the nimbus type and OS has the following values:
  - nimbus\_type: 0 (This indicates that alarm policy should work for both VM and robot.)
  - os\_type: null (This indicates support for all the operating systems.)

Reason: If the template exists with all proper settings, query `ssrv2policytargetstatus` with the policyID along with groupID/device ID to check the retry count and status.

To troubleshoot:

1. If no entry exists in the table, check `policy_management.log` at `<Drive>\Nimsoft\probes\service\wasp`. Search with the policy ID to see any error.
2. If an entry exists with the state as 'NEW' and retry count as 0, review the MCS logs at `<Drive>\Nimsoft\probes\service\mon_config_service\mon_config_service.log`.
3. If the MCS logs have connectivity issues or lock issues with the database, restart the mcs probe.
4. If an entry exists in new and the retry count is greater than 0, check the `ssrv2audittrail` table with (objecttype: POLICY, objectId: <policy\_id>). The objectvalue column must contain the reason for the failure.
 

```
select * from ssrv2policytargetstatus where policy_id=<policyID> and group_id=<groupID>
select * from ssrv2policytargetstatus where policy_id=<policyID> and cs_id=<csID>
```

### **Default Alarm Policy Conditions Not Coming Correctly**

After you migrate a legacy profile to an enhanced profile and find that the alarm policy conditions are not coming as expected, verify the following points:

- Review the threshold type value:
 

```
select * from ssrv2configvalue where profile=<enhanced_profileId> and variable like '%thresholds_table-thresholdtype-%' and value!='None'
```

 The value must be "static", "dyn\_scalar", "dyn\_pct", or "dyn\_stddev".
- Review the operator value:
 

```
select * from ssrv2configvalue where profile=< enhanced_profileId > and variable like '% thresholds_table-operator-%'
```

 The value must be "NE", "L", "LE", "EQ", "G", or "GE".
- Review the severity value:
 

```
select * from ssrv2configvalue where profile=<enhanced_profileId> and variable like '%thresholds_table-severity-%'
```

 The value must be 1,2,3,4,or 5.

## **Admin Console in OC**

The Admin Console application allows you to manage and maintain the hubs, robots, and probes on your system. You can access Admin Console through Operator Console (OC).

### **NOTE**

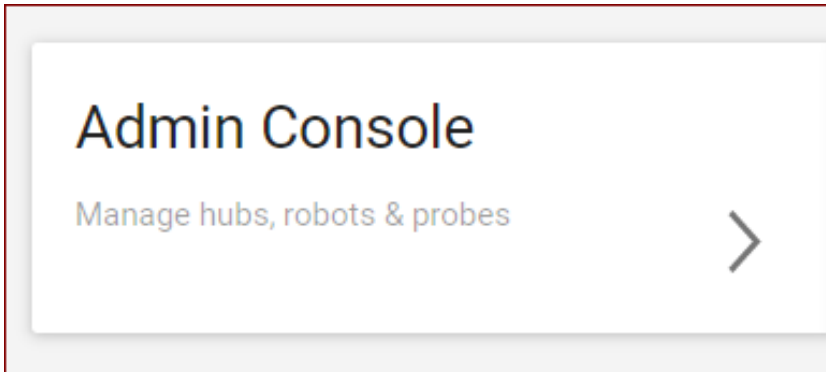
This functionality is available only to the bus users.

### **Follow these steps:**

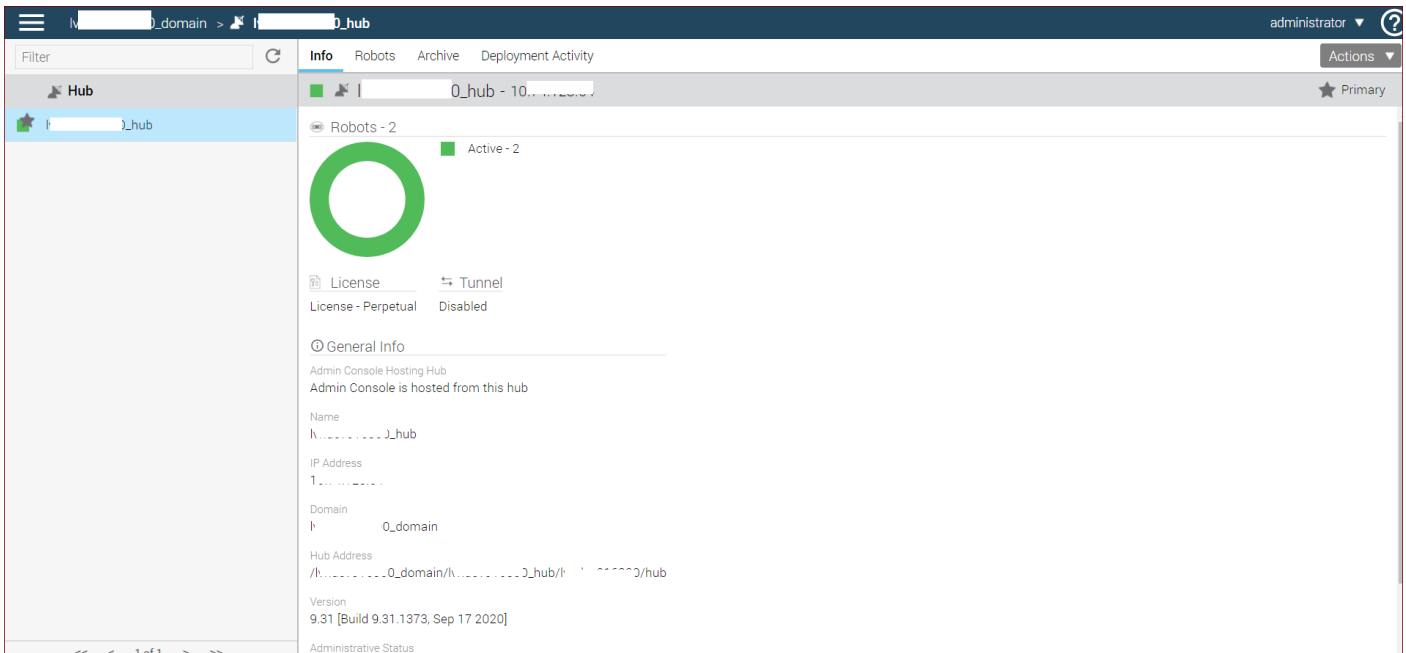
1. Access the OC UI.
2. Click the Settings icon (gear) in the left navigation bar.

The **Settings** page opens.

3. Locate the **System Administration** section.
4. Click the **Admin Console** tile.



The Admin Console application opens in a new tab.



You have successfully accessed the Admin Console UI from OC.

## Deprecated Portlets

The following table lists the deprecated portlets that have reached end-of-life and will not run with UIM 20.3.0 and later:

| Portlet                       | Status     | Replacement                                                                                                                                                                                                                                            |
|-------------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">List Designer</a> | Deprecated | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Dashboard Designer (List Widget)</a></li> <li>• <a href="#">Metric Viewer</a></li> <li>• <a href="#">Ad-hoc Reporting Using CABI</a></li> </ul> |



|                                                |                                                                                             |                                                                                                                                                                                                                                                        |
|------------------------------------------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">List Viewer</a>                    | Deprecated                                                                                  | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Dashboard Designer (List Widget)</a></li> <li>• <a href="#">Metric Viewer</a></li> <li>• <a href="#">Ad-hoc Reporting Using CABI</a></li> </ul> |
| <a href="#">Mobile</a>                         | Deprecated                                                                                  | No replacement is available.                                                                                                                                                                                                                           |
| <a href="#">MyTickets</a>                      | Deprecated                                                                                  | No replacement is available.                                                                                                                                                                                                                           |
| <a href="#">QoS Chart</a>                      | Deprecated                                                                                  | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">View and Export Quality of Service (QoS) Data</a></li> </ul>                                                                                    |
| <a href="#">Reports</a>                        | Deprecated                                                                                  | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Metric Viewer</a></li> <li>• <a href="#">SLA Reports in OC</a></li> </ul>                                                                       |
| <a href="#">Report Scheduler</a>               | Deprecated                                                                                  | No replacement is available.                                                                                                                                                                                                                           |
| <a href="#">ServiceDesk</a>                    | Deprecated                                                                                  | No replacement is available.                                                                                                                                                                                                                           |
| <a href="#">Unified Reports</a>                | Deprecated                                                                                  | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Use CABI Reports</a></li> </ul>                                                                                                                 |
| <a href="#">USM</a>                            | Deprecated                                                                                  | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Use Operator Console</a></li> </ul>                                                                                                             |
| <a href="#">SAML</a>                           | The portlet is deprecated; however, SAML integration is still supported.                    | You can access the integration information as follows: <ul style="list-style-type: none"> <li>• <a href="#">Configure OC to Use SAML Single Sign-On</a></li> </ul>                                                                                     |
| <a href="#">Dashboard Portlet</a>              | Deprecated                                                                                  | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Dashboard Designer in OC</a></li> <li>• <a href="#">DX Dashboard (DX Platform)</a></li> </ul>                                                   |
| <a href="#">Performance Reports Designer</a>   | Deprecated                                                                                  | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Metric Viewer</a></li> </ul>                                                                                                                    |
| <a href="#">SNMP Device Self-Certification</a> | The portlet is deprecated; however, the functionality is replaced with the SelfCert webapp. | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">SNMP Device Self-Certification</a></li> </ul>                                                                                                   |
| <a href="#">Unified Dashboards</a>             | Deprecated                                                                                  | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Use CABI Dashboards</a></li> </ul>                                                                                                              |
| <a href="#">Geo Views</a>                      | Deprecated                                                                                  | No replacement is available.                                                                                                                                                                                                                           |
| <a href="#">Alarm Console</a>                  | Deprecated                                                                                  | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Use Alarms View in OC</a></li> </ul>                                                                                                            |

|                                      |                                                                       |                                                                                                                                                                                                      |
|--------------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Custom Dashboards</a>    | Deprecated                                                            | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Dashboard Designer in OC</a></li> <li>• <a href="#">DX Dashboard (DX Platform)</a></li> </ul> |
| <a href="#">Dashboard Designer</a>   | Deprecated                                                            | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Dashboard Designer in OC</a></li> </ul>                                                       |
| <a href="#">Dynamic Views</a>        | Deprecated                                                            | No replacement is available.                                                                                                                                                                         |
| <a href="#">Maintenance Mode</a>     | The portlet is deprecated; however, the probe is still a part of UIM. | You can now access this functionality as follows: <ul style="list-style-type: none"> <li>• <a href="#">Configure Maintenance (Manage Groups)</a></li> </ul>                                          |
| <a href="#">Nimsoft Remote Admin</a> | Deprecated                                                            | No replacement is available.                                                                                                                                                                         |

## Operator Console Endpoints

You can navigate to any specific view in OC using direct urls. You might want to do this if you want to link to any specific view in OC from another application, or if you want to display data in group view or device details view in OC on a web page.

There are two ways to launch a OC window: using a URL, and using an HTML file. Using a URL is simple and flexible. Using an HTML file allows you to hide the user name and password or to incorporate OC in another web page (displaying it in a frame, for example).

### NOTE

Tomcat running in the wasp probe is upgraded for increased security. As a result, URLs containing certain characters (specifically: {, }, and |) may not be read properly. To avoid this issue, run new URLs (for example, to open OC) through a URL encoder utility. If you experience problems with URLs created in previous versions of the product, run these through a URL encoder and resave them.

## Contents

### Launch OC Endpoints

You can launch a new instance of OC using a URL and can append one or more parameters to customize the display.

The most basic syntax displays OC in the Home view:

```
http://<OC_hostname_or_IP>/operatorconsole_portlet/standalone_login.jsp?
user=<user_name>&password=<user_password>
```

### NOTE

If the user name and password are omitted from the URL, the OC instance requires login credentials when launched.

### Specify a View

You can specify a view to display by appending the following parameters to the URL:

- **tree**

Displays UIM groups in the tree view. For example:

```
http://<OC_hostname_or_IP>/operatorconsole_portlet/standalone.jsp?view=tree
```

- **badge**

Displays UIM groups in the badge view specified. For example:

```
http://<OC_hostname_or_IP>/operatorconsole_portlet/standalone.jsp?view=badge
```

- **list**

Displays UIM groups in the list view. For example:

```
http://<OC_hostname_or_IP>/operatorconsole_portlet/standalone.jsp?view=list
```

- **alarm**

Displays the alarm view of the devices in OC. For example:

```
http://<OC_hostname_or_IP>/operatorconsole_portlet/standalone.jsp?view=alarm
```

- **device specific alarms**

Display the alarms specific to a device. For example

```
http://<OC_hostname_or_IP>/operatorconsole_portlet/standalone.jsp?view=alarm&cs_id=<computer_system_id>
```

- **device**

Displays the device view of the computer system. Obtain the ID number by querying your UIM API or UIM database. For example:

```
http://<OC_hostname_or_IP>/operatorconsole_portlet/standalone.jsp?view=device&cs_id=<computer_system_id>
```

## **Launch OC Using an HTML File**

You can use an HTML file to launch the OC. You might want to do this if:

- You do not want to pass parameters, such as user name and password, in a URL.
- You want to display the OC as part of an HTML page, such as in a frame.

### **Follow these steps:**

1. Create an HTML file with the following syntax:

```
<html>
 <body onload="javascript:document.autoForm.submit()">
 <form name="autoForm" method="post" action="http://<OC_hostname_or_IP>/operatorconsole_portlet/standalone_login.jsp">
 <input type="hidden" name="view" value="alarm">
 <input type="hidden" name="cs_id" value="<computer_system_id>">
 <input type="hidden" name="user" value="<USER NAME>">
 <input type="hidden" name="password" value="<USER PASSWORD>">
 </form>
 </body>
</html>
```

#### **NOTE**

Supported values for the parameter "view" are tree, badge, list, alarm, and device. "cs\_id" is used only for device and alarm views as additional parameter.

2. Execute the HTML file.

For example, enter the path to the file as a URL in a browser:

```
http://<SERVER>/<PATH TO HTML FILE>
```

The OC opens in a browser window without displaying parameters in the URL.

3. (Optional) To display the OC as part of an HTML page, refer to the HTML file created in step 1.

For example, to display OC in an iframe, include syntax similar to the following example in your HTML page:

```
<html>
 <body>
 <iframe src="http://<SERVER>/<PATH TO HTML FILE>" width="100%" height="300" frameborder="0">
 </iframe>
 </body>
</html>
```

## Monitor Technologies Using RESTMon

You can now monitor any technology or device data using the REST APIs. Using the templates that are provided by UIM you can upload the schema, which details the QoS and the aggregation logic with the http/https REST end points. You can define the metrics, alarms, and can populate dashboards for the monitored devices. For more information, see [Monitor Technologies Using RESTMon](#).

## The Settings View

Use the left navigation to open the **Settings** view. You can perform the following operations in the settings view in the Operator Console:

- [Account Admin](#)
- [Alarm Policies](#)
- [Administration](#)
- [Dashboard Designer](#)
- [RESTMon](#)
- [Device Self-Certification](#)

The screenshot displays the Settings View interface, organized into three main sections:

- Alarms and Notifications:** Contains three cards:
  - Account Admin:** Manage accounts using account admin.
  - Alarm Policies:** Manage when alarms are created (19 existing policies).
  - Administration:** Configure automatic groups.
- Dashboard and Reports:** Contains one card:
  - Dashboard Designer:** Create dashboards using dashboard designer.
- Integrations:** Contains two cards:
  - RESTMon:** Create custom RESTful API Monitoring.
  - Device Self Certification:** Device self certification for SNMP collector.

For more detail on configuring the probes and applying monitoring with templates, see the [Probes Documentation Space](#).

## The Dashboard Designer

Dashboards display data in graphic elements, such as gauges, charts, tables, images, or shapes. These elements can display data from several types of data sources and can be customized with a wide range of colors, fonts, and sounds.

The Dashboard view allows you to create, edit, preview, save, and publish dashboards. Others can view dashboards in several ways:

- An account contact user can log into the system and navigate to the dashboard,
- A user can view the dashboard in a browser by entering the URL for the dashboard.
- The dashboard creator can save the dashboard to PDF and send it to a user on a defined schedule.
- The dashboard creator can export the dashboard for a user on another computer system running Operator Console (OC).

The Dashboard view is installed by default with Operator Console (OC) and appears as a view in the header bar.

## Contents

### Create a Dashboard

On opening the Dashboard view, a dialog box prompts the user to create a dashboard or open an existing dashboard.

#### Follow these steps:

- Click the Create button to create a dashboard.  
OR
- Click a dashboard from the list or open a folder for the path to an existing dashboard, and click Open.

The dashboard is displayed in Edit mode.

#### NOTE

You can open an existing dashboard in a web browser by supplying the path to the dashboard as a URL parameter. The path is the full path separated by '/'. For example, the URL

`http://(server)/dashboard/jsp/standalone.jsp?path=folder/file`

takes you to a dashboard where "(server)" is the server where Operator Console (OC) is running and "folder/file" is the folder and file names under which the dashboard was saved in Dashboard Designer. The dashboard appears in the browser window.

If you are an account contact user, the URL takes you to the published version of the dashboard. If you are a bus user, you are taken to the working version of the dashboard.

#### NOTE

While creating the dashboard, make sure that there are no special characters like "&" in the dashboard name as these are not supported.

### View Modes

When you create dashboards, you typically switch between the Live view and Edit modes. Dashboards are created in Edit mode. Live view allows you to display of the dashboard with real-time data.

- **Edit mode**

To edit a dashboard, select **Dashboard, New**, or **Dashboard, Open**. A new dashboard opens in edit mode. An existing dashboard opens in Live view mode.


#### NOTE

You must have Administrator permissions to create, edit, or delete private dashboards. If you are an Account user, you will only have the **Open** option for dashboards assigned to your account.

- **Live view mode**

The view mode for dashboards that are previewed, saved, or published. The Live view does not display an alignment grid in the dashboard field or editing column at the right. In Live view, options under the Edit menu icon include only those assigned to your permissions.

To preview the dashboard you are editing, select **Dashboard, Live View**. In live View mode, you can view a dashboard with live data as it would appear once published. Live view mode allows you to preview your dashboard temporarily, and is not the same as publishing a dashboard.

You can take these actions from live view mode using the Edit menu icon () (located in the black tab at the top-center of the dashboard window):



Create a dashboard. The new dashboard opens in Edit mode.



Open a dashboard. The dashboard opens in Edit mode.



Edit the dashboard currently in Live View.




View full screen.





Download the current dashboard to PDF.

#### NOTE

If the black tab containing the  icon is not displayed in Live View, move your mouse over the dashboard. The black tab is hidden when there is no activity in the window.

- **Full screen mode**

To open your dashboard in a new browser tab or window without displaying the Operator Console (OC) view environment, save your dashboard and then select **Dashboard, Full screen mode** from edit view, or click  and then  from live view.

#### NOTE

After making changes, save your dashboard. Any unsaved edits are not shown in the full screen window. Edits should be done in only one window as it is possible to overwrite edits from another open window.

Press F11 to switch between browser full-screen and Edit or Live View mode within the same browser window.

To save a dashboard, select **Dashboard, Save** from Edit mode.

To publish a dashboard, select **Dashboard, Publish** from Edit mode. Save a dashboard in order to publish it. Published dashboards are available for authorized users to view.

### Prepare the Canvas

Set up the canvas for working on a dashboard.

You can set the size and grid functions of the canvas or can set the background for the dashboard.

### Size the Canvas

Set the canvas to an appropriate size for your dashboard.

### **Follow these steps:**


1. Click the **Canvas Properties** () tab.

2. Click **Size** to expand the menu.
3. Set the **Width** and **Height** of the canvas.

### **Set the Background Properties**

Set the color for the dashboard background to enhance contrast, add an image as the background to brand the dashboard, and set the opacity of the background to avoid clutter.

#### **Follow these steps:**

1. Click the **Canvas Properties** () tab.
2. Click **Background** to expand the menu.
3. Set the properties for the dashboard background:
  - **Background Color**  
Sets the color for the dashboard background. Enter a hex code or click the Background Color field to display a color picker. By default the background is white, hex code #FFFFFF. Use the slider on the right of the color picker to set the opacity for the color.
  - **Background Image**  
Sets an image as the background for the dashboard.
  - **Opacity**  
Sets the opacity of the background. Click the slider to adjust the opacity.


### **Set a Background Image**

You can set a background image for the dashboard to orient information or brand the dashboard to your company.

#### **NOTE**

If you want the dashboard to have a background image, use this procedure instead of using an image widget. Using this procedure automatically places the background image behind the layers on the canvas, and any actions you take on the canvas do not affect the background image.


#### **Follow these steps:**

1. Click the **Canvas Properties** () tab.
2. Click **Background** to expand the menu.
3. Click in the **Background Image** field to display the Image Gallery. To add an image to the Image Gallery, click **Upload Image** and browse to the image.
4. (Optional) Click the opacity slider to adjust the opacity of the background image.

### **Set the Grid Functions**

You can turn the grid on or off or can change its color or spacing to help align widgets on the dashboard. You can also turn the **Snap to grid** function on or off.

#### **Follow these steps:**

1. Click the **Canvas Properties** () tab.
2. Click **Grid** to expand the menu.
3. Set the properties for the dashboard grid:
  - **Grid On/Off**  
Turns display of the grid on or off.
  - **Color**  
Sets the color for the grid.
  - **Spacing**

Sets the spacing between lines of the grid.


– **Snap to grid On/Off**

Turns the **Snap to grid** function on or off. When turned on, items snap to the nearest grid line as you drag them around the canvas. Snap is useful for aligning items.

### **Add a Widget**

Widgets are dashboard elements that display data. Widget formats present data in specific ways, so different widgets are used for different types of data. Matching the widget to its data is an important consideration of dashboard design.

#### **Follow these steps:**

- Click the **Widgets** () tab at the top of the right pane of the dashboard.
- Click a widget and drag it to the canvas.
- Click sides or corners of the widget to size it and move it on the canvas.

For a full list of available widgets, see the article [Add a Dashboard Widget](#).

### **Create and Assign a Data Source**

In order for widgets to display data, assign a data source to one or more widgets. First, create a data source. Then, drag-and-drop the data source onto widgets.

Once created, data sources are available to any of the widgets on the dashboard, and a single data source can be assigned to multiple widgets.

#### **NOTE**

Data sources are specific to a dashboard and must be created for each new dashboard. However, a dashboard with data sources that is saved with another name retains its data sources.

Available data source types are:

- Alarm
- Dashboard
- Metric
- SLA/SLO

Advanced data sources require special knowledge, such as familiarity with your environment or with creating database queries. Advanced data sources are:

- Probe
- QoS
- SQL

#### **NOTE**

Not all widgets support all data sources. When you drag a data source onto a widget, the widget border turns green if the widget supports the type of data source and turns red if it does not.

For a full list of data sources, see the article [Create and Assign the Data Source for a Widget](#).


### **Save a Dashboard**

Save a dashboard for future use.

Save a dashboard in order to publish it.



**Follow these steps:**

1. Open the dashboard in **Edit** () mode.
2. Click **Dashboard, Save, or Dashboard, Save as**.
3. Enter a name in the **Path** field.  
To group dashboards in a folder, enter the folder name before the dashboard name. For example, to save a dashboard that is named "CPU Usage" in a folder named "Servers," enter the following:  
/Servers/CPU Usage.



**Publish a Dashboard**

Publish a dashboard to save a version of the dashboard for viewing by users with appropriate permissions. Dashboards saved to 'Private' can be viewed only by the creator; dashboards saved to an account can be viewed only by account users; dashboards saved to 'Public' can be viewed by any user.

Published dashboards open in **Live view** mode, and dashboard queries are updated when the dashboard is opened, so the dashboard is always current. A published dashboard is unaffected by subsequent changes made to the dashboard in Edit mode until the dashboard is republished. For example, if you publish a dashboard, add an image widget, and save the dashboard, the published version does not yet include the image widget. If you republish that dashboard, the published version is updated to include the image widget. In this way, you can make changes to the dashboard without affecting the version that others can view.

Published dashboards are displayed in a frame with a toolbar. Hover over a toolbar icon to see a description of its function.


**NOTE**

If you make changes to the dashboard in Edit mode and decide that you want to go back to the published version, click on the View Published icon () and then click the Revert icon (.

**WARNING**

Publishing a dashboard that contains widgets with dashboard data sources also publishes those dashboards.

**Follow these steps:**

1. Open the dashboard in **Edit** () mode.
2. Go to **Dashboard, Publish**.

**NOTE**

Save the dashboard in order to publish it. Otherwise, this menu item is grayed-out.

- a. Choose a setting for the **Visibility** field:

**No Account**

When the dashboard is published, all bus users with the proper permissions can view the dashboard.

**Public**

When the dashboard is published, all bus and account contact users with the proper permissions can view the dashboard.

**Accounts**

Account contact users that are members of one of the selected accounts and have the proper permission can view published versions of the dashboard. Accounts are created and managed in the Account Admin view.

**NOTE**

Re-publish a dashboard in order to change the visibility setting.

- b. Click **Publish**. The dashboard is published.
3. (Optional) Go to **Dashboard, View published version**.


The published version is displayed.

A customer can view a published dashboard by logging into the system with a valid username and password, opening the Dashboard Designer view, and opening a dashboard from the dialog box that appears. Account contact users will only see dashboards in the dialog box that are assigned visibility for their accounts or assigned Public visibility. contact account users will only see the dashboard in Live view and will not be able to edit the dashboard.

### **Delete a Dashboard**

Delete a dashboard you no longer need.

#### **Follow these steps:**

1. Open the dashboard in **Edit** () mode.
2. Go to **Dashboard, Delete**.


### **Export a Dashboard**

You can export a dashboard in order to import it into another instance of the Dashboard view. This allows you to share dashboards with users on other systems. However, exporting a dashboard does not export its data sources, so an imported dashboard must have these data sources reassigned to the appropriate database.

#### **NOTE**

Dashboards can only be imported to the same UIM/Operator Console (OC) version from which they were exported. For example, a dashboard exported from UMP 8.51 can only be imported to another UMP 8.51 system. Dashboards are not compatible between versions.

#### **Follow these steps:**

1. Open the dashboard in **Edit** () mode.
2. Go to **Dashboard, Export**.

A zip file containing the dashboard file and any dashboard dependencies is created and saved in your browser's download location.

#### **NOTE**

Save changes to the dashboard in order to export it. If **Export** is not active on the menu save the dashboard.


### **Import a Dashboard**

You can import a dashboard zip file that was exported from the Dashboard view.

#### **NOTE**

You may need to reassign data sources after importing the dashboard.

#### **Follow these steps:**

1. Open the Dashboard in **Edit** () mode.
2. Go to **Dashboard, Import**.
3. Browse to the dashboard file you want to import and select it.
4. Click **Open**.  
The dashboard is imported and you can now open it.

**NOTE**

Dashboards can only be imported to the same UIM/Operator Console (OC) version from which they were exported. For example, a dashboard exported from UMP 8.51 can only be imported to another UMP 8.51 system. Dashboards are not compatible between versions.


**Generate a Dashboard PDF**

You can capture a dashboard as a PDF for viewing, saving, printing, or emailing.

**NOTE**



Dashboards can be scheduled and exported to PDF for all operating systems except Solaris and RHEL 8, which currently does not support PDF creation.

**Follow these steps:**

1. Create or open a dashboard in **Edit** () mode.
2. Go to the **Dashboard** menu and click **Generate PDF**.
3. View or save the file from the menu that appears.

You can also capture a dashboard from the Live view mode.

**Follow these steps:**

1. View a dashboard in **Live view** mode
2. Pull down the Edit menu from the **Edit menu** () icon.
3. Click the **Generate PDF** () icon.
4. View or save the file from the menu that appears.

**NOTE**

On some Linux distributions, PDF generation of a dashboard may fail. This is due to a missing library on the system required to perform PDF generation. You will be able to determine if this condition exists by enabling debug logging for: "com.firehunter.dashboard.service". If you are seeing the PDF creation problem, you may see the following error in the log file: "error while loading shared libraries: [libfontconfig.so.1](#)".

Here are example commands to install the necessary library.

Fedora-based system:

```
sudo yum install fontconfig freetype libfreetype.so.6 libfontconfig.so.1 libstdc++.so.6
```

Ubuntu/Debian-based system:

```
sudo apt-get install libfontconfig
```

**NOTE**

In Linux environments, if you experience any rendering issues with the dashboard PDF like blank report or garbled characters in the report.

**Follow these steps:**

1. For Linux, OpenJDK does not provide the file lib/fontconfig.properties and the folder lib/fonts.
2. Create a fontconfig.properties file in [Nimsoft JRE Home]/lib folder for linux with the below entries:
 

```
version=1
sequence.allfonts=default
```
3. Create a folder lib/fonts in [Nimsoft JRE Home].

- Install "dejavu-fonts" on the linux system and copy the .ttf files to [Nimsoft JRE Home]/lib/fonts folder.
- Restart UIM robot.




### Schedule a Dashboard Report

As a bus user, you can schedule dashboard PDF creation and distribution by email or file transfer. This lets you send updated dashboards on a timed basis to customers.

#### Follow these steps:

- Create or open a dashboard in **Edit** mode.
- Save and publish the dashboard.
- Click the **Dashboard** menu and select **Schedule...**  
A window opens.
- Fill out the appropriate fields.
- Click the **Preview** button to view the PDF.
- Click the **Create** button to create the job.

In the report window, the left-hand pane contains a list of existing reports for the current

dashboard. Click the icons to **Create** () a new report or to **Edit** () or **Delete** () an existing report.

The right-hand pane contains fields for defining the report and transferring it by email or FTP. Required fields are indicated with an asterisk.

#### General

- Name** - A name for the report.  
**Run report as user** - The user associated with the report.  
You must be a bus user to create the scheduled report. As the report creator, you can select the name of an account with permission to view the report. Account users in the list are taken from Account Admin settings, with the format *account/user*.
- Description** - Any description or details of the report.
- Disabled** - A checkbox that allows the user temporarily to suspend report creation.

#### Schedule

- Type** - The interval of the report.  
The report can be scheduled to run only once or recursively on an hourly, daily, weekly, or monthly basis.
- Run this job** - The scheduling parameters for report creation.  
The window displays the following fields according to the selected Type:
  - **Once only**  
**Starting** - The date (selectable from a calendar page) and time to run the report. The current date and time are entered as the default.

#### NOTE

You can select any portion of the date and time string to change it. The month appears as a numeric value for editing and as a character string for ease of reading. You can also click the calendar to select a different date.

- With time zone** - The time zone, selected from a pull-down menu. The default is the server's time zone.
- **Hourly/Daily/Weekly/Monthly**  
**Starting** - The date and time to start the job,

**Every hour(s)/Every day(s)/On day(s)/On** - The hourly interval/the number of days between reports/the days of the week/or the day or date of selected months to run the report.

**Ending** - Radio buttons to run the reports with no ending date (**Never**) or until a given date and time. Selecting the **Ending date** radio button activates the field for selecting the ending date and time.

**With time zone** - The time zone, selected from a pull-down menu. The default is the time zone of the server.

## Context

This section is automatically populated with fields for the dashboard context selector widget, if used. All columns from the dashboard context widget are listed by name. Changing selectors in the job definition window overrides settings in the context selector widget of the dashboard. In this way, different jobs can run from the same dashboard with different context settings.


The parameters fields can be used to change any of the parameters that are used in dashboard data sources.

- **Time** - The time period for the context selector, if used.  
A drop-down list provides options from the last hour to the last 12 months.

### NOTE

The dashboard context period and the report interval are independent. This allows the report to capture stepped data updates.

- **Other selectors** - Fields from a context selector widget, if used, by name.  
The values for these selectors can be changed here and applied to the context selectors in the dashboard for the job.
- **Parameters**

Parameters values for dashboard data sources. By default, the report uses parameters listed in the Parameters () tab of the dashboard, but the values for these parameters are changed by manually entering the parameter names and their new values.

### NOTE


Changing context selector and report parameter values further customizes the output of the dashboard. To capture all desired data, the person creating the report should have a thorough knowledge of the dashboard data sources and parameters.

### NOTE

Be aware that, when using the context selector, `${startTime}` and `${endTime}` parameters in the SQL query are converted to epoch time, which is not aware of daylight savings time. Comparing to a datetime/timestamp column in the database might give you an hour offset if you are in daylight savings. You will need to adjust your query to add daylight savings in if applicable.

## Delivery

- **Email** - The email address for delivery. You can send the PDFs for the job to multiple addresses.

Clicking the **Configuration** () icon for email delivery opens a dialog box for the email settings for the sender, including SMTP server and port, and security and authentication options.

- **FTP** - FTP server, port, and user settings for transfer.

### NOTE

You can schedule to send reports using one or both of these options.


- **Passive** - A selector to change the FTP protocol from Active (the default) to Passive.

Buttons at the bottom of the window are context-sensitive, and allow the user to:

- **Preview** the report.
- **Cancel** the creation of a new job or cancel editing of an existing job.
- **Update** an existing job.
- **Create** a new job.

#### NOTE

The contents of a scheduled report can be changed in two ways: by editing parameters in the scheduled job or by changing the contents of a dashboard. To edit job parameters, select the job from the left pane, click the

Edit () icon, and change the settings described previously. To change the contents of a dashboard, open the dashboard, make the necessary changes, and then save and republish the dashboard.

#### View a Dashboard URL

You can view a dashboard from a remote computer within a browser window outside of Operator Console (OC). Others with appropriate permissions can also view the dashboard.

#### Follow this step:

- In a browser navigation field, type in: `http://(server)/dashboard/jsp/standalone.jsp?path=folder/file` where "(server)" is the server where Operator Console (OC) is running and "folder/file" is the folder and file names where the dashboard was saved in Dashboard Designer. The dashboard appears in the browser window. An account contact user sees the published version of the dashboard. A user with administrative privileges (such as a bus user) sees the working version of the dashboard.

#### Specify a Default Dashboard for Users

You can specify the default dashboard that a user or group of users sees when using the dashboard view.

Access the Preferences dialog by clicking the **Options** icon



then clicking **Preferences**.

#### Follow these steps:

1. Enter **Height** in pixels for this instance of the view.  
If there is more than one view on the page, assign the height so that all views can be seen.
2. Select the default dashboard for the view to display.
3. Click **Save** to save your changes.

## Migrate Dashboards from the Legacy Dashboard Designer portlet

If you have published dashboards that were created with the legacy Dashboard Designer portlet, they are automatically migrated when wasp starts as part of CA UIM beginning with CA Nimsoft Monitor 7.5.


Legacy dashboards that have been saved but not published are not migrated.

Any dashboards that were previously migrated are not migrated again.

#### NOTE

A dashboard that has been migrated can be migrated again if you save it under a different name.

In most cases, no action is required to migrate your published legacy dashboards. However, if there were errors during migration, you will see a sticky note widget when you open the dashboard in the new Dashboard portlet. Click the sticky

note widget to select it, and then click the **Properties** () tab. Information regarding the migration is displayed in the Notes section.

If there was an error with a property, a default value was used for the property value during migration. Edit the value as needed.

If you cannot open a migrated dashboard, you can view messages about the migration in the `../Nimsoft/probes/service/wasp/portal.log` file.

CA strongly recommends that you use the new Dashboard portlet to edit and create dashboards. Legacy dashboards are only migrated once; any further edits that are made with Dashboard Designer to a migrated dashboard will not be reflected in the Dashboard portal. New published dashboards that are created with Dashboard Designer will be migrated the next time the wasp probe is restarted.

### **WARNING**

Dashboards that are created with the Dashboard portlet cannot be opened by the legacy Dashboard Designer.

### **Migration of Alarm Widgets**


Dashboards that are created with the legacy Dashboard Designer portlet might include alarm widgets, which are replaced by the alarm data source in the Dashboard portlet.

The alarm filter for the alarm data source, defined when you create an alarm data source, has some differences from the alarm filter for the legacy dashboards alarm widget:

- The alarm data source filter is case-sensitive, while the legacy alarm widget filter was not.
- The alarm data source filter does not support the wildcard shortcut notation that the legacy alarm widget supports.
- There might be minor differences in the way regular expressions are interpreted.

Because of these factors, alarm data sources that were migrated from legacy alarm widgets might behave differently than the legacy alarm widgets. If this happens, modify your alarm filters in the alarm data source.

#### **Follow these steps:**

1. In the right pane, **Data Sources** () tab.
2. Click **Alarm** to expand the menu.
3. Double-click the data source that you need to modify.
4. Modify the alarm filter so that it contains case-sensitive text matches or standard regular expressions.

### **Migration of Curved Lines**

Dashboards created with the legacy Dashboard Designer portlet might include curved lines, which are replaced by a multisegmented line during migration. Attempting to manipulate a migrated curved line by clicking and dragging only affects the selected segment of the line. You must select the entire multisegmented line to move or resize it.

## **Add a Dashboard Widget**

You can place widgets on the dashboard to display the status of devices you are monitoring. They can also be used as graphical elements in dashboard layout. Available widgets include shapes, images, tables, lines, gauges, and charts.

After you add a widget, assign it a data source. You can also set properties for widgets, change their appearance, and connect them with lines.

### **NOTE**

You must be in edit mode to work with widgets. Switch to Live View mode to view widgets with current data values.

### **Contents**

## Add a Shape

Add a circle or rectangle to display information about the dashboard. The shape does not display the value of its data source, but the color of the shape reflects that value. After assigning a data source to the shape, you can create a color map so that the color reflects different thresholds.

The circle and rectangle widgets support the following data sources:

- Alarm
- Dashboard
- Metric
- Probe
- QoS
- SLA
- SQL

### Follow these steps:

1. Click the **Widgets**



in the right pane.

) icon

2. Click **General** to expand the menu.
3. Drag a circle or rectangle onto the canvas.

You can now assign a data source for the shape, then set any properties that you wish to change.

### NOTE

You can also use shaped widgets as graphical elements within the dashboard, for instance, to group other widgets within a theme. You are not required to assign data sources to a shape widget. To control the layering order of widgets on the dashboard, click the **Move to front** and **Move to back** buttons on the toolbar at the top of the window.

## Add a Line


Add a line to indicate a relationship between widgets or as a graphical element within a dashboard. Lines can also represent tunnels or other links between network elements and reflect operating values.

You can easily connect two widgets by drawing an anchored line between points on the widgets. When you move the widgets, the anchored lines move with the widgets.

You can also create a standalone line (not anchored to widgets) by dragging a line widget onto the canvas, adjusting its length and placement.

Lines support the following data sources:



- Alarm
- Dashboard
- Metric
- QoS
- SQL


The line does not display the value of the data source, but the color of the line reflects the value. After assigning a data source to the line, you can create a color map so that the color changes for different thresholds. Select the line on the canvas and go to **Color** under the **Widget Properties** (  ) tab to set colors for the line.


You can also play sounds for different data values.



**Follow these steps:**

1. Click the **Widgets**  icon in the right pane.
2. Click **General** to expand the menu.
3. Drag a line widget onto the canvas.
4. Click the **Line Endpoints**  icon on the toolbar at the top of the dashboard to turn on line endpoints.
5. Drag an endpoint of the line to size it or to the widget where you want the line to connect. Anchor points for the widget appear when the endpoint of the line nears the widget.  
To move a line around the canvas, drag its end points or change the **Points** settings under **Line** in the **Widget**

**Properties**  tab to define the coordinates of the endpoint. You can also multiselect the line and other types of widgets and move them as a group.

6. Click the line endpoints icons on the toolbar to turn off line anchor points.
7. Click the line to select it.
8. Click the **Widget Properties**  tab.
9. Click **Line** to expand the menu.
10. Set the properties for the line:
  - **Thickness**  
Sets the thickness of the line.
  - **Points**  
Defines the coordinates for the endpoints (or mid-points) of the line.
  - **x, y**  
The **x** fields set the horizontal position of the endpoints, and the **y** fields set the vertical position of the endpoints. Enter the x and y position for each endpoint or mid-point and click on the canvas to move the endpoints.
  - **Widget**  
Names the widget if the line is connected to a widget anchor point.
  - **Anchor**  
Specifies the location of the anchor point on the widget where the line connects.

**NOTE**

If the Widget and Anchor information does not appear when creating the line, clear the line and then reselect it.

11. (Optional) Add one or more mid-line points to the line:
  - a. Click the line endpoints icon on the toolbar to turn on line end points.
  - b. Click the line on the canvas to add a mid-line point. You can add as many mid-line points as you need.  
You can now drag the anchor line midpoints to create angles in the line. This can be useful when multiple lines cross to avoid confusion in their paths.

**NOTE**

You can add angles to a line, but you cannot create a line curved to an arc.

12. (Optional) Add arrows to the line:
  - a. Click the On/Off button next to **Arrows** to turn it on.
  - b. Click **Arrows** to expand the menu.
  - c. Set the properties for the arrow:
    - • **Type**

Defines whether there is a single or multiple arrow heads on the line. If you click **Multiple**, an arrow head is displayed in the center of each line segment.

- **Direction**

Sets whether the arrowheads point in the direction that the line was created (**Head**) or back to the origination point (**Tail**).

You can now assign a data source to the line, if desired or change other properties of the line, such as adding a shadow or border, or creating a color map.


### **Add an Image**

Add an image widget to display an image on the dashboard. The image can be used (for instance) to represent a network or device, a network or device location (such as a map), or any other graphical element to provide context to the dashboard.

The following types of image files are supported:

- .gif
- .jpg
- .jpeg
- .tiff
- .png

#### **NOTE**

To add a background image to the dashboard, use the **Background Image** setting in the **Canvas Properties** () tab instead of an image widget. The **Background Image** setting automatically places the image at the back of the layers on the canvas, and actions you take on the canvas do not affect the image.

The image widget supports the following data sources:

- Alarm
- Dashboard
- Metric
- QoS
- SLA
- SQL

#### **Follow these steps:**

1. Click the **Widgets**



tab.

2. Click **General** to expand the menu.
3. Drag the **Image** widget onto the canvas.
4. Click the image widget to select it.

5. Click the **Widget Properties** () tab.

6. Click **Image** to expand the menu.
7. Click in the **Image** field to display the Image Gallery.

8. Click an image to select it.

To add an image to the Image Gallery, click **Upload Image** and browse to the image.

9. Click **Select**.

The image is displayed in the widget. By default **Stretch to fit** is turned off. To size the image to fit the frame of the widget, click the button to turn this on.

You can now assign a data source to the image widget or change the widget properties, including defining an image map.

### **Add an SQL Table**

Add an SQL table widget to display data from an SQL query.

#### **NOTE**


You must have an SQL data source configured to display data in the table widget. You can assign a previously written query or can create a new query while defining the widget.

#### **Follow these steps:**

1. Click the **Widgets**



tab.

2. Click **General** to expand the menu.
3. Drag the **SQL Table** widget onto the canvas.
4. Click the **Data Sources** () tab.

#### **NOTE**

If you do not see the **SQL** pane, click **Options**




**Show advanced data sources.**


5. Click **SQL** to expand the menu.
6. Drag an SQL data source onto the table widget.

#### **NOTE**

If you do not see any SQL data sources, [create one](#).

The table is created with the appropriate rows and columns and is populated with data. You can set the properties for the columns in the following steps.

7. Click the table to select it.
8. Click the **Widget Properties** () tab.
9. Click **Table** to expand the menu.
10. Set the **Row Height** for the table.
11. Click **Columns** to expand the menu.
12. Select a column by clicking the column header in the table widget or by clicking its column header in the Header.
13. Set the properties for the columns:

- **Header**  
Sets the header of the selected column.
- **Width**  
Sets the width of the selected column.
- **Data Type**  
Defines the column data as alphanumeric strings or as numbers.
- **Visible**  
Shows or hides a column in the widget. With the column header selected in the Properties column, click on the **On/Off** button to hide or display the column data. An icon () beside the properties header indicates that the column is hidden in the widget.
- **Renderer**

Sets the format for data display for the selected column. Choose the type of renderer from the pull-down menu. The available column properties depend on the type of renderer selected.

– **Bar:**

- **Show Value**  
Turns on or off the display of the numeric value next to the bar in the column.
- **Minimum**  
Sets the minimum value to display for the bar.
- **Maximum**  
Sets the maximum value to display for the bar.
- **Bar Color**  
Sets the color of the bar.
- **Bar Color Map**  
Sets different colors for different values. For example, for a bar displaying percent, you can set 90 percent to red and all values of 90 percent or greater are displayed in red in the bar. Click the plus sign to add more color settings.

– **Gauge:**



Sets the shape of the gauge, semicircle, or circle.

- **Min**  
Sets the minimum value to display for the gauge.
- **Max**  
Sets the maximum value to display for the gauge.
- **Default Color**  
Sets the color to use to indicate the position of the gauge.
- **Color Map**  
Sets different colors for different values on the gauge. For example, for a gauge displaying percent, you can set 90 percent to red and all values of 90 percent or greater are displayed in red on the gauge. Click the Add button to add more color settings.

– **Image:**

- **Default Image**  
Sets the image to display in the column. Click in the **Default Image** field to display the Image Gallery. To add an image to the Image Gallery, click **Upload Image** and browse to the image.
- **Stretch to fit**  
Sizes the image to fit the frame of the widget. Click the button to turn this on.
- **Image Map**  
Click the Add button to add different images to be displayed for different data values. For example, for a column displaying percent, you can set 90 percent to an image of a warning icon and all values of 90 percent or greater are displayed as the warning icon in the column.

– **Link:**

Click the open row or on the Add button to create a URL link to navigate to a website or to another dashboard. All entered URL addresses appear in a drop-down list when you right-click anywhere in the dashboard in **Live view** mode. An external URL opens a new page in a browser.


– **Text:**

- **Font Size**  
Sets the size of the text font.
- **Color**  
Sets the color of the font. Click in the **Color** field to display a color picker. Use the slider on the right of the color picker to set the opacity for the color.
- **Color Map**

Sets different colors for different values. For example, for a column displaying percent, you can set 90 percent to red and all values of 90 percent or greater are displayed in red in the column. Click the plus sign to add more color settings.

- **Sort**

Column data is sortable as alphanumeric strings or as numbers. In the dashboard widget, click on the column header once to sort in ascending order, a second time to sort in descending order, and a third time to return to the default order. An arrow appears beside the column header to indicate an ascending or descending column data sort.

- From 20.3.0, you can export the widget data to the CSV file. Click Export Data (  ) to export the widget contents into the CSV file.

**NOTE**

Only nimbus users with dashboard design permission can export the dashboard data. You can only export the list and SQL data.

To add links to an SQL table, see [Create and Assign the Data Source for a Widget](#).

### **Add a List Widget**

You can add a List widget to the dashboard to provide a quick view of computer systems and performance in numeric or graphic format. You can use the List widget to add detail to dashboard widgets displaying, for instance, alarms or gauges.

**Follow these steps:**

1. Click on the **Widgets**



icon at the upper right to bring up the list of widgets.

2. Drag a **List** widget icon onto the dashboard.



### **Filter Systems for Display**

When you drag the List widget to your Dashboard, the List Designer screen starts automatically. You can create filters to populate the list and test the filters within the screen before applying them to the list. Common filters include systems and devices.

Operators in the filters include:

- and/or
- not
- is/contains/starts with/ends with/in

**Follow these steps:**


- Define a filter using the dropdown menus and text fields.
- Add another filter by clicking on the **Add filter** (  ) icon on the right side above the filter list.
- Delete a filter by clicking on the **Delete filter** (  ) icon to the right of the filter.
- Reorder the filters by dragging a filter box up or down in the list of filters. If you are reordering the first two filters, the "and/or" expression automatically moves to the second filter box; otherwise, the "and/or" expression will stay with its filter.
- Test the filters by clicking on the **Test Filters** button at the lower-left corner of the window.
- Click on the **Next** button at the lower-right corner of the screen.

The filter screen disappears and the list layout screen appears.

## Format the Display

Once you have defined the system data, you can format the display of that data. The screen creates the rows necessary to hold the information from the previous screen. The first data column is by default the system field and shows the results of the filter test. You can add data columns as necessary.

### To define the data layout:

1. Click on the **Add Column** () icon. A data column is added to the list.
2. Enter the column definition fields from the dropdown menus at the bottom of the screen:
  - Column Header
  - Column Type
  - Renderer Type
  - Metric (metric types contain their own dropdown menus, and an additional metric filter can be entered)
  - Renderer Properties
3. Click on the **Edit Column**, to modify an existing metric parameter. Additional display parameters can be defined at the bottom of the screen. To move between parameters for each column, click in the column display at the top of the screen. Table characteristics (number and height of rows) can be adjusted through the **Table Properties** tab. The screen displays a sample of the output so you can make changes before committing to the dashboard.
4. From 20.3.0, an option **QOS** is listed in the **Column Type** field. When you select the QOS option, another field **Select Target** appears prompting you to select the server whose metric you want to view. Select the target and click **Save**.

#### NOTE

Targets list includes \$HOST, \*, and other targets from the existing QOS that belongs to the filtered computer systems.

- If target is selected as \$HOST, it considers all the QOS with targets of the same name as device name.
- If target is selected as \*, it matches any QOS with the target and displays the maximum (sample\_value) of all the selected QOS with any target.

5. Once the output is acceptable, click **Finish**. The List widget is added to your dashboard.

6. For 20.3.0, click the Export Data () option to export the widget contents into a CSV file.

#### NOTE

Only nimbus users with dashboard design permission can export the dashboard data. You can only export the list and SQL data.

7. You can rerun the list filters on the List widget by clicking the Reload Data



icon or can edit the widget by clicking the Open Wizard



icon, both on the tab at the upper-right side of the widget.

## Add Text

A text widget allows you to place text on the dashboard.

A text widget is different from a widget label. Use a label to assign a title or name to a widget. Use a text widget instead of a label if you want to:

- Use standalone text.
- Use a different text format, such as date or numeric.
- Assign a different data source to the text than the widget.
- Set properties for the text separately from the widget.

For example, using a text widget allows you to position the text independently of the widget or to apply a shadow to the text box rather than to the widget.

There are two types of variables you can use in text widgets:

- \$VAR - Use this to display the current value of the data source.
- Parameters - Use variables that you created in the



(Parameters) tab.

The text widget supports the following data sources:


- Alarm
- Metric
- Probe
- QoS
- SLA
- SQL

#### Follow these steps:

1. Click the **Widgets**



icon in the right pane.

2. Click **General** to expand the menu.
3. Drag a text widget onto the canvas.
4. Click the text widget to select it.
5. Click the **Widget Properties** () tab.
6. Click **Text** to expand the menu.
7. Choose the text format that you want from the **Type** menu. Additional menu items associated with the chosen text type is displayed.
  - **Date**  
Sets the format for the text as *mm/dd/yy hh:mm* by default.
  - **Show natural date**  
Communicates time in "natural" language, for example: "Yesterday".
  - **Use current date and time**  
Continuously displays the current date and time.
  - **Date Format**  
Sets your preferred format.
  - **Time zone**  
Sets your preferred time zone.
  - **Numeric**  
Sets the value based on the following fields:
  - **Default Number**  
Sets the initial number value.
  - **Fixed Decimal Places**  
Sets the number of places to the right of the decimal. The value is rounded to the number of decimal places specified.
  - **Unit Multiplier**  
Sets the number that the numeric value is multiplied by.
  - **Unit Divisor**

- Sets the number that the numeric value is divided by.
  - **String**  
Sets the text format as alphanumeric, which accepts all character keys on the keyboard.
  - **Default Value**  
Sets the initial character string. You might also set this value by double-clicking the widget on the canvas and entering text.
  - **Font Size**  
Sets the size of the text.
  - **Word Wrap**  
Turns the word-wrap feature on or off. When on, text that is too wide for the text widget is displayed on multiple lines. When off, text that is too wide for the text widget is displayed on a single line with an ellipsis (...) indicating that not all text is visible.
  - **Text Vertical Alignment**  
Defines whether the text appears at the top, middle, or bottom of the text box.
  - **Text Color**  
Sets the color of the text. Enter a hex code, or click in the **Text Color** field to display a color picker. Use the slider on the right of the color picker to set the opacity for the color.
  - **Background Color**  
Sets the background color for the text widget. Enter a hex code, or click in the **Background Color** field to display a color picker. Use the slider on the right of the color picker to set the opacity for the color.
8. (Optional) Set a background image for the text widget:
- a. Click **Background Image** to expand the menu.
  - b. Click in the **Image** field to display the Image Gallery.
  - c. Click an image to select it. To add an image to the Image Gallery, click **Upload Image** and browse to the image.
  - d. Click **Select**.

The image is displayed in the text widget. By default **Stretch to fit** is off. To size the image to fit the frame of the widget, click the button to turn this function on.

You can now assign a data source to the text widget. Depending on the assigned data source type, you can define additional properties on the **Widget Properties** tab, such as a color map using the **Color** menu or an audio notification using the **Sound** menu.

### **Add a Gauge**

Add a gauge widget to display a data value within a semi-circular or circular needle gauge in the dashboard.

The gauge widget supports the following data sources:

- Metric
- Probe
- QoS
- SLA
- SQL

### **Follow these steps:**


1. Click the **Widgets**



icon in the right pane.

2. Click **Gauges** to expand the menu.
3. Drag a gauge onto the canvas.
4. Click the gauge to select it.



5. Click the **Widget Properties** (  ) tab.
6. Click **Gauge** to expand the menu.
7. Set the properties for the gauge:



- Sets the shape of the gauge: semicircle or circle.
- **Min**  
Sets the minimum value for the gauge.
- **Max**  
Sets the maximum value for the gauge.
- **Unit Divisor, Unit Multiplier**  
Performs calculations on the data before displaying the value. For example, a value reported in bytes per second can be displayed as bits per second by setting the Unit Multiplier to 8 and the Unit Divisor to 1.
- **Default Color**  
Sets the color to use to indicate the position of the gauge.
- **Color Map**  
Sets different colors for different values on the gauge. For example, for a gauge displaying percent, you can set 90 percent to red and all values of 90 percent or greater are displayed in red on the gauge. Click the plus sign to add more color settings.
- **Decimal Places**  
Sets the number of decimal places that are displayed on the gauge. Add decimal places to see finer grained measurements. For example, for a metric that has a minimum value of 0 and a maximum value of 5, you may want to add a decimal place so that the gauge needle displays a more precise position. However, for percentages, with a minimum value of 0 and a maximum value of 100, you might want to leave the decimal places set to 0.

You can now assign a data source to the gauge or change properties such as the label, size and position.



### **Add a Linear Gauge**

Add a linear gauge to display a data value within a thermometer-style gauge. This gauge can be oriented vertically or horizontally.

The linear gauge widget supports the following data sources:

- Metric
- Probe
- QoS
- SLA
- SQL

### **Follow these steps:**

1. Click the **Widgets** (  ) icon in the right pane.
2. Click **Gauges** to expand the menu.
3. Drag a linear gauge onto the canvas.
4. Click the linear gauge to select it.
5. Click the **Widget Properties** (  ) tab.
6. Click **Gauge** to expand the menu.
7. Set the properties for the linear gauge:
  - **Vertical**

- Defines whether the gauge is vertical or horizontal. Turn on for a vertical gauge, off for a horizontal gauge.
- **Ticks Visible**  
Defines whether ticks (lines) indicating unit intervals are shown.
- **Labels Visible**  
Defines whether labels for the ticks are shown.
- **Labels Size**  
Sets the size of the numbers on the gauge.
- **Labels Offset**  
Sets how far from the ticks, and on which side, the numbers are displayed.
- **Min**  
Sets the minimum value for the gauge.
- **Max**  
Sets the maximum value for the gauge.
- **Unit Divisor, Unit Multiplier**  
Performs calculations on the data before displaying the value. For example, a value reported in bytes per second can be displayed as bits per second by setting the Unit Multiplier to 8 and the Unit Divisor to 1.
- **Bar Thickness**  
Defines the width of the bar that indicates the value.
- **Bar Offset**  
Sets where the bar is displayed.
- **Tick Size**  
Defines the vertical length of the ticks.

You can now assign a data source to the linear gauge or change properties, such as its label, size, and position.

### **Add a Line Chart**

Add a line chart to display a graph of data in the dashboard.

The line chart widget can display data series for one or more data sources. Data that are collected while a data source is in maintenance mode displays in the chart with a gray overlay.

The line chart widget supports the following data sources:

- Metric
- QoS
- SQL query


SQL data sources must contain data from two columns in the SQL query: a timestamp (date/time or milliseconds) column and a values column.

### **Follow these steps:**

1. Click the **Widgets**



icon in the right pane.

2. Click **Charts** to expand the menu.
3. Drag a line chart onto the canvas.
4. Click the chart to select it.
5. Click the **Widget Properties** (  ) tab.
6. Click **Chart** to expand the menu.
7. Set the properties for the chart:
  - **X-Axis Label**

- Displays a label for the x- (horizontal) axis. The x-axis displays the time interval for the chart.
- **Y-Axis Label**  
Displays a label for the y (vertical) axis. The y-axis displays the unit for the QOS measurement.
  - **Series Duration in Hours**  
Sets the number of hours of data that are displayed, ending with the current full hour. For example, if the current time is 10:15 and you set the duration to 4 hours, data from 6:00 to 10:00 is displayed.
  - **Min Value**  
Sets the minimum value to display on the y-axis. If no value is entered, the chart will use autoscaling to define the range.
  - **Max Value**  
Sets the maximum value to display on the y-axis. If no value is entered, the chart will use autoscaling to define the range.
  - **Timezone**  
Sets the time zone for the chart.
8. Click **Series** to expand the menu.
  9. Click the **Add** (+) sign to add a data series to the chart.
  10. Click the name of the data series to select it.
  11. Enter a name for the data series.
  12. Set the properties for the data series:
    - **Series Data Source Type**  
Sets the type of data source for the selected data series.
    - **Series Data Source Name**  
Sets the data source for the selected data series. If no data sources are listed in the pull-down menu, [create the data sources for the chart](#).
    - **Display Type**  
Sets the type of chart to display for the selected data series: area, line, or plot.
    - **Color**  
Sets the color for the selected data series. Click in the **Color** field to display a color picker. Use the slider on the right of the color picker to set the opacity for the color.
    - **Size**  
Sets the size of the line or plot points for the selected data series.
    - **Drop Shadow**  
Turns on or off the display of a shadow below the selected data series.
    - **Unit Multiplier, Unit Divisor**  
Performs calculations on the data before displaying the value. For example, a value reported in bytes per second can be displayed as bits per second by setting the Unit Multiplier to 8 and the Unit Divisor to 1.
  13. (Optional) Create additional data series.
  14. (Optional) Use the up and down arrows to move the selected data series up or down in the list.  
If data for multiple data series overlaps, the series highest in the list is displayed. For example, if you have a data series measuring CPU usage for the user and a data series measuring CPU usage for the system, and the values for both are 0 for the time interval, the data for the data series that appears first in the list is displayed.

You can now change other properties for the line chart, such as its label or size and position.

### **Add a Pie Chart**

Add a pie chart to display a percentage distribution chart in the dashboard.

The pie chart widget supports the following data sources:

- SQL

**WARNING**

You must use an SQL data source where the query returns at least two columns of information. The first column must be a label, the second column a quantity. The following example shows a database query that returns the severity (label) and count (quantity).

```
SELECT
 severity, count(severity)
FROM
 nas_alarms
GROUP by severity
```

**Follow these steps:**1. Click the **Widgets**

icon in the right pane.

2. Click **Charts** to expand the menu.

## 3. Drag a pie chart onto the canvas.

## 4. Click the chart to select it.

5. Click the **Widget Properties** () tab.

## 6. (Optional) Add a legend to the pie chart:

a. Click **Pie** to expand the menu.

b. Click the **On/Off** button next to **Legend** to set whether the legend displays or not.

## 7. (Optional) Display labels on the pie chart:

a. Click the **On/Off** button next to **Pie Labels** to set whether labels display or not.

b. When labels for the pie chart are shown, click **Pie Labels** to expand the menu.

c. Set the properties for the labels in the pie chart, such as alignment, font size, font color, or background color.

## 8. (Optional) Add a label for the pie chart:

a. Click **Label** to expand the menu.

b. You can now add or change the label properties.

## 9. (Optional) Change the size or position of the pie chart in the dashboard:

a. Click **Size & Position** to expand the menu.

b. You can now set the size or position properties of the pie chart.

You can now assign a data source to the pie chart or change the widget properties.

**Add a Context Selector**


Add a context selector widget to the dashboard to display data in other widgets dynamically. Use of context selectors allow you to view data otherwise requiring multiple dashboards.

Context selectors include a time selector, custom selectors, and dashboard links. The Time selector passes time values that are used by dashboard SQL data sources. A custom selector passes values from a URL link, SQL query, or static table as SQL parameters to other dashboard widgets. A Dashboard selector passes context values to other dashboards with common parameters.

You can use the time selector to view data for one particular time interval and then change the parameter to view the same data for a different time interval. You can use the custom context selector to switch dashboard SQL parameters at runtime. You can use the dashboard selector to pass parameters from one dashboard to other dashboards in order to view data in series.

**Follow these steps.**

**For a Time selector:**



1. Click the **Widgets**  tab.
2. Click **General** to expand the menu.
3. Drag the **Context Selector** widget onto the canvas. The **Time** selector is the default.
4. Pull down the dropdown menu for the **Time** selector (the default) and click on a time period.

**NOTE**

Dropdown selections within the Time selector perform parameter substitution within dashboard SQL queries on the start and end times in milliseconds since epoch. The format for the parameters in the SQL query is `${startTime} ${endTime}`. For example, the following SQL query can be defined through the Advanced Data Sources tab and assigned to a widget and time values assigned at runtime: the base query displays the names of resources that are in the UIM inventory and the Time selector allows you to filter by date.

```
select name, create_time from cm_computer_system where
create_time > dateadd (SECOND, ${startTime}/1000, '1970-1-1') and
create_time < dateadd (SECOND, ${endTime}/1000, '1970-1-1') and
origin = '${originTag}'
```

At runtime, the `${startTime}` and `${endTime}` values are taken from the Time selector selection. Remember that SQL data returned is limited by the type of widget used.

5. Click the **Widget Properties** () tab and the Add context selector () icon to add a context selector.
6. Click on the type of column being added:
  - Custom
  - Dashboard
7. Double-click on the header name for the context selector in the Properties column to change the header name.
8. Insert the parameter name for the column value.

**NOTE**

Custom context selections take precedence over any parameter that might be defined elsewhere with the same name.

9. For a Custom context selector, click on the option button for the data source type:
  - URL
  - SQL
  - Manually entered values

**For a website location:**

- a. Enter the URL for an external REST web service.

**NOTE**

An external web service for a URL data source must:

- Accept a GET request to the specified URL.
- Return a JSON string that includes the label and value for each entry in the required format.

For example:

```
[
 {
 "label": "foo",
```

```

 "value": "bar",
 "children": [
 {
 "label": "foochild",
 "value": "barchild"
 }
]
 }
]

```

**For an existing SQL query:**

- a. Click on the dropdown list in the **Database** section.
- b. Click on the name of an existing SQL query.

**For a new SQL query:**

- a. Click Add button.
- b. In the dialog box, enter a name for the query in the **Name** field.
- c. Click on the **Database** for interest.
- d. Enter a query in the **Query** field.
- e. Click on **Test Query**.
- f. If the query does not return a failure message, click **Save**.

**NOTE**

Custom SQL context selectors require one or two data columns. The data appear under one of these conditions:

- The SQL query returns a single column of data when the column is used for both a label and a value.
- The SQL query returns two columns of data for a label and value pair.
- The SQL query returns the first two columns of data where more than two columns are queried.

**For manually entered values:**

- a. Type the label and values into the open fields in the **Properties** column.
- b. Click on the context selector pulldown menu and the label for the desired value.

10. Click on **Dashboard, Live View** to view the data results.

When both dashboards contain common custom context selectors (such as the Time selector), the value from the custom context dashboard is passed to the linked dashboard. Custom context selector values in a linked dashboard can be set to another value, but those new values are not passed back to the previous dashboard.

The Dashboard selector allows you to navigate between dashboards during runtime. The list of available dashboards can be limited to a specified folder.

**For a Dashboard selector:**

1. Click on the header for the **Dashboard** selector.
2. Click on the dashboard folder in the **Dashboard Folder** section.
3. Click on the dashboard of interest.
4. Click on **Live view**.
5. Click on the **Dashboard** selector to navigate to the linked dashboard. Parameters from the linking dashboard are automatically passed to the linked dashboard.

A list of substituted values is displayed in the Inherited section under the **Parameters** tab. The sequence of opened dashboards appears beside the **Modes** menu in the top-center tab of the **Live view** window.

**NOTE**

A list of substituted parameters in linked dashboards are displayed in the Edit mode, under the **Parameters** tab, in the Inherited section.

## Create and Assign the Data Source for a Widget

In order for widgets to display data, assign a data source. First create a data source, then drag-and-drop the data source onto widgets.

Once created, data sources are available to any of the widgets on the dashboard, and a single data source can be assigned to multiple widgets.

**NOTE**

Data sources are specific to a dashboard and must be created for each new dashboard. However, a dashboard with data sources that is saved with another name retains the data sources.

Available data source types are:

- Alarm
- Dashboard
- Metric
- SLA/SLO

Other advanced data sources that require special knowledge, such as familiarity with your environment or with creating database queries. Advanced data sources are:

- Probe
- QoS
- SQL

**NOTE**

Not all widgets support all data sources. When you drag a data source onto a widget, the widget border turns green if the widget supports the type of data source and turns red if it does not.

### Contents

#### **Create an Alarm Data Source**

Create an alarm data source to display the highest data severity condition.

To specify alarm criteria, create a filter that defines which alarms to include. This filter is separate from alarm filters that are defined for the user's access control list (ACL) in the Account Admin view.

For example, if account contact users are restricted in their ACL to seeing only alarms from a particular hub, only these alarms are included in alarm data that are displayed by Dashboard widgets. In the Dashboard view, the administrator creating the dashboard can further limit the alarm data that are displayed for particular widgets, such as including only alarms from a particular subsystem. This selection is done by defining a filter when you create an alarm data source.

**NOTE**

Alarm filters for ACLs might also be defined in Infrastructure Manager, but these filters are not applied in the Dashboard view. We recommend using the Account Admin view to manage accounts, users, and ACLs.

**Follow these steps:**

1. In the right pane, click the **Data Sources**



tab.

2. Click **Alarm**, then click the **Add** icon.

3. Enter information in the fields of the dialog to create the filter:

- **Name**

Enter a name for the data source.

- **(blank) or not**

Choose **not** to search for all systems except those systems that meet this row of the filter definition. Otherwise, leave this field blank.

- **Select a field for filtering**

Choose the criterion to filter on, such as Hostname, Source, and Message.

- **Select operator**

Choose the appropriate operator, such as **is**, **contains**, **starts with**, **ends with**, or **matches**.

**NOTE**

From UIM 20.3.3, the **matches** operator is no longer available. Therefore, if you are using the **matches** operator in your existing dashboards, you must update the alarm filters. Otherwise, you might not get the desired output.

- **Text field**

Enter the appropriate text for the criterion you chose. You can enter regular expressions in this field.

**NOTE**

Alarm filters use the Java RexEx pattern format. For a full list of supported constructs, see the [Java documentation](#).

- **Plus/Minus Sign**

Click to add or remove rows for the filter definition.

4. Click **Test Filter**. Alarms that match the filter are listed. Verify that the results are as expected and adjust the filter if necessary.

5. Click **Create**.

**Create a Dashboard Data Source**

You can use a dashboard with alarm data sources as a data source for another dashboard. Create this type of data source if you want to drill down from one dashboard to another. The parent dashboard displays the highest severity alarm from the child dashboard.

**NOTE**

The dashboard data source is supported only for dashboards with alarm data sources.

Use this functionality to logically group elements together, emphasizing the geographical, topographical, structural, or organizational placements of monitored systems.

For example, you have a dashboard named Regions with widgets that show the alarm status for North America, Asia, Europe, Africa, and Latin America. You create a child dashboard named North America that shows the alarm status for West Coast, Midwest, and East Coast. In the Regions dashboard, you assign the North America dashboard as a data source for the North America widget. When you see an alarm status of major for North America in the Regions dashboard, hover over the North America widget and click the link to the North America dashboard in the tooltip. This opens the North America dashboard, where you can see which area of North America generated the major alarm.



**NOTE**

The tooltip with the drill-down link for a dashboard data source is displayed only in Live View or in a published dashboard. It is not displayed in Edit mode.

Publish the parent and child dashboards with the same visibility setting (private, public, or account). For example, if you publish the parent dashboard as an account dashboard and the child dashboard as private, account contact users cannot drill down from the parent to the child because they do not have permission to view the child dashboard. Publish the child dashboard again and change the visibility setting to match the parent dashboard.

You must republish a dashboard for a new visibility setting to take effect.

**Follow these steps:**

1. In the right pane, click the **Data Sources**



tab.

2. Click **Dashboard**.

Your dashboards are listed as data sources.

**Create a Metric Data Source**

Create a Metric data source if you want widgets to display the current metrics being monitored on a system.

Metric sources are listed in a hierarchical tree. Data is grouped under either the **Groups** or **Other** nodes in the tree and **Accounts** under the **Groups** node.

1. **Groups**
  - **Accounts** - List of systems that belong to specific accounts.
  - **All** - List of systems that belong to all accounts.
2. **Other**  
List of systems that do not belong to a group.

**NOTE**

Groups and Accounts are defined by an administrator through OC. If you do not find the group or account of interest in the dropdown menus, contact the system administrator to create them.

**Follow these steps:**

1. In the right pane, click the **Data Sources**



tab.

2. Click **Metric** to expand the menu.
3. Click to navigate through the lists and display the systems with metrics available.
4. When you find the desired system name, click to select it.

**Create an SLA or SLO Data Source**

You can use a Service Level Agreement (SLA) or Service Level Objective (SLO) as a data source. Create this type of data source if you want widgets to display the compliance percentage of the SLA or SLO.

For more information about SLAs and SLOs, see the help for the SLA Reports view.

**Follow these steps:**

1. In the right pane, click the **Data Sources**



tab.

2. Click **SLA/SLO**. Your SLAs and SLOs are listed as data sources.

**NOTE**

SLAs and SLOs are defined by the system administrator through the Service Level Manager (SLM) view. If the SLA or SLO of interest is not in the list, contact the administrator to create it.

**Create a QoS Data Source**

Create a quality-of-service (QoS) data source if you want widgets to display the current value for a QoS metric.

You can display QoS metrics stored in the UIM database or in any database with a connection configured in the Java database connectivity driver (jdbc) tab of the Web Application Server Probe (wasp) configuration file.

Wasp is a probe that is distributed to the system during the Operator Console (OC) installation, and afterward appears as a probe in OC or the Admin Console. For more information about configuring a database for wasp, see the wasp probe guide.

**Follow these steps:**

1. In the right pane, click the **Data Sources**



tab.

2. If **QoS** is not listed as a data source, click the **Options**



icon and select **Show advanced data sources**.

3. Click **QoS**, then click the **Add** icon.

4. Enter information in the fields of the dialog:

- **Name**

Name for the data source.

- **QoS**

Select the QoS.

- **Source**

Select the source for the QoS metric. Typically the source is the system where the probe is running. For example, for a CPU usage metric the source is the system where the cdm probe is installed.

- **Target**

Select the target for the QoS metric. Typically the target is the system being monitored.

For example, for a CPU usage metric the target is the source where CPU usage is measured. For a URL response metric the target is the endpoint of the measurement.

5. Click **Test QoS (Single)** to view the latest value for the QoS, or **Test QoS (Multi)** to view values for the last hour.

**Test QoS (Multi)** is useful to preview data for the line chart widget.

After clicking the **Test QoS** button, you see the value and date for the metric.

6. Click **Create**.

**Create a Probe Data Source**



Create a probe data source if you want widgets to display data from a specific probe. Each probe has a set of commands you can execute by creating a probe data source.

For example, use the `get_info` command for the `cdm` probe to return various information about the system, including OS, uptime, and CPU usage.

#### NOTE

The probe data source is an advanced data source and requires knowledge of the probe command set and parameters. The probe command set can be explored using the Probe Utility. For more information about the Probe Utility, see [Use the Probe Utility](#).



#### Follow these steps:

1. In the right pane, click the **Data Sources**  tab. )
2. If **Probe** is not listed as a data source, click the **Options**  icon and select **Show advanced data sources**. )
3. Click **Probe**, then click the **Add** icon.
4. Enter information in the fields of the dialog:
  - **Name**  
Enter a name for the data source.
  - **Hub**  
Choose the hub for the probe.
  - **Robot**  
Choose the robot where the probe is installed.
  - **Probe**  
Choose the probe.
  - **Command**  
Choose the probe command to collect the data you want to display. For example, if you want to display CPU status information from the `cdm` probe, select **cpu\_status**. The `cpu_status` command collects metrics related to CPU status, such as `cpu idle`, `processor queue length`, and `cpu wait`.
  - **Parameters**  
If the probe command has parameters, enter them here.
  - **Results**  
Ignore this field until after the next step.
5. Click **Test Probe**.  
The metrics collected by the command you selected are listed in the Results table.
6. In the Results table, select the metric that you want widgets to display.  
Only results with a single value are supported. Results that return multiple objects are not supported by the probe data source.
7. Click **Create**.

#### Create an SQL Data Source

Create an SQL data source if you want widgets to display a metric from a database.

#### Follow these steps:

1. In the right pane, click the **Data Sources**  tab. )
2. If **SQL** is not listed as a data source, click the **Options**  icon and select **Show advanced data sources**. )

- Click **SQL**, then click the **Plus Sign**



icon next to the database you want to query.

- Enter information in the fields of the dialog:

- **Name**

Enter a name for the data source.

- **Database**

Accept the default (the database that is created at installation) or click on the name of another database.

- **Type**

Choose **SQL Statement** to enter an SQL query or **Stored Procedure** to execute a stored procedure.

- **Query**

Enter the SQL query or stored procedure call.

For a stored procedure call, use the following syntax:

```
exec <storedProcedureName> <parameter1> <parameter2>
```

For example, for a stored procedure named getMetrics with two parameters the syntax is:

```
exec getMetrics version_param increment_param
```

#### NOTE

Substitution parameters are available to dashboard SQL data sources, including `${username}`, `${accountName}`, `${origins}`, and `${originsSqlList}`. In this way, dashboards can support multi-tenancy: values for SQL parameters are substituted at runtime for the dashboard account user. The `${origins}` value is a comma-separated list of the user account origins. The `${originsSqlList}` value is a comma-separated list of the user account origins with single quotes ready to use in a SQL IN list.

#### NOTE

For bus (not account contact) users, `${accountName}` becomes the empty string and `${originsSqlList}` becomes the string value of two apostrophes ("").

#### NOTE

To create an SQL data source for a line chart, the query must be structured so that the first column is the timestamp for the parameter of interest *in ISO 8601 format* and the second column is the resulting value. Each data series requires a separate SQL data source with that two-column result.

- Click **Test Query**.

Results of the query are displayed. Verify the results and adjust the query if necessary.

- Click **Create**.

### Add a Database Connection for SQL Data Sources

By default the UIM database is available for creating SQL data sources. You can add other SQL databases to display data that are stored there.

#### Follow these steps:

- In the right pane, click the **Data Sources**



tab.

- If **SQL** is not listed as a data source, click the **Options**



icon and select **Show advanced data sources**.

- Click **SQL**, then click **Add** Icon above the list of databases.

The Create Database Connection dialog is displayed.

- Enter information in these fields:

- **Name**  
Name for the database connection.
  - **Driver Class**  
Defines the type of driver to use to access the database. For example, here are some possible settings:  
com.microsoft.sqlserver.jdbc.SQLServerDriver  
oracle.jdbc.driver.OracleDriver  
com.mysql.jdbc.Driver
  - **JDBC URL**  
JDBC connection URL. For example, here are some possible settings:  
jdbc:sqlserver://<dbserver>;DatabaseName=<dbname>  
jdbc:oracle:thin:@<dbserver>:CA Portal:<service name>  
jdbc:mysql://<dbserver>:CA Portal/<dbname>
  - **User**  
User name to access the database.
  - **Password**  
Password to access the database.
5. Click **Create**.
  6. Restart the wasp probe.

### **Delete a Database Connection for for SQL Data Sources**

In the event that a database connection is no longer needed for SQL queries, you can delete it.

#### **NOTE**

Deleting a database connection will affect any widgets that depend on the connection. Be sure that a connection is not used before deleting it.

To remove the connection, navigate to the wasp.cfg file in the system files and delete the database information there.

#### **NOTE**

You can view the dashboard database connections in the wasp configuration GUI but not delete it there.

### **Follow these steps:**

1. Navigate to the wasp.cfg file.  
The default location of the file is <uim\_install>\nimsoft\probes\service\wasp.
2. Open the wasp.cfg file in a text editor.
3. Scroll to the **webapps** section for **dashboard**.
4. Locate the database information under the appropriate <jdbc> tag and delete the database information.
5. Save the file.
6. Restart the wasp probe.

### **Assign a Data Source**

Assign a data source to a widget to display the current value for that data source.

#### **NOTE**

Not all widgets support all data sources. When you drag a data source onto a widget, the border around the widget turns green if the widget supports the type of data source and turns red if it does not.

**Follow these steps:**

1. In the right pane, click the **Data Sources**



tab.

Widgets that do not have a data source assigned to them are gray and have a missing data source icon overlaid on them, such as this text widget:



2. Drag a data source from the right pane and drop it onto a widget.  
The data source is now assigned to the widget.
3. (Optional) Choose **Live view** from the **Dashboard** menu to view the widget with current data.
4. (Optional) To change the data source, drag a different data source onto the widget.

**NOTE**

You can also view or assign a data source for a widget under the **Data Source** menu in the **Widget Properties** tab.

**Unassign a Data Source**

You can unassign a data source if you want no data source assigned to the widget.

**NOTE**

To change the data source assigned to a widget to another data source, assign a different data source. You do not need to unassign the current data source first.

**Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** tab.
3. Click **Data Source** to expand the menu.
4. Click the **Remove data source**



icon.

No data source is assigned to the widget. The data source that you removed is still available to assign to other widgets.

**Delete a Data Source**

Delete a data source if you no longer want it to be available to assign to widgets.

You cannot delete a data source that is in use. First verify the data source is not assigned to any widgets, then delete the data source.

**Follow these steps:**

1. In the right pane, click the **Data Sources**



tab.

2. Click on the header for the type of data source to expand the data source list.
3. Locate the data source of interest in the list. For an SQL query, click the checkbox beside a data source to select it.
4. Click the **Delete Selected Data Sources**



icon

The data source is deleted and is no longer listed in your data sources

## How to Use Parameters

You can create dashboard parameters (variables) for use in multiple widgets. This allows you to reuse widgets or data sources, updating them simply by changing parameter definitions.



The dashboard view uses both global and local parameters.

For example, you have a dashboard with three widgets displaying information about a computer system. You create a parameter named System1 and enter the host name as the value. You enter `${System1}` in the **Label** field in the Widget Properties tab for each widget. If the host name changes, or if you want to use the same dashboard for another customer, you can update the parameter value and the host name is updated in all three widget labels.

You can also use parameters when defining data sources. For example, if you have a parameter named 'Robot1' and the value is the path to the robot, you can enter `${Robot1}` as the parameter in the **Robot** field for the probe data source. If the data source changes, you can redefine it in the parameter list rather than the data source for the widget.

The text widget also supports the use of parameters.

### Follow these steps:

1. Click the **Parameters** () tab.
2. Click in the **Global** or **Local** header to expand the list of parameters.
3. Click the **Add** () icon.  
A dialog box appears.
4. Click the **Name** field and enter a name for the parameter.
5. Click the **Value** field and enter the value for the parameter. The value can be any text, such as a host name or path to a system.
6. Click the **Create** button.
7. Go to **Dashboard**, **Save** to save the parameters that you have created.
8. In the data field where you want to use the parameter, enter the parameter name preceded by a dollar sign and enclosed in curly brackets:

```
${parameter}
```


## Set the Properties for a Widget

You can set several properties for a widget, such as its name, label, position on the canvas, or a URL link.

Depending on the type of widget and the data source that is assigned, you might be able to set sounds for different data values. For image widgets, you can set images for different data values (an image map).

### Contents


#### Name a Widget

Name a widget to be able to identify it in your list of widgets in the **Navigator** () tab. If you do not enter a name, a default name, such as Circle\_0, is assigned to the widget.

#### NOTE

The name of a widget does not appear on the dashboard. To display a name for a widget, add a label for the widget.


**Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** () tab.
3. Click **General** to expand the menu.
4. Enter the name in the **Name** field.

**Label a Widget**

Label a widget to display text for the widget on the dashboard.

**Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** () tab.
3. Click **Label** to expand the menu.
4. Enter or edit text in the **Label** field.
5. (Optional) To change label properties:
  - Change the placement of the label using the **Label Position** buttons.
  - Change the font size, font color, or the background color by using the appropriate fields.


**NOTE**

To edit an existing widget label, click in the label on the dashboard. The label area is outlined in blue.

**Set a URL for a Widget**

Set a URL for a widget to display a web page when you click on the widget. You can add URL links to a widget to access information that is stored locally or remotely or to pass values to other dashboards and websites.

**Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** () tab.
3. Click **Link** to expand the menu.
4. Enter a fully qualified URL in the **URL** field.  
For example, <https://www.myserver.com>

The link type default is set to access an internal link: that is, a URL for a local dashboard or other page. The dashboard automatically passes the current user's name and password to the page to open it.


To access an external URL, select the box for **External URL**. For security reasons, the link will not pass the current user's name and password to the page. If the page requires these, they must be entered in any dialog box that appears.

**Define an Image Map for an Image Widget**

You can create an image map for an image widget.

An image map displays different images for different data values. For example, for an image widget with an alarm type data source you can display a different icon for each alarm severity level.

**Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** () tab.
3. Click **Image** to expand the menu.



4. Set the default image if you have not done so:
  - a. Click in the **Image** field to display the Image Gallery.
  - b. Click an image to select it.  
To add an image to the Image Gallery, click **Upload Image** and browse to the image.
  - c. Click **Select**.  
The image is displayed in the widget. By default **Stretch to fit** is turned off. To size the image to fit the frame of the widget, click the button to turn this on.
5. Create the image map:
  - a. Assign a data source to the image widget if you have not already done so.

**NOTE**

You can set the default image but cannot define an image map if a data source is not assigned.

- b. Click the **Add** icon to add image rows.

**NOTE**

If you assigned the alarm type data source to the widget, a field for each alarm level is displayed.

- c. Click in the image field to display the Image Gallery.
- d. Click an image file to select it.  
To add an image to the Image Gallery, click **Upload Image** and browse to the file.
- e. Click **Select**.
- f. Enter a value in the field to the right of the image field.  
This value functions as a threshold, and when the threshold is met the image is displayed. For example, if you enter 20, the default image is displayed unless the current value for the data source is 20 or greater.
- g. Repeat these steps to add as many images and associated data values as wanted.


**Set Sounds for a Widget**

For most widgets, you can play sounds for different data values.

All widgets except the table, the line chart, and the pie chart support sounds. Sounds are not available if a QoS data source is assigned to a widget.

The types of sound files you can play depend on your browser. If you want sounds to play in multiple browser types, consider using a portable format such as MP3 or ogg.

**Follow these steps:**

1. Assign a data source to the widget if you have not already done so.
2. Click the widget to select it.
3. Click the **Widget Properties** () tab.
4. Click **Sound** to expand the menu.


**NOTE**

You must assign a data source before the **Sounds** tab is displayed.

5. Click the **Add** icon to add a sound row.

**NOTE**

If you assigned the alarm type data source to the widget, a field for each alarm level is displayed.

6. Click in the left-hand field of the row to open the Sound Gallery.
7. Click an audio file to select it.
8. – To listen to an audio file, click the **Play Sound** () icon next to the file name.
9. – To add an audio file to the Sound Gallery, click **Upload Sound** and browse to the file.
10. Click **Select**.

11. Enter a value in the field to the right of the sound field.

This value functions as a threshold, and when the threshold is met the sound is played. For example, if you enter 20, the sound is played if the value of the data source is 20 or greater.

12. Repeat these steps to add a sound for each threshold level that you want a sound notification for.

### **Add Links to a Table**

You can add dashboard and URL links to an SQL table to access information that is stored locally or remotely or to pass values to dashboards and websites. You can add a link to the table as a whole or to any column in the table. A linked dashboard appears in the current window. A URL linked to a table opens the website in a new browser tab.

Links can also be used to pass table values as part of the URL or to parameters in the linked dashboard. The link can pass values from any column in the table.

### **Add a URL Link to a Column**

For a URL link to a column, value substitution appends column values to an SQL query. For example, values from the second table column are appended to the URL for Google in the format:


```
http://www.google.com?q=$2
```

When a user clicks a link in the table, the designated column value is added to the end of the URL.

Values in one dashboard can be passed to another dashboard to view related data. When a user clicks in a cell of the linked column of the table, the designated column value in the same row is passed to the linked dashboard for the same parameter name.

The names of linked dashboards are displayed in the Modes dropdown menu. Passed parameters and values are listed under the Parameters tab.

### **Follow these steps:**

1. Click the table widget to select it.
2. Click the **Widget Properties** () tab.
3. Click a table column
4. Pull down the **Data Type** menu and click on the type: **Number** or **String**.

#### **NOTE**

The table allows you to do sorting on a column based on the format of the data. Select the type appropriate to the data..

5. Click the **Visible** button to show or hide the column in the dashboard.
6. Click the **Renderer** pulldown menu and click on **Link**.
7. Click the **Type** pulldown menu and click on **URL**.
8. Under **URL**, enter the URL and any column designations to be passed as part of the URL.  
If the URL is for a page within Operator Console (OC), such as a Performance Reports Designer report, you can use a relative URL. Otherwise, use a fully qualified URL (such as <http://www.mypage.com>).  
For a URL, use the syntax `?<getVariable>=${parameterName}` in the URL. For example, to append a value in the fourth column of the table to the URL, enter `?q=$4` in the URL, as in: [http://www.Google.com?q=\\$4](http://www.Google.com?q=$4)

#### **NOTE**

Multiple parameter substitution can be used to populate the URL. For example, the link to append values from the third and fifth columns of the table to the URL would have the following syntax:

```
http://www.google.com?p=$3&q=$5
```

**NOTE**

To support a single-login option for Operator Console (OC) applications, insert *\$persistLogin* as part of the the URL.

Example:

```
http://www.mypage?sid=$persistLogin
```

- Under **URL Request Method**, pull down the menu and click on GET or POST.

**NOTE**

External websites will accept either GET or POST queries but not both. A failure in either of these request methods will generate a 404 failure code in the new browser window.

- To enter a URL link available from anywhere in the dashboard, click **Links** to expand the menu.
- Click the **Add** icon to add a links row.
- Enter a name for the link and the URL for that name.
- Switch to **Live view** mode or publish the dashboard.
- Left-click in a linked cell of the table to open the website in a new tab.  
The specified URL is displayed in a new window.

**Add a URL Link to a Table**

A table can contain multiple URL links. The specific link can be selected from a pop-up menu at runtime.

**To create the table link:**

- Switch display modes to **Edit**.
- Click the table to select it.
- In the **Properties** tab, click on Links.
- Click the **Add** link icon (the plus sign) to enter a URL.
- Click in the open column and enter the name and URL for a link. The name of the link appears in the pop-up box to activate the URL link.
- Click the **Add** link icon (the plus sign) to add another URL.

The URLs are associated with the table but are run from anywhere in the dashboard.

**To activate the link:**

- Pull down the Dashboard menu in the upper-left corner of the dashboard and select **Live view**.
- Right-click anywhere in the dashboard to open a website in a new tab.
- Click the link name in the pop-up menu.

The link opens a tab in a browser window.

**Add a Dashboard Link to a Table**

You can create links to other dashboards within a table widget. These links can be used to pass values between dashboards.

**NOTE**

When assigning dashboard data sources to widgets, avoid creating a circular reference within the dashboards. Circular references result in no data propagation to the dashboard data source and cause potential performance issues with dashboard data retrieval.

**Follow these steps:**

1. Click the table widget to select it.
2. Click the **Properties** tab.
3. Click a table column
4. Pull down the **Data Type** menu and click on the type: **Number** or **String**.

**NOTE**

The table allows you to do sorting on a column based on the format of the data. Select the type appropriate to the data.

5. Click the **Visible** button to show or hide the column in the dashboard.
6. Click **Links** to expand the menu.
7. Click the **Add** icon to add a links row.
8. Click the **Renderer** pulldown menu and click on Link.
9. Click the **Type** pulldown menu and click on Dashboard.
10. Click the **Dashboard** target name.
11. Click the **Parameters** to be passed to the target dashboard.
  - The **Name** column is the common parameter name in the dashboards.
  - The **Value** column indicates the table column value to be passed to the child dashboard for the parameter using positional substitution (for example: for the name/value pair  $x/\$3$ ).
12. Click the **Add** icon to add another parameter and table column.
13. Switch to **Live view** mode or publish the dashboard.
14. Click in a linked cell of the table. The linked dashboard is displayed in the existing window.
15. Click the **Parameters** tab to view global, inherited, and local parameters and values.

To return to the parent dashboard, pull down the tab at the center-top of the window and select the parent directory name.

**Set Display Properties**

Once a data source has been applied to a widget, you can customize the widget properties to make the data view meaningful. Properties include setting alarm colors and thresholds and defining ranges for data collection and display. The following instructions do not address all widget properties but represents basic formatting functions that can be applied to various widgets.

**Define Alarm Thresholds**

Shape and gauge widgets can both display alarm states by color. You can change the default color for the widget and threshold values to display different alarm states in those widgets.

**Follow these steps:**

- Click an alarm widget to select it.
- Click the **Widget Properties** icon at the top of the widgets column.
- Click the **Color** heading to open the menu.
- Click the default color square to redefine the default color.
- Drag the slider bar for the color map to the desired range and click in the color map to select a color.
- Drag the slider bar for the transparency setting to change the transparency of the widget color.

This changes the default color for displaying all data values. You can add as many more colors and thresholds as necessary to display alarm states.

**Follow these steps:**


- Click the **Plus** sign in the menu.
- Repeat the previous steps to select a new color.
- Insert a threshold value for each color based on the system's parameters.
- Repeat these steps to create more colors and threshold values.

Threshold values are given as lowest values for the data display. Each color replaces the previous color when the value is reached, so there is no need to insert a range for the alarm state. The alarm widget displays the color that corresponds to the returned data when the dashboard is viewed in Live view mode.


### **Define Display Ranges**

You can change the details of the display for gauges and charts in the Widget Properties menu.

#### **For a gauge, follow these steps:**

- Click a gauge to select it.
- Click the **Widget Properties** icon (  ) at the top of the widgets column.
- Click the **Gauge** heading to open the menu.
- Click the buttons to change the gauge orientation and visibility settings.
- Enter values to change the display units for the gauge.

#### **For a chart, follow these steps:**

- Click a line chart to select it.
- Click the **Widget Properties** icon (  ) at the top of the widgets column.
- Click the **Chart** heading to open the menu.
- Click the up and down arrows for **Series Duration in Hours** to change the time period for the chart.

#### **NOTE**

The chart adjusts the increment for the selected range according to the chart size. Above 47 hours, the x-axis displays dates for the data.

- Click the up and down arrows for **Min Value** and **Max Value** fields or enter values to change the display units for the chart.

#### **NOTE**

If you do not enter a minimum or maximum value, the chart automatically scales the y-axis to center data.

- Hover the cursor over the chart to display times and units within the report period and value range.

## **Change a Dashboard Widget on the Canvas**

Several tools to help you manage widgets on the canvas. You can clone widgets, move them to the front or back, or select multiple widgets.

You can also do other common tasks such as aligning widgets, changing the type of widget, or deleting widgets.

### **Contents**

#### **Position Widgets**

Use these tools to position widgets:

- Guide lines
- Arrow keys on the keyboard
- x and y positions


Generally, it is easiest to position and align widgets by dragging them into place with the help of the guide lines.

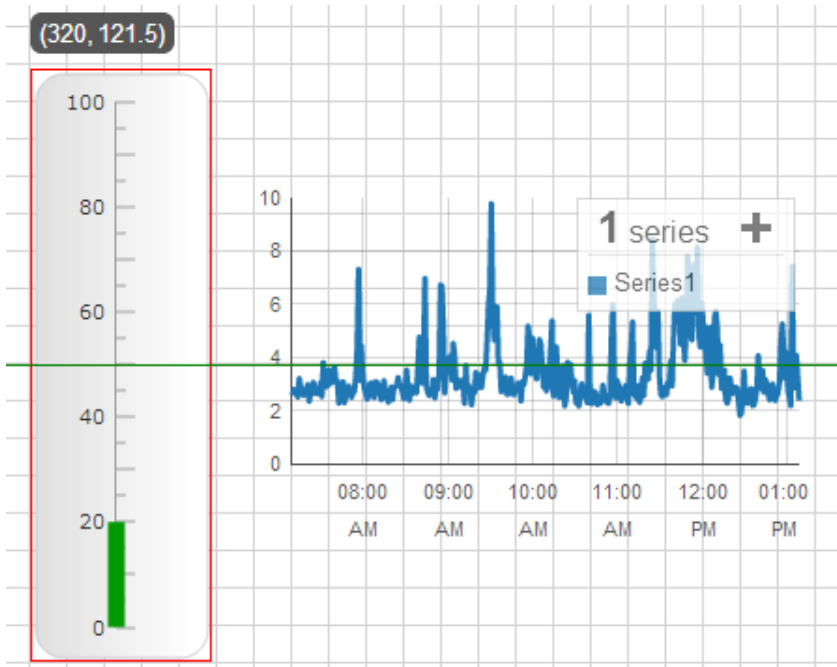
You can also position widgets using the arrow keys on your keyboard or by entering the x and y position.

### **Position Widgets Using Guide Lines**

Align widgets by using the guide lines. The guide lines show you when the edges or centers of widgets are aligned.

#### **Follow these steps:**

1. Click the **Toggle Guide Lines** (  ) icon to turn guidelines on if they are not already on. If the background of the icon is blue, guidelines are turned on.
2. Drag the widgets to position them where you want them. As you drag a widget, a green guide line appears when widgets are aligned. The guide lines indicate when widgets are aligned horizontally or vertically. For example, the green line in the following image indicates that the centers of the linear gauge and line chart are aligned horizontally.



### **Position Widgets Using Arrow Keys**

To position widgets from your keyboard, select one or more widgets, then press the arrow keys.

Depending on the settings you select, you can use the arrow keys to nudge widgets a pixel at a time or to move them quickly across the canvas.

| Action                   | Widget Behavior                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Press arrow key          | If snaptogrid is turned on - moves the distance of one grid square. For example, if the grid spacing is set to 20, the widget moves 20 pixels each time you press the arrow key.<br>If snap-to-grid is turned off - moves 1 pixel<br>To adjust the grid spacing or to turn snap to grid on or off, go to the <b>Grid</b> menu in the <b>Canvas Properties</b> tab. |
| Press and hold arrow key | Accelerates movement                                                                                                                                                                                                                                                                                                                                               |
| Ctrl + arrow             | Snaps into alignment with the closest widget                                                                                                                                                                                                                                                                                                                       |
| Shift + arrow            | Moves 10 pixels                                                                                                                                                                                                                                                                                                                                                    |

#### Follow these steps:

1. Click a widget to select it, or drag the mouse to draw a box around multiple widgets to select them.
2. Press an arrow key.

#### Position Widgets Using x and y Settings

The x and y settings allow you to position widgets precisely.

The x and y settings for a widget are displayed as you drag it around the canvas.

#### Follow these steps:

1. Click the widget to select it.
2. Click the **Widget Properties** tab.
3. Click **Size & Position** to expand the menu.
4. Enter settings in the **X Position** and **Y Position** fields.

#### Move a Widget to the Front or Back

You can move overlapping widgets to the front or back on the canvas.

#### Follow these steps:

1. In Edit mode, click the widget that you want to move.
2. Do one of the following actions:
  - To move the widget all the way to the front or back, click **Move to front** or **Move to back** on the toolbar.
  - To move the widget one layer at a time to the front or back, select **Move forward** or **Move backward** from the pull-down menus on the toolbar.

#### Clone a Widget


Clone a widget to duplicate the widget and its properties.

#### Follow these steps:

1. Click the widget to select it.

#### **NOTE**

Select multiple widgets by dragging the cursor around the widgets and releasing.

2. Click the **Clone**  icon on the toolbar.
3. Select **Live View** from the **Dashboard** drop-down. The data is displayed in the cloned widget.
4. Save the dashboard.

### **Multi-Select Widgets**

You can select multiple widgets. You can then move the widgets as a group or clone or delete all selected widgets.

#### **Follow these steps:**


1. In Edit mode, drag the cursor around the widgets on the canvas and release.

#### **NOTE**

You can also select a widget, then use Ctrl + click to select additional widgets.

The widgets are selected. To move the widgets as a group, click on one of the widgets and drag.

### **View a List of Widgets on the Canvas**

You can view a list of widgets on the canvas by clicking the **Navigator**  tab. Click a widget in the list to select it.

This means of selection is useful to select widgets that are layered or positioned close together, or to select invisible widgets (where the opacity is set to 0). Once a widget is selected, you can change its properties in the **Widget Properties** tab.

Widgets that are selected on the canvas are displayed in bold type in the Navigator tab.

### **Change the Type of Widget**

You might on occasion want to change the type of widget on the canvas, such as changing a gauge to a linear gauge. To change the widget type, delete the widget and add a new one.

## **Change the Appearance of a Dashboard Widget**

You can change the way a widget looks, including the size, color, border, or opacity, or you can add a drop shadow.

### **Contents**

#### **Resize a Widget**

Change the size of a widget as needed.

#### **Follow these steps:**

1. Hover over the edge of a widget so that the cursor changes to a line with arrows at each end.
2. Click and drag to change the dimension of the widget.  
Or, click a corner of the widget (except the lower right corner) and drag it to change both the width and height.

#### **NOTE**

Dragging the lower right corner does not change the width and height of the widget. This is so that for small widgets you can click in this area and drag the widget to move it on the canvas.

3. (Optional) Refine the size by entering the number of pixels for the width and height.
  - a. Click the **Widget Properties** tab.



- b. Click **Size & Position** to expand the menu.
- c. Enter the number of pixels for **Width** and **Height**.


### **Set the Opacity**

Change the opacity to make the widget fainter or darker.

#### **Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** tab.
3. Click **General** to expand the menu.
4. Click the **Opacity** slider to adjust the opacity.

#### **NOTE**

If you set the opacity to 0 the widget is invisible. To select an invisible widget, go to the **Navigator** () tab and click the name of the widget. You can then go to the **Widget Properties** tab and change the properties of the widget.

### **Add a Shadow**

You can add a shadow around the edges of a widget.

#### **Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** tab.
3. Click the **On/Off** button next to **Shadow** to turn the shadow on.
4. (Optional) Use the color picker and the **Angle**, **Distance**, and **Blur** sliders to adjust the appearance of the shadow.

#### **NOTE**

Use the slider on the right of the color picker to set the opacity for the color.

### **Add a Border**

You can add a border to a widget.

#### **Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** tab.
3. Click the **On/Off** button next to **Border** to turn the border on.
4. (Optional) Use the **Color** and **Width** fields to adjust the appearance of the border.

### **Set the Color**

You can change colors within widgets (circle, rectangle, line, charts, and gauges) for both data and backgrounds. For some widgets, you can define a color map to assign colors to different value ranges. For example, for a widget with an alarm-type data source, you can display a different color for each alarm severity level.

#### **Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** tab.
3. Click **Color** to expand the menu.
4. Enter a hex code, or click the **Default Color** field to display a color picker.

**NOTE**

Use the slider on the right of the color picker to set the opacity for the color.

5. (Optional) Create a color map, if available:
  - a. Assign a data source to the widget if you have not already done so.

**NOTE**

You can set the default color but cannot define a color map if a data source is not assigned.

- b. Click the **Add** icon to add color rows.

**NOTE**

If you assigned the alarm type data source to the widget, a field for each alarm level is displayed. There is no plus sign as you do not need to add any color rows.

- c. Enter a hex code or click in each color field to display a color picker.
  - d. Enter a data threshold value for each color.

Note that the value range requires only a single threshold value: the lower-end threshold. The default color is applied from 0 to the maximum value for the data source unless another defined threshold value is reached first, changing the display to the new color. This new assigned color is applied from the threshold to the maximum data value unless the value reaches another assigned threshold first, at which the next assigned color is applied. This replacement is carried out for all thresholds in the order that they are entered.

If a value does not reach another threshold, the assigned color does not change.

**Set the Width of a Line**

You can set the width of a line that connects two widgets.

**Follow these steps:**


1. Click the line to select it.
2. Click the **Widget Properties** tab.
3. Click **Line** to expand the menu.
4. Enter a value in the **Width** field.

Change the opacity to make the widget fainter or darker.

**Follow these steps:**

1. Click the widget to select it.
2. Click the **Widget Properties** tab.
3. Click **General** to expand the menu.
4. Click the **Opacity** slider to adjust the opacity.

**NOTE**

If you set the opacity to 0 the widget is invisible. To select an invisible widget, go to the **Navigator**  tab and click the name of the widget. You can then go to the **Widget Properties** tab and change the properties of the widget.


**Restrict Dashboard Navigation**

In the Dashboard view, you can change dashboard navigation and display characteristics. These options are useful for restricting navigation among dashboards for a specific user.

## **Set a Default Dashboard**


You can set a default dashboard for the Dashboard view. This setting also restricts navigation to those dashboards linked to the current dashboard.

### **Follow these steps:**

1. Open the **Dashboard** view.
2. Click the **Options** icon ()
3. Select a dashboard from the menu.
4. Click **Save**.
5. Click **Return to Full Page**.

The view opens to the selected dashboard in **Live View**. This dashboard is the default dashboard whenever the view is opened under the current account.

The pull-down menu under the dashboard tab **gear** icon () shows only two options: **View full screen** () and

**Publish to PDF** ()

Without access to the **Edit** view, the user has no access to the 'Open' option under the Dashboard menu. Navigation is restricted to dashboards linked to the current dashboard through widgets. This limitation applies to each dashboard that is opened through such links. To recover edit and navigation capability for all dashboards, follow the previous steps but select 'None' as the dashboard default.

## **Disable Dashboard Breadcrumbs**

When navigating between dashboards, the header at the top of the dashboard displays the name and path to the dashboard, including instances in which the current dashboard was opened previously. This function can produce a long path. You can suppress the path information so that only the name of the current dashboard is displayed.

### **Follow these steps:**

1. Open a dashboard.
2. Select **Edit** from the dashboard tab pull-down menu ()

#### **NOTE**

If the **Edit** option of the dashboard pull-down tab has been disabled, set the default dashboard to 'None' through the steps above.

3. Select the **Canvas Properties** icon () in the right-hand pane header.
4. Uncheck the box for **Show breadcrumbs**.

To enable breadcrumbs, follow the previous steps and check the box for **Show breadcrumbs**.

#### **NOTE**

Breadcrumb settings are inherited from the current dashboard. Disabling breadcrumbs in the current dashboard also disables breadcrumbs in all subsequent dashboards.

## **Disable Widget Tooltips**

Tooltips are displayed when hovering over a dashboard widget in **Live View**, showing either the data for the widget or the target of any link assigned to the widget. You can suppress the tooltip for the widget without suppressing any link assigned to it.


### **Follow these steps:**

1. Open a dashboard.

2. Select **Edit** from the dashboard tab pulldown menu (  ).

**NOTE**

If the Edit option of the dashboard pulldown tab has been disabled, set the default dashboard to 'None' through the previous steps.

3. Select a widget.
4. Select the **Widget Properties** icon (  ) in the right-hand pane header.
5. Uncheck the box for **Show tooltip**.

To enable the tooltip for a widget, follow the previous steps and check the box for **Show tooltip**.

**NOTE**

The **Tooltip** setting is set for each widget individually and is not inherited by other widgets.

## Monitoring Configuration Service

Creating and managing monitoring configurations for hundreds of target devices or resources is time-consuming. You can streamline the manual configuration process by using the Monitoring Configuration Service. The Monitoring Configuration Service allows Administrators and other authorized users to create a set of configuration profiles. The profiles are applied concurrently to hundreds of target devices. The Monitoring Configuration Service also automatically deploys probes to target devices as needed.

You use the provided profile types to create monitoring configuration profiles. The profile types are designed to focus on the components or network elements that probes can monitor. You no longer have to determine which probes to deploy and configure to monitor your devices.

After monitoring configuration profiles are applied to target devices, you can always modify profiles as your monitoring needs change.

### Contents

#### Required Permissions

The Account Admin view in Operator Console (OC) lets bus users create accounts and modify ACL permissions for accounts. See [Using Account Admin](#) for more details.

The following table shows which ACL permissions are required to manage configuration profiles created with the Monitoring Configuration Service. The ACL permissions are listed vertically, and the tasks a user might perform are shown horizontally.

| ACL Permissions                                 | Manage Group Profiles | Manage Device Profiles | Manage Configuration Service Options | View Profiles |
|-------------------------------------------------|-----------------------|------------------------|--------------------------------------|---------------|
| Monitoring Configuration Service                | YES                   | YES                    | YES                                  | YES           |
| Modify Individual Monitors for Computer Systems | N/A                   | YES                    | N/A                                  | N/A           |
| Group Modification                              | YES                   | N/A                    | N/A                                  | N/A           |
| Probe Configuration                             | N/A                   | N/A                    | YES                                  | N/A           |
| Edit Monitoring Templates                       | YES                   | YES                    | N/A                                  | YES           |

## **Verify Requirements**

The Monitoring Configuration Service uses the following items that are installed with UIM Server and the OC installer:

- **Operator Console (OC):** Select the **Monitoring Config** icon in the Groups View or after selecting the groups or devices in Inventory View to access the Monitoring Configuration Service.
- **mon\_config\_service probe:** This probe is deployed to the primary hub during installation. This probe is required if you want to use the Monitoring Configuration Service.

In preparation for using the Monitoring Configuration Service, verify that you have:

- Downloaded the probes that you can configure with the Monitoring Configuration Service to the local archive. See [Download, Update, or Import Packages](#) for instructions on downloading probes to the local archive.
- Installed the appropriate probe licenses.

### **NOTE**

From CA UIM 9.2.0 onward, hub/robot- and probe-level licensing requirements have been removed. Deploy the hub, robot, and distsrv versions released with CA UIM 9.2.0 to remove the license dependency. If you want to continue with the older versions of hub and probes that require an extension of the license, contact Support so that they can assist you in extending the license (if required).

- Reviewed the Release Notes for the probes you want to configure with the Monitoring Configuration Service. You can find Release Notes for each probe on the [Probes Documentation Space](#).

### **NOTE**

Verify the UIM Server and Operator Console are at the same version level.

## **Probe Supported by Monitoring Configuration Service**

For new installations, the following probes appear in either the Local Version or the Web Version column on the **Archive** tab in Admin Console. Use Monitoring Configuration Service to deploy and configure the following versions of probes. The configuration in the profile overwrites the existing monitoring settings for a probe. When probe configuration fields are not included in the monitoring profile, the existing default or configured setting is retained.

- adevl 2.02 (or later)
- ad\_server 1.91 (or later)
- ad\_response 1.70 (or later)
- apache 1.62 (or later)
- aws 5.21 (or later)
- axa\_log\_gateway 1.00 (or later)
- azure 3.01 (or later)
- cdm 5.80 (or later)
- cdm-MC 5.80 (or later)
- dirscan 3.14 (or later)
- docker\_monitor 1.42 (or later)
- dns\_response 1.68 (or later)
- emailgtw 2.82 (or later)
- email\_response 1.44 (or later)
- ews\_response 2.03 (or later)
- exchange\_monitor 5.31 (or later)
- iis 1.90 (or later)
- jdbc\_response 1.25 (or later) (for the PostgreSQL profile type)
- ldap\_response 1.35 (or later)
- log\_forwarder 1.00 (or later)
- log\_monitoring\_service 1.00 (or later)
- logmon 3.55 (or later)
- mysql 1.48 (or later)
- net\_connect 3.31 (or later)
- netapp\_ontap 1.21 (or later)
- ntevl 4.12 (or later)
- ntperf and ntperf64 2.03 (or later)
- ntservices 3.24 (or later)
- nutanix\_monitor 1.51 (or later)
- office365 1.00 (or later)
- openstack 1.36 (or later)
- oracle 4.91 (or later)
- processes 4.01 (or later)
- rsp 5.20 (or later)
- sap\_basis 1.31 (or later)
- snmpgtw 1.40 (or later)
- sharepoint 1.81 (or later)
- sqlserver 4.94 (or later)
- telemetry 1.20 (or later)
- url\_response 4.41 (or later)
- vmware 6.81 (or later)
- vnxe\_monitor 1.01 (or later)
- xtremio 1.01 (or later)

Refer to the [Probes Documentation Space](#) for information about probes.

---

## Profile Types Included with CA UIM

The following are some of the profile types that you can use to create configuration profiles for monitoring probes. You can configure most profile types for Windows, Linux or HP-UX systems, unless noted.

### NOTE

The two kinds of profile types are:

- Setup - Use the setup profile types to configure how the probe operates. The setup profile types are in the lower half of the list.
- Monitoring - Use the monitoring profile types to configure what a probe monitors, and the types of alarms and QoS metrics the probe generates. The monitoring profile types appear at the top of the profile type list.

Some probes have a single profile type; whereas, others have a *setup* and one or more *monitoring* profile types. When there are several profile types, create a Setup configuration profile first. Some of the setup profile types have settings that are related to the monitoring profile types. For example, the Setup cdm profile type lets you configure sample collection intervals that apply to CPU, disk, memory, and NIC monitoring.

- 
- Active Directory Events Exclude
  - Active Directory Events Include
  - Active Directory Response
  - Active Directory Server
  - Apache
  - Application Discovery Scripts
  - CPU Monitor
  - Default Disk(s)
  - Disk IO Monitors
  - Disk(s)
  - DNS Response
  - Email Gateway
  - Email Response
  - Event Log Exclude
  - Event Log Include
  - Exchange Monitor
  - File and Directory Scan
  - IIS
  - Iostat
  - LDAP Response
  - Log Forwarding
  - Log Forwarding Apache
  - Log Forwarding Catalina
  - Log Forwarding Log4j
  - Log Forwarding Oracle Alert
  - Log Monitoring
  - Log Monitoring Service
  - Memory Monitor
  - MS Exchange Server Response
  - MySQL
  - NIC Monitor
  - NT Performance Metrics
  - Oracle
  - Port Check
  - PostgreSQL
  - Processes
  - Remote System Monitoring
  - SAP ABAP
  - SAP NetWeaver
  - Setup adevl
  - Setup Application Discovery Defaults
  - Setup AWS
  - Setup axa\_log\_gateway
  - Setup Azure
  - Setup DB2
  - Setup cdm
  - Setup dirscan
  - Setup dns\_response
  - Setup Docker
  - Setup emailgtw
  - Setup log\_forwarder
  - Setup log\_monitoring\_service
  - Setup logmon
  - Setup net\_connect



(Used only for Solaris systems)

- Setup rsp
- Setup SAP
- Setup snmpgtw
- Setup telemetry
- Setup URL Response
- Setup VMware
- SharePoint
- SNMP Gateway
- SQL Server
- URL Check
- Windows Services

#### **NOTE**

MCS also provides enhanced profiles. Enhanced profiles enable you to configure metrics, baselines, alarm thresholds, alarms - including Time Over Threshold alarms - and custom alarm and close alarm messages, all within a single MCS profile. In the UI, enhanced profiles are displayed with the term "(Enhanced)" added to the profile name; for example, CPU Monitor (Enhanced).

### **Preliminary Tasks**

This section describes the one-time setup tasks to perform before you create a configuration profile.

The one-time setup tasks are:

- Verify that devices in more than one group are managed by the same UIM account.
- Deploy robots to all target devices
- Optionally, configure proxy options especially if there are firewalls in your environment.

### **Create OC Groups**

When you create groups in OC for the purpose of applying configuration profiles with Monitoring Configuration Service, MCS applies configuration profiles to devices (in the group) that have the resources that match a profile. For example, Monitoring Configuration Service can apply the Disk(s) or CPU Monitor profile to a group of Windows or Unix devices. But MCS would not apply an NT Performance configuration profile to a group of Unix devices.

Some probes, such as the net\_connect or rsp probes, monitor remote target devices from a host computer. For these probes, you can create a group in OC with the host systems that monitor remote devices, and another group with the remote devices the probe monitors.

#### **TIP**

You use MCS to manage configuration profiles for groups automatically created with the Application Discovery feature. See [Use Application Discovery](#) for details.

### **Move a Device to Another Group**

You can move devices between groups. It can take MCS some time to apply group configuration profiles to devices added to groups or remove profiles after a device is removed from a group. See [Manage Groups in OC](#) for more details about managing devices in groups.

#### **NOTE**

If you remove a device from a group, and then add the device back to the same group later, restart the robot on the device. This allows Monitoring Configuration Service to reapply the current group configuration profiles at the next evaluation interval.

**TIP**

**Best practice:** Add devices to only one OC group.

**Using Groups and Accounts with Monitoring Configuration Service**

Monitoring Configuration Service fully supports the CA UIM accounts, groups, and origin concepts used to create multi-tenancy or restricted control environments. Carefully create the account and group structure to avoid operator confusion and errors.

Always implement non-overlapping management privileges for any element managed through Monitoring Configuration Service. All users allowed to deploy a profile to an element must be able to see the element, the actual profile, and any potential group profiles. This avoids situations where multiple users can unknowingly apply conflicting configuration profiles to the same device.

**Best Practice Example:**

A CA UIM administrator works with two IT sites, Accounting IT, and Engineering IT. The administrator wants unified performance reports for all servers, but also wants to allow both departments to override settings. In this scenario, there is a small group of servers that are shared by and are important to both groups.

The CA UIM administrator creates the following structure of groups and permissions:

- **Standard Profiles:** The Standard Profiles group includes a small set of servers with several configuration profiles, created with Monitoring Configuration Service, applied. *All* operators have access to this group and can copy profiles from this group to their servers and groups.
- **Accounting IT Servers:** The Accounting IT Servers group includes all servers managed by the Accounting IT team. *Only* the Accounting IT team has access to the servers. The Accounting IT team can copy profiles from the Standard Profile group to this group and can apply any overrides needed.
- **Engineering IT Servers:** The Engineering IT Servers group includes all servers managed by the Engineering IT team. *Only* the Engineering IT team has access to the servers. The Engineering IT team can copy profiles from the Standard Profile group to this group and can apply any overrides needed.
- **Shared Servers:** The Shared Servers group includes all servers important to both Accounting IT and Engineering IT. *Only* the administrator has access to manage the shared servers. All configuration changes must be requested from the administrator. The administrator implements the requested changes if appropriate for both teams.

**Deploy Robots to Target Devices**

A robot must be running on each device. The robot allows the Monitoring Configuration Service to deploy probes and apply configuration profiles to target devices. Robots also facilitates communication between a probe and the network resources or elements the probe monitors. See [Deploy Robots](#) for more information.

**Getting Started**

This section explains some basic Monitoring Configuration Service concepts.

- What are profile types?
- Why are there two versions of the cdm probe in the Local Version column on the **Archive** tab in Admin Console?
- Why are there two Setup Processes profile types?
- Can I specify precedence for a configuration profile?

**Profile Types**

Monitoring Configuration Service profile types are displayed on the **Monitoring Config** in OC. Each profile type is designed to focus on system resources or elements probes can monitor. For example, the Disk(s) profile type focuses on monitoring disk drives on a computer system. Determine what you want to monitor and use the appropriate profile type to create a monitoring configuration profile.

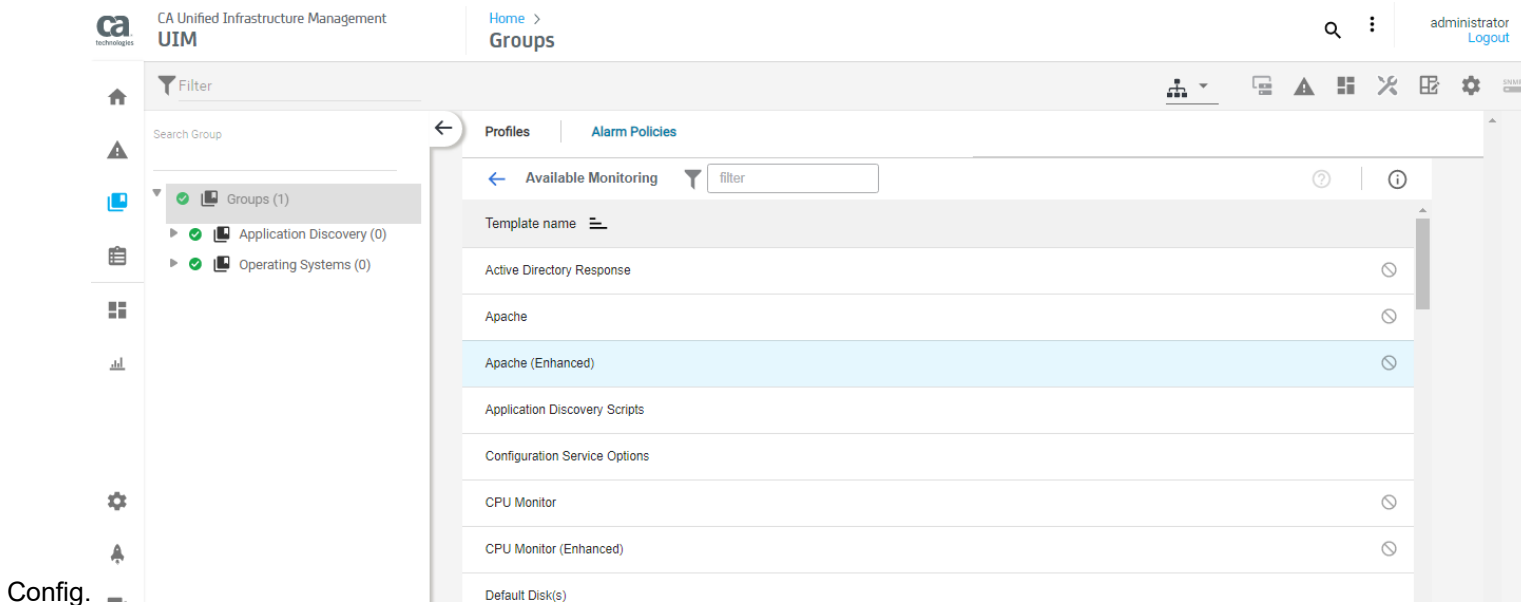
Profile types are grouped and displayed in the following order:

- **Profile Types with configuration profiles:** Appear alphabetically at the top of the list. Use the expand icon to view, access, or hide the configuration profile. For profile types that support multiple profiles, all existing configuration profiles are displayed when you expand a profile type.
- **Profile Types without profiles:** Appear alphabetically after the profile types with configuration profiles. You can create or modify configuration profiles with the profile types that are displayed in normal text. Italicized profile types are inactive, meaning you cannot use them to create configuration profiles. Profile types are italicized in the following scenarios:
  - A probe is not in the hub's local archive. (View the **Archive** tab in Admin Console to determine if a probe is in the local archive.)
  - The required version of a probe is not in the local archive. See Probe Versions Supported by Monitoring Configuration Service for a list of supported probes.
  - Probes requirements are not met. For example, to create a configuration profile with the IIS profile type, the iis and perfmon probes must be in the local archive.

#### NOTE

MCS also provides enhanced profiles. Enhanced profiles enable you to configure metrics, baselines, alarm thresholds, alarms - including Time Over Threshold alarms - and custom alarm and close alarm messages, all within a single MCS profile.

The following figure shows the major components that are displayed when you select the **Monitoring**



#### Two Versions of the cdm Probe

UIM Server Installer delivers the cdm-MC vx.xx or later probe and the standard cdm probe in the hub's local archive. Both versions of the cdm probe provide the same monitoring and alarm functionality. The cdm-MC vx.xx probe replaces the standard cdm probe that you are used to manually deploying and configuring on devices in your infrastructure.

Some key things to know about the two versions of the cdm probe are:

- cdm-MC vx.xx or later does not emit QoS data and alarms until configuration profiles are applied to target devices. The standard cdm probe has preconfigured settings and emits QoS data and alarms immediately after installation.
- Use Monitoring Configuration Service to configure, deploy, and manage cdm-MC vx.xx in your infrastructure.
- When you create configuration profiles, cdm-MC vx.xx is deployed (with the configuration applied) when no cdm probe is running on a target device. If the cdm probe is running on a target device, Monitoring Configuration Service applies the configuration profile to the cdm probe running on a device.
- If you manually deploy cdm-MC vx.xx to a target device, it remains silent. The probe does not emit QoS data and alarms until configuration profiles are applied to target devices.

**For new Installations of CA UIM:**

- After installation, both versions of the cdm probe appear in the primary hub's local archive.
- The Operator Console Installer places the standard cdm probe on the Operator Console Server to monitor its performance and critical resources. Leave cdm running on the Operator Console Server.

For more information about the cdm probe, see the cdm article on the Probes Documentation Space.

**Using the Setup Processes Profile Types**

There are two Setup Processes profile types. Use the profile type that matches the operating system of the target device.

- **Setup processes** profile type  
Use this profile type to create a profile for Windows, Linux, or HP-UX target devices.  
**Note:** If you configure the Setup Processes profile type for a group that has an Oracle Solaris device, the configuration profile is applied to all devices in the group. However, the monitoring results for the Solaris devices might be inaccurate. To monitor processes for Solaris zones, use the Setup processes Solaris profile type.
- **Setup processes Solaris** profile type  
Use this profile type to create a profile for Oracle Solaris or Solaris target devices. The Setup processes Solaris profile type lets you configure the zones to monitor.  
**Note:** The system displays an error if you attempt to use the Setup processes Solaris profile type for Windows, HP-UX, or Linux devices.

**Use Group Profile Priority to Set Precedence**

Only one instance of a configuration profile can be applied to a target device. When devices are members of more than one OC group, the following criteria determines the configuration profile that is applied to a device:

- Higher Group Profile Priority  
For devices that are members of several groups, the configuration profile with the higher Group Profile Priority number is applied.  
Consider the sample scenario in the following table. A user creates an Apache configuration profile for OC groups Denver and Boston. Device A is a member of both OC groups. The Apache configuration profile for the OC group Boston has a group profile setting of 200. This priority setting is higher than the priority (100) assigned to the Apache configuration profile for OC group Denver. Therefore, the Apache configuration profile for OC group Boston takes precedence and is applied to Device A.

| OC Group | Members                     | Configuration Profile | Group Profile Priority |
|----------|-----------------------------|-----------------------|------------------------|
| Denver   | <b>Device A</b><br>Device B | Apache                | 100                    |
| Boston   | <b>Device A</b><br>Device C | Apache                | <b>200</b>             |

- Device Profile

After group configuration profiles are applied to devices in a group, an administrator can temporarily overwrite the group configuration settings for a device. The device configuration profile overwrites any group configuration profile settings. See [Modify Configuration Profiles](#) for more details.

#### NOTE

- When the same profile type is configured for several groups in OC but different monitoring elements are configured in each configuration profile, both profiles are applied to overlapping devices.
- When the same profile type is configured for several groups in OC and the same monitoring elements are configured in each configuration profile, the order in which the profiles are applied is non-deterministic.
- Device configuration profiles that are created from the same profile type must have unique profile names.

### Select a Reference Device

When you create group configuration profiles with profile types that require data from a probe, you must select a *reference device*. Monitoring Configuration Service gathers data for the profile type from probes running on a reference device.

By default, the Reference Device field is populated with all devices in the selected group that have a robot and the probe associated with the selected profile type installed. You can add devices to the Reference Device drop-down list by selecting one of the following options:

- **Include Devices Not in Group:** Select this option to choose any device in another group that has a robot and the probe associated with the selected profile type installed.
- **Include Devices Without Probe:** Select this option to choose any device in the same group with a robot installed. The devices are not required to have the probe associated with the selected profile type installed. If you select this option and select a reference device without the probe installed, Monitoring Configuration Service deploys the probe to the selected reference device and the probe collects data required for the selected profile type.
- **Select both options:** Select both options to choose any device in your environment with a robot installed. The devices are not required to have the probe associated with the selected profile type installed. If you select a reference device without the probe installed, Monitoring Configuration Service deploys to the selected reference device and the probe collects data required for the selected profile type.

### User Scenario

- **Prerequisite**
  - Verify that the processes probe is in the local archive.
- **Environment**
  - A group in OC with three test Windows devices.
  - A robot is installed on all three devices.
  - The processes probe is not installed on any of the devices in the OC group.
  - The processes v4.31 probe is in the local archive.
- **Scenario**
  - I want to create a Processes group configuration profile to monitor processes running on the devices in a OC group.
  - I want to use a device in the selected group as a reference device.

Most people prefer to create a group configuration profile and let Monitoring Configuration Service deploy probes and apply the monitoring configuration profiles to devices in a group. This is the case for this sample scenario.

In this scenario, the first time you view the processes profile type, the Reference Device field is empty because the processes probe has not been deployed to devices in the group. To populate the Reference Device field, you can select the **Include Devices Without Probe** option. This option adds all the devices (with an installed robot) in the selected group to the drop-down list.

After you select a reference device, Monitoring Configuration Service deploys the processes probe to the reference device and then gathers data from the probe. Monitoring Configuration Service populates the Available Processes drop-down

list. Select the process you want the processes probe to monitor and configuration the remaining settings. Create the configuration profile. Monitoring Configuration Service deploys the processes probe and then applies the monitoring configuration to all devices in the group.

The group configuration profile remains locked until Monitoring Configuration Service is finished applying the profile to all devices in the group. Once the configuration profile is unlocked, you can modify the configuration or copy the profile to another group or to a device in another group.

### Can I Change the Reference Device?

When you create or modify a configuration profile, you can change a reference device. Monitoring Configuration Service gathers data from the newly selected reference device and returns a list of available processes. The list of available processes could be different. You can select a different process to monitor.

Also, if the newly selected reference device does not have the probe associated with the profile type installed, Monitoring Configuration Service deploys the probe to the reference device and then MCS retrieves the required data.

### Create a Processes Group Configuration Profile

The following procedure shows you how to create a processes group configuration profile in the environment described at the beginning of this user scenario. The configuration process includes how to use the **Include Devices Without Probe** option to populate an empty Reference Device field, activate a configuration profile, select the type of process the probe monitors on target devices, and configure the Process Restart alarm.

#### Follow these steps:

1. Select the test group in OC.
2. Click the **Monitoring Config**.
3. Select '+' and select the Processes profile type.
4. (Optional) Modify the Group Profile Priority setting. See Use Group Profile Priority to Set Precedence for more details.
5. Select the **Active** check box to enable the probe to generate the configured alarms and metrics.
6. Enter a unique **Profile Name** and a brief **Description** for the configuration profile.
7. Select the desired process in the **Available Processes** field.  
Monitoring Configuration Service populates the Process Name, Command Line, and Process Owner fields with data retrieved by the reference device.
8. Select the **Track Process by Process Identifier** option.  
You must select this option to configure the Process Restart alarm settings.
9. Select the **Process Restart** option.
10. In the Report on Process field, select **Down**.
11. In the Severity fields, select **Information** and **Critical**.
12. **Create** the configuration profile.

The following diagram shows the group Processes configuration profile we just created. Notice that the configuration profile appears at the top of the profile type list.

The screenshot displays the CA Unified Infrastructure Management (UIM) interface. At the top left, the CA logo and 'UIM' are visible. The main header shows 'Home > Groups'. A left-hand navigation pane contains various icons for home, alerts, reports, and settings. The main content area is titled 'Processes' and shows the configuration for a 'Processes Profile'. The profile is currently 'Active' (indicated by a blue toggle). The 'Profile Name' is 'Processes 1A' and the 'Description' is 'Group configuration Profile'. Under 'Recognize Process By', the 'Available Processes' dropdown is set to 'cdm.exe'. The 'Mode' is set to 'Name + Command line'. A 'Process Name' field is partially visible at the bottom.

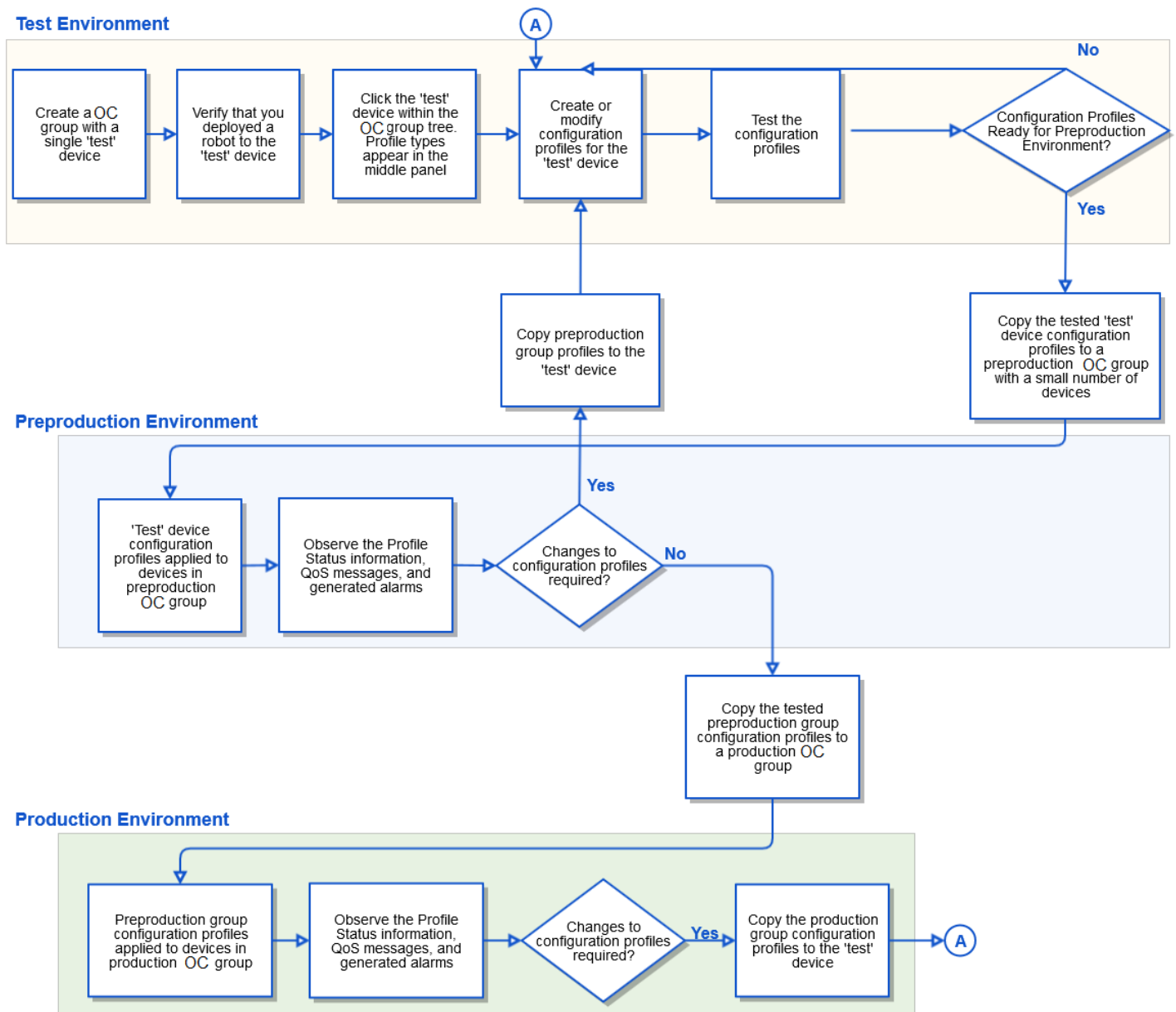
### **Workflow for Managing Configuration Profiles**

The process of creating and managing configuration profiles, and then rolling out the configurations to production groups consists of the following tasks:

- Develop and Test Configuration Profiles**  
 Configure profiles for a 'test' device in a test environment. If probes are not running on target devices, Monitoring Configuration Service deploys the appropriate probes to the target 'test' device and applies the configuration profiles that you created. Observe the QoS data and alarms emitted.
- Move Configuration Profiles to Production**  
 Continue to modify configuration profiles for the 'test' device until you determine that the monitoring configuration is correct. When the device configuration profiles are fully tested, copy the device configuration profiles to a preproduction or production group. The copied configuration profiles are applied to all devices in the group. See [Copy Profiles for Consistent Monitoring](#) for more details about the copy function.
- Modify Production Configuration Profiles**  
 When you want to modify production group configuration profiles, copy the group profiles to the 'test' device. Modify the profiles for the 'test' device. Test the monitoring results to verify that you are seeing the expected QoS data and alarms emitted. When fully tested, copy the configuration profiles from the 'test' device to the production group. The modified group configuration profiles are applied to all devices in the group.

The following figure shows the recommended end-to-end process of creating and copying device configuration profiles to a production group.

**Figure 26: Create and Deploy a Configuration Profile**



**TIP**

Always copy pre-production or production group configuration profiles back to the 'test' device in the test environment to modify and test profile configuration changes. Observe QoS messages and alarms in the test environment. When configuration profiles are fully tested, copy the device profiles to a pre-production group. Test, observe results, and then copy the pre-production group profile to a production group.

**WARNING**

When upgrading to a newer version of CA UIM with existing MCS configuration profiles applied to target devices, you might notice that probes are not generating the expected metrics or alarms after the upgrade.

To resolve this issue, we recommend the following actions:



- If an error condition appears in the Profile Status section of a configuration page, manually delete the probe associated with a configuration profile. Use Admin Console to delete probes from target devices.
- Move the newest version of a profile type to production.
- Make a minor change to the configuration profile with an error status.

Result: Monitoring Configuration Service deploys the version of the probe in the local archive and applies the configuration profile to target devices. The probe generates the correct metrics and alarms.

#### NOTE

Monitoring Configuration Service attempts to apply configuration profiles to a probe on a target device. The Profile Status can show an error condition when Monitoring Configuration Service cannot apply a configuration profile to an older version of a probe. You might also notice that probes are not generating the expected metrics or alarms. To resolve this issue, manually remove an older version of a probe from target devices. Make a minor change to the configuration profile Monitoring Configuration Service applied to target devices. This makes Monitoring Configuration Service deploy the version of the probe in the local archive to target devices. Then MCS applies the configuration profile to the target devices. The probe should begin to generate metrics and alarms.

### Correcting the plugin\_metric.cfg File

When you create an alarm policy or an enhanced profile, its configuration information is written in the `plug_in` file.

In robot versions prior to the secure version, sometimes, this information is not written properly in the `plugin_metric` file. For example, you create an alarm policy, but that alarm policy configuration is not deployed properly. In this case, the corresponding information is not updated correctly in the `plugin_metric` file and this creates issues. Similarly, when you delete a child profile from the Operator Console UI, the same information is not deleted from the `plugin_metric` file. This issue has been fixed in the robot version released with CA UIM 9.2.0 and later releases.

To resolve such issues in your environment, you can use the `plugin_metric_correction` callback that is available for the `mon_config_service` probe. This callback re-deploys enhanced profiles and alarm policies based on your input.

#### Follow these steps:

1. Ensure that you do not create any MCS profiles or alarm policies when you are performing this operation.
2. (Optional) Open the `mon_config_service` raw configuration and increase the thread count to 10 in the `timed` section for each parameter:
  - `device_processing_threads`
  - `config_deployment_threads`

We recommend that you increase the thread count so that the process completes quickly. After you complete the process, change the settings back to the original values.
3. Access the probe utility (pu) for the `mon_config_service` probe.
4. Locate and select the `plugin_metric_correction` callback from the drop-down list.
5. Enter the appropriate information for the following parameters, as required:
  - `process_all_devices_flag`  
Enter the value as true if you want to re-deploy enhanced profiles or alarm policies on all the devices. If you select this parameter, all the remaining parameters are not required.
  - `robot_names`  
Enter the specific robot name on which you want to re-deploy the enhanced profiles or alarm policies. If you want to use more than one entry, enter a comma-separated list.
  - `computer_system_ids`  
Enter the specific computer system ID (`cs_id`) on which you want to re-deploy the enhanced profiles or alarm policies. If you want to use more than one entry, enter a comma-separated list.
  - `cm_group_ids`

Enter the specific group ID on which you want to re-deploy the enhanced profiles or alarm policies. All the devices that are part of that group are considered for re-deployment. If you want to use more than one entry, enter a comma-separated list.

**Note:** You can use any combination of

```
robot_names
,
computer_system_ids
, and
cm_group_ids
.
```

6. Run the callback.

A message appears in the right pane stating that the process has started for the devices. However, note that no completion message is displayed. The process completes all related tasks in the background. If you want to check the status, you need to verify the database.

7. Verify the status by running the following queries:

```
- select * from ssrv2policytargetstatus where cs_id in (<ID>);
- select * from ssrv2profile where cs_id in (<ID>);
```

The status OK means that the re-deployment has occurred without any issue.

8. Similarly, to find whether any error has occurred, run the following query:

```
- select * from ssrv2audittrail where userid like 'plugin_correction%';
```

From the result of this query, note down the object IDs (failed computer system IDs), review the error messages, resolve them, and then again run the callback for these failed devices.

You have successfully repaired the plugin\_metric file.

## Manage Monitoring Using MCS Profile Types

Determine what you want to monitor in your environment and create the corresponding configuration profiles. You can create a configuration profile for each device or you can create a group configuration profile that MCS applies to all devices in a group. Use the profile types that are displayed in the Monitoring Config page to create configuration profiles.

The safest way to roll out configuration profiles is to create preliminary device-level configuration profiles on a 'test' device. Perform tests on the device configuration profiles and verify the results. When the device configuration profile is fully tested, copy the tested device profile to production groups.

### Contents

#### NOTE

Enhanced profiles enable you to configure metrics, baselines, alarm thresholds, alarms - including Time Over Threshold alarms - and custom alarm and close alarm messages, all within a single MCS profile.

### Create a Device Configuration Profile

Always create device configuration profiles, and then copy the fully tested profiles to groups.

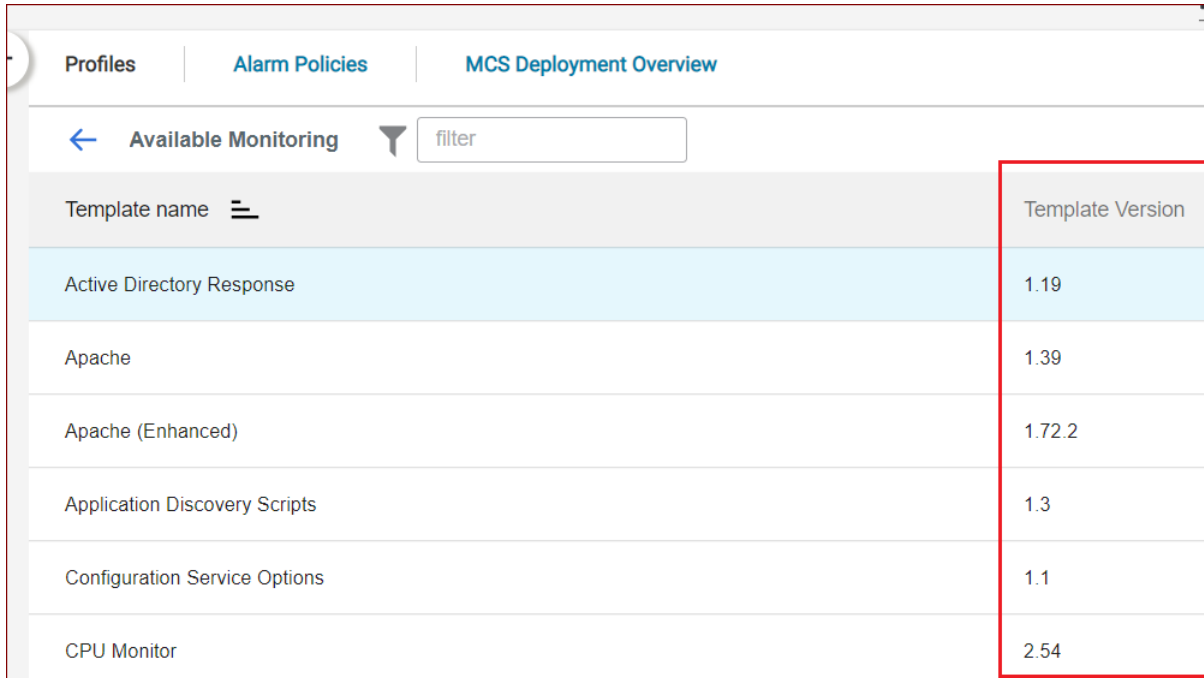
#### Follow these steps:

1. In Operator Console, expand a group in the Groups view and select a device.  
The OC group can be one of the predefined OC groups (for example, the Unix and Windows groups) in a test environment or in a test group that you created. The OC group should have at least one device.
2. Select the Monitoring Config icon in the top-right menu.  
The profile types that apply to the selected device appear.

**NOTE**

If you select a device and profile types do not appear in the Profiles tab, deploy a robot to the device.

- In the Profiles tab, click '+' to add a profile.  
Profile types are displayed alphabetically. Consider configuring the Setup profile types first. You can also view the version of the template in the Template Version column. The following screenshot shows the Template Version column:



| Template name                 | Template Version |
|-------------------------------|------------------|
| Active Directory Response     | 1.19             |
| Apache                        | 1.39             |
| Apache (Enhanced)             | 1.72.2           |
| Application Discovery Scripts | 1.3              |
| Configuration Service Options | 1.1              |
| CPU Monitor                   | 2.54             |

- (Optional) Select **Yes** if you see a dialog asking if you want the probe to be installed. Verify that the probe resides in the local archive of the hub.
- Configure the monitoring settings.
- Create the configuration profile.

View the profile status information to verify that the configuration profile was successfully applied to the target device. Until the configuration profile is applied, you cannot modify or copy the profile. When the configuration profile is successfully applied, the status changes to Deployed and the lock disappears.

**Create a Group Configuration Profile**

You can create group configuration profiles, although we recommended that you copy tested device profiles to a group. Monitoring Configuration Service applies group profiles to all devices in a group that have a robot installed. If a robot is not installed on a device, Monitoring Configuration Service cannot communicate with that device.

Some profile types require data from a device before you can create a group configuration profile. For these profile types, you must select a *reference device*. Monitoring Configuration Service retrieves the data the profile type requires from a probe that is deployed to the selected reference device. Once the data is populated in the profile type, you can continue to create a group configuration profile.

Monitoring Configuration Service can take some time to apply a group configuration profile to every device in a group. After Monitoring Configuration Service has successfully applied a group profile to all devices in a group, make configuration changes to the group profile. The group profile controls the configuration for the member devices.

**Follow these steps:**

- In Operator Console, select a group in the Groups view.

- The OC group can be one of the predefined OC groups (for example, the Unix and Windows groups) in a test environment or in a test group that you created. The OC group should have at least one device.
2. Select the Monitoring Configuration icon.  
The profile types that apply to the selected group appear.
  3. In the Profiles tab, click '+' to add a profile.  
Profile types are displayed alphabetically. Consider configuring the Setup profile types first. You can also view the version of the template in the Template Version column.
  4. (Optional) Select **Yes** if you see a dialog asking if you want the probe to be installed. Verify that the probe resides in the local archive of the hub.
  5. If you select a profile type that requires Monitoring Configuration Service to retrieve data from a probe, the *reference device* fields appear in the Group Profile Settings section. By default, only devices in the selected group with the required probe installed appear in the Reference Device drop-down list. To add more devices:
    - a. Select a reference device. Monitoring Configuration Service retrieves the required data from the probe running on the selected reference device, and the appropriate fields are populated on the profile type.
  6. Configure the remaining monitoring settings.
  7. Create the configuration profile.

View the profile status information to verify that the configuration profile was successfully applied to all devices in the group. Until the configuration profile is applied, you cannot modify or copy the profile. When the configuration profile is successfully applied, the status changes to Deployed and the lock disappears.

### Using Variables in Configuration Profiles

For some configuration profiles, it is more practical to enter a variable instead of a value. For example, when you create an Apache device configuration profile, the IP address of the device is automatically populated in the configuration profile. If you want to copy the device profile to a group of Apache Servers, you can enter the '{device.ipaddress}' variable in the *Hostname* and *URL for HTTP Response* fields.

The following figure shows variables that are entered for the the *Hostname* and *URL for HTTP Response* fields. When you copy the device profile to an OC group, Monitoring Configuration Service resolves the variables with the IP address of each server when it deploys the configuration profile to the member devices.

The screenshot displays the CA Unified Infrastructure Management (UIM) interface. The top navigation bar shows 'CA Unified Infrastructure Management UIM' and 'Home > Groups'. The user is logged in as 'administrator'. The main content area is titled 'Profiles' and 'Alarm Policies'. The 'Apache' profile is selected, showing a filter 'filter' and 'Showing 51 Configured 0 Total 51' items. The profile configuration includes a description 'Apache Server Monitored' and a note: 'Define the hostname or IP address of the system where the Apache server is hosted. Specify the URL where the probe sends the HTTP response and server status.' The configuration fields are:
 

- Hostname or IP Address: {device.ip}
- URL for HTTP Response: http://{device.ip}:80/server-status?auto

 Both fields have a note: '{Variables} are substituted with actual values.'

The variables that you can enter in MCS profile types are:

- device.name
- device.ipaddress
- device.origin
- device.os\_type
- device.usertag1
- device.usertag2

These variables are also supported with Operator Console.

### **Verify Overlapping Devices Are Managed by the Same UIM Account**

If a device is a member of two or more OC groups, ensure that the groups are managed by the *same* UIM account. This allows users who are members of the UIM account to see the configuration profiles applied to the overlapping device and any future configuration changes.











When the same device is in two or more OC groups that are managed by *different* UIM accounts, users in each account can concurrently configure and manage configuration profiles. However, users in one account cannot see the changes being made by users in another account until the changes are applied to the overlapping device. Changes that are made by users in one account could overwrite changes that are made by users in another account. This creates a confusing situation and should be avoided. See [Using Groups and Accounts with Monitoring Configuration Service](#) for more information.

### **View Profile Details Information**

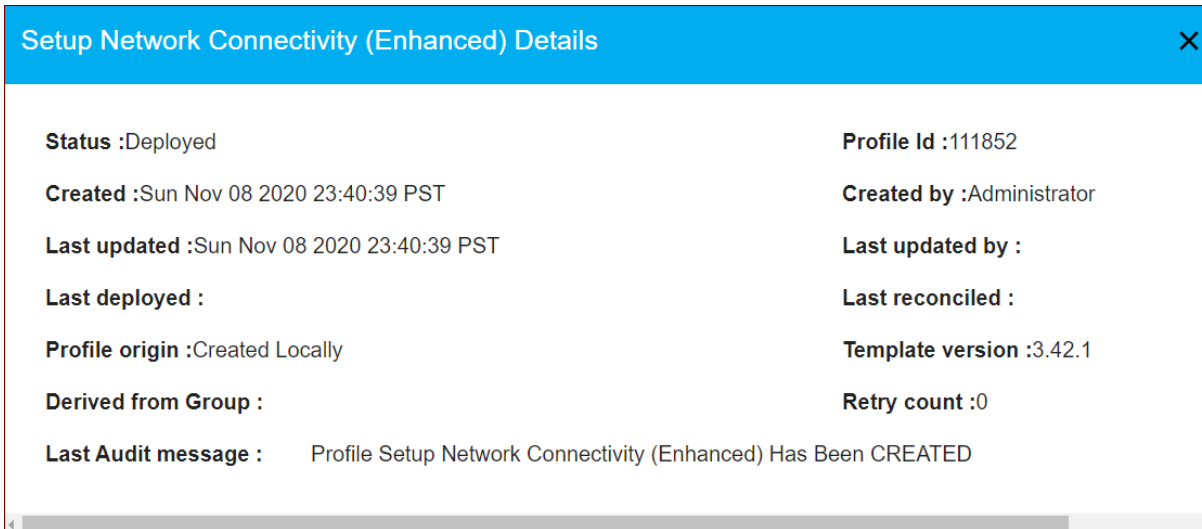
After you create or modify a configuration profile, you can view the profile details information. You can use this information to determine if a configuration profile was successfully applied to target devices. This detailed information also helps you take informed decisions.

#### **Follow these steps:**

1. In OC, navigate to the page that lists the created MCS profiles.
2. Locate the **Actions** column.

| State                                                                               | Profile Id | Profile name  | Template Name  | Alarm Policy                   | Actions                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------|------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | 93         | CPU Monitor (Enhanced)                                                                           | CPU Monitor (Enhanced)                                                                            | CPU Monitor (Group: Test_Test) |    |
|  | 98         | Test                                                                                             | SQL Server (Enhanced)                                                                             | Test (Group: Test_Test)        |    |

3. Click the profile details icon (under Actions) for the required profile. A dialog with required profile details opens:



4. The profile details dialog displays the following information:
  - a. **Status**: Displays the state of the configuration profile that was deployed.
  - b. **Created**: Displays the day, date, and time the configuration profile was created.
  - c. **Last updated**: Displays the day, date, and time the configuration profile was previously modified.
  - d. **Last deployed**: Displays the day, date, and time the configuration profile was previously applied to target devices.
  - e. **Profile origin**: Indicates how the configuration profile was created. A user can create a profile or a group profile can be applied to a device. For a group, the Profile Origin appears as 'locally'. For a device, if the configuration was created at the device level before a group profile was applied, the Profile Origin appears as 'locally'. Once a group profile is applied to a device, the Profile Origin changes to 'group profile'.
  - f. **Derived from Group**: Specifies whether a configuration profile was copied.
  - g. **Last Audit message**: Displays the last message added to the audit log. For example, an initial message might be generated after the current version of a profile is applied. This message is not displayed. The second message (generated when the profile is reconciled) is the last audit message that appears in this field.
  - h. **Profile Id**: Displays a unique ID that is automatically assigned to each configuration profile when it is created.
  - i. **Created by**: Displays an identifier of who configured the original configuration profile.
  - j. **Last updated by**: Displays an identifier of who updated the configuration profile.
  - k. **Last reconciled**: Displays the latest day, date, and time the configuration profile was reconciled.
  - l. **Template version**: Displays the version of the probe template that was used to create a profile.
  - m. **Retry count**: Displays the number of times the MCS tries to deploy the profile.
5. Review the information.

### **Monitoring Configuration Service and Probe Upgrade**

MCS does not automatically upgrade probes when a new probe version is available. For example, if you:

1. Deploy an older version of the cdm probe (cdm v4.78).
2. Configure the cdm probe.
3. Open MCS and apply the **Disk(s)** template.

MCS does not prompt you to install the latest version of the cdm probe, so you must deploy it manually. You can use the `upgrade_probe_to_eligible_robots` callback to deploy a new probe version to all applicable robots at the same time. For more information, see [Simultaneous Deployment of a Probe on Applicable Robots](#).

### **Simultaneous Deployment of a Probe on Applicable Robots**

MCS provides a callback that lets you deploy a probe to all applicable robots at the same time. This ability is helpful in situations where you have deployed a specific probe version on certain robots. Now, when a new version of a probe becomes available, you do not want to manually deploy the new probe version on each robot. You want an automated mechanism that gives you an option to deploy the probe version on the required robots.

#### **Follow these steps:**

1. Verify that the local archive includes the appropriate version of the probe that you want to deploy.
2. Open the probe utility for `mon_config_service`.
3. Select **`upgrade_probe_to_eligible_robots`** and specify the value for the following parameters:
  - **`probe_name`**  
Specifies the name of the probe that you want to deploy. For example, `cdm`.
  - **`probe_version`**  
Specifies the version of the probe that you want to deploy. For example, `1.2`.
  - **(Optional) `computer_system_ids`**  
Specifies the robots (`robot_csld`) on which you want to deploy the probe version. Enter the appropriate `robot_csld` value in this field. You can use comma-separated values; for example, `1,2,4`.  
If you do not provide any value, the callback deploys the new probe version on all the robots where the existing probe version is not the same as the new version.

When you run this callback, it deploys the required probe version on all the specified robots. You do not need to manually deploy it on each individual robot.

4. Execute the callback.  
The specified probe version is deployed to all the required robots.
5. Use the `get_robots_not_having_probe` callback to verify whether all required robots have been updated with the requested probe version. Select **`get_robots_not_having_probe`** and specify the value for the following parameters:
  - **`probe_name`**  
Specifies the name of the probe for which you want to find out the robots on which this probe is not deployed. For example, `cdm`.
  - **`probe_version`**  
Specifies the version of the probe for which you want to find out the robots on which this probe version is not deployed. For example, `1.2`.
6. Execute the callback.
7. When you run this callback, it lists all the robots where the specified probe version is not deployed.

You have successfully deployed a probe on all the required robots.

### **Get Devices Not Having Group Profile Deployed**

The `get_devices_not_having_group_profile_deployed` callback lets you get a list of devices that do not have a specified group profile deployed on them.

#### **Follow these steps:**

1. Open the probe utility for `mon_config_service`.
2. Select **`get_devices_not_having_group_profile_deployed`** and specify the list of group profile IDs.
3. Execute the callback.  
All the devices that do not have specified group profile deployed on them are displayed.

### **Copy Configuration Profiles for Consistent Monitoring**

Copying configuration profiles reduces the time that it takes you to configure monitoring for your environment. It also provides consistent monitoring for groups of target devices.

Always test a configuration profile before you copy it. Confirm that the QoS data and alarms that are emitted by the probe are what you expect. When configuration profiles are fully tested, you can copy the configuration to any group or device with a robot. If you later want to make changes, you can copy the group configuration profiles back to a 'test' device.

The system prohibits you from copying invalid targets. In the following scenarios, the system prevents you from selecting invalid targets:

- **Redundant copy:** You cannot select the copy source as a target. If you attempt to perform a duplicate copy operation, you receive a message indicating that the copy operation resulted in no changes.
- **Different Operating Systems:** The copy source and targets should have the same operating system.
- **No robot deployed:** You can only copy or apply configuration profiles to devices that have deployed robots.

When you copy a configuration profile to a group, the configuration is applied to the devices in the group. The group configuration profile for the target group is independent, meaning there is no link to the copy source. All device configuration profiles in the target group correctly show in the profile status that configuration is derived from the group profile.

You can temporarily change configuration settings that are derived from a group profile for any device in a group. These device-level changes are overridden only for the device. You can copy overridden device configuration profiles to any device or group in your environment











### Copy Tested Configuration Profiles

When configuration profiles are fully tested, you can copy the profiles to devices or groups. Copy only applicable configuration profiles to target groups or devices. For example, the *Apache* or *CPU Monitor* configuration profiles are applicable for any device or group. The *Event Log Exclude* or *Windows Services* configuration profiles apply only to Microsoft Windows devices or groups of Windows devices.

#### NOTE

If you inadvertently copy a configuration profile that does not apply to a target group or device, the profile is copied to the target. However, the configuration profile is not applied to the group or device. Delete the profile from the target group or device. See [Delete Monitoring Profiles](#) for information about deleting profiles.

For detailed information about the copy function and user scenarios, see [How to Copy and Apply Profiles in MCS](#). The following screenshot shows the location where you can find the copy profile icon (first icon under the Actions column):

| State                                                                               | Profile Id | Profile name  | Template Name  | Alarm Policy                   | Actions                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------|------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | 93         | CPU Monitor (Enhanced)                                                                           | CPU Monitor (Enhanced)                                                                            | CPU Monitor (Group: Test_Test) |    |
|  | 98         | Test                                                                                             | SQL Server (Enhanced)                                                                             | Test (Group: Test_Test)        |    |

#### NOTE

In UIM 20.3.0, Filter and Activate Filter options have been removed from the monitoring configurations of the MCS templates. You can use the normal drop-down to select the values without any filtering conditions on the values by scrolling the drop-down list.

When you copy a configuration profile to a group, the configuration profile is applied to all devices in the selected group. The copied configuration profile overwrites any existing configuration settings.

When you copy a configuration profile to another device, the configuration profile is only applied to the selected device. If the copy target is a device with a group-level configuration previously applied, any settings on the copied profile override any group settings.



**NOTE**

If a probe license expires after configuration profiles are applied, the probe continues to monitor the device and to emit QoS data and alarms.

**Profile Types That Allow Multiple Configuration Profiles**

Many profile types are restricted to one configuration profile. However, some profile types let you create multiple configuration profiles. Some of the profile types that support multiple profiles are:

- **Log Monitoring** - Create a configuration profile for each log file, web page, message in the queue, or command output you want to monitor. For each log monitoring configuration profile, you can create a sub-profile for exclude rules, exit codes, format rules, and watcher rules to filter what you want to monitor.
- **Processes** - Create a configuration profile for each process you want to monitor on a host operating system.
- **Disk(s)** - Create a configuration profile for each disk or file system you want to monitor.

**Follow these steps:**

1. On the Monitoring Config, click '+' to add a profile.
2. (Optional) Select the **Active** option to make the profile active.
3. Enter a unique profile name.
4. Configure monitoring settings. **Example:** Select the Log Monitoring profile type and configure the general log monitoring settings. Then configure the desired Rules profiles. When **Generate metrics** and **Generate alarms** are enabled, the probe generates QoS metrics and alarms when the content of a monitored log matches the configured exclude rules, exit codes, format rules, or watcher rules profiles.
5. Create this profile.

**Create a Log Monitoring Profile**

The Log Monitoring profile type lets you create an initial profile and one or more Rules sub-profiles. After you create a new Log Monitoring configuration profile, the Exclude Rules, Exit Code Monitoring, Format Rules, and Watcher Rules sub-profiles appear. Configure the desired log monitoring rules.

When you create device log monitoring configuration profiles, you can continue to modify the device configuration settings and add or delete rules at any time. This configuration profile is applied only to the selected device. The same holds true for group configuration profiles.

After group log monitoring configuration profiles are applied to devices in the group, you can override the group configuration for a selected device. There are two ways to do this:

- **Modify a few configuration settings:** Select a device log monitoring profile or one of the associated rules sub-profiles. Modify configured settings to override the group settings for a device. The configuration changes are applied only to the selected device. An \* (asterisk) appears for each setting override. You can revert device overrides back to the group configuration settings by using the Revert arrow. However, you cannot delete the device profiles or sub-profiles. And you cannot add or delete sub-profiles.

**NOTE**

In UIM 20.3.0, you cannot revert device overrides back to the group configuration settings.

- **Modify several configuration settings and add or remove rules:** Select the desired device log monitoring profile. Clear the **Active** option to deactivate the configuration profile for the selected device, and then save the change. For the selected device, create a replacement device log monitoring configuration profile and add rules sub-profiles. At the device level, you can continue to modify device configuration settings and add or remove rules sub-profiles for this new device configuration profile. Group configuration changes are not applied to the new device configuration profile. However, group configuration changes are applied to the deactivated device configuration profile, although changes do not affect log monitoring because the device profile is deactivated.

**NOTE**

If you are using a MySQL database, all sub-profile names must be unique across all monitoring profiles. If you attempt to create a sub-profile with a name that is already in use, an error stating that a duplicate name profile already exists. The system prevents you from creating the new sub-profile with a duplicate name.

**Modify Configuration Profiles**

After configuration profiles are applied to a selected device or a group of devices, you can modify the configuration. Any modifications to a group configuration profile are applied to all devices in the group. Any changes to a device configuration profile are applied *only* to the selected device. The order in which configuration profiles are applied to devices determines if configuration settings are *applied*, *overwritten*, or *overridden*.

**Group Profile Applied**

When you configure group configuration profiles or copy a configuration profile to a group, the group configuration is *applied* to all devices in the group. If this is the first time the group configuration is applied to the group, the group configuration *overwrites* any device configuration settings.

After group configuration profiles are applied, you cannot delete profiles at the device level because device configurations are now derived from the group profile. The delete (trash) icon no longer appears next to the configured profile name at the device level. You can, however, delete group configuration profiles.

**NOTE**

If you inadvertently delete a OC group, the group profiles and any overriding device configuration are removed from devices in the group. If a device is a member of other groups, active group profiles are applied to the device according to the Group Profile Priority (or precedence) assigned to group profiles. The group profile with the highest priority number is applied to the devices in the group.

**Override Group Configuration Settings - Temporary Configuration Changes for Selected Devices**

After group profiles are applied, you can temporarily *override* group configuration settings for a specific device in the group. You might do this while troubleshooting an issue with a specific device. Overriding group configuration settings lets you adjust monitoring settings to generate more reported data only for the selected device. For example, you might select more QoS options or you might adjust thresholds to receive more alarms.

When you override a group configuration setting, an \* (asterisk) appears next to a field name to denote that a setting differs from the group configuration. A **Revert** arrow appears to the right of the profile name. Use the Revert arrow to return the device configuration overrides to the group configuration profile settings. After the revert action completes, any future group configuration profile changes are applied to this device.

**Modify Group Configuration when Device Overrides Exist**

After group configuration profiles are applied to devices in a group, device configuration is derived from the group profile. When group configuration overrides are made on the device level, the override values are applied only to the selected device. Future group configuration changes are not applied to overridden fields, although they are applied to device settings that do not have override values.

**Delete Monitoring Profiles**

You can delete configuration profiles for devices or OC groups when your monitoring requirements change. The system lets you delete a device or group profile one at a time. Deleting a group profile removes the configuration from all devices in a group.

While the delete action is in progress, the affected profiles are locked. When Monitoring Configuration Service removes the configuration from the appropriate devices, the associated probe stops emitting alarms and QoS data.

After profiles are deleted, the Profile Types that are displayed on the **Profiles** tab are reordered. The profile types that had profiles removed are moved to the lower portion of the list of profile types. Profile types that can have multiple configuration profiles are only redistributed within the list of profile types after all profiles have been removed.

### Delete a Group Profile

You can delete group configuration profiles as long as the profiles are not locked. The delete process removes the selected group profile from all devices in the group, including device profiles that override the group profile.

### Delete a Device Profile

You cannot delete device profiles that are derived from group profiles. When a device profile is derived from a group profile, the delete (trash) icon next to the device profile name is replaced by the Revert arrow. Use the Revert arrow to reapply the group profile and remove device overrides.

**Note:** If a target device is unreachable and the retry attempts are exceeded, the configuration profile remains unchanged.

### Delete Configuration Profiles

#### Follow these steps:

1. Navigate to the appropriate device or group.
2. Click the Monitoring Config icon to display the list of created MCS profiles.
3. Locate the profile that you want to delete, and follow one of the methods to delete a profile:
  - Locate the **Actions** column and click the delete profile icon (trash) for the required profile:

| State | Profile Id | Profile name           | Template Name          | Alarm Policy                   | Actions |
|-------|------------|------------------------|------------------------|--------------------------------|---------|
|       | 93         | CPU Monitor (Enhanced) | CPU Monitor (Enhanced) | CPU Monitor (Group: Test_Test) |         |
|       | 98         | Test                   | SQL Server (Enhanced)  | Test (Group: Test_Test)        |         |

- Click the required MCS profile to navigate to the profiles page and use the delete (trash) icon that is displayed in the top-right menu to remove the configuration profile:

Profiles | [Alarm Policies](#) | [MCS Deployment Overview](#)

← Default Disk(s) filter

Parent state      Service

Disk(s) | Sub-profiles available: 0

4. Select **Yes** on the Delete Confirmation dialog.  
Select **No** to cancel the delete request.

While the delete action is taking place, the profile remains visible on the **Profiles** tab but is locked. It can take some time to remove configuration profiles.

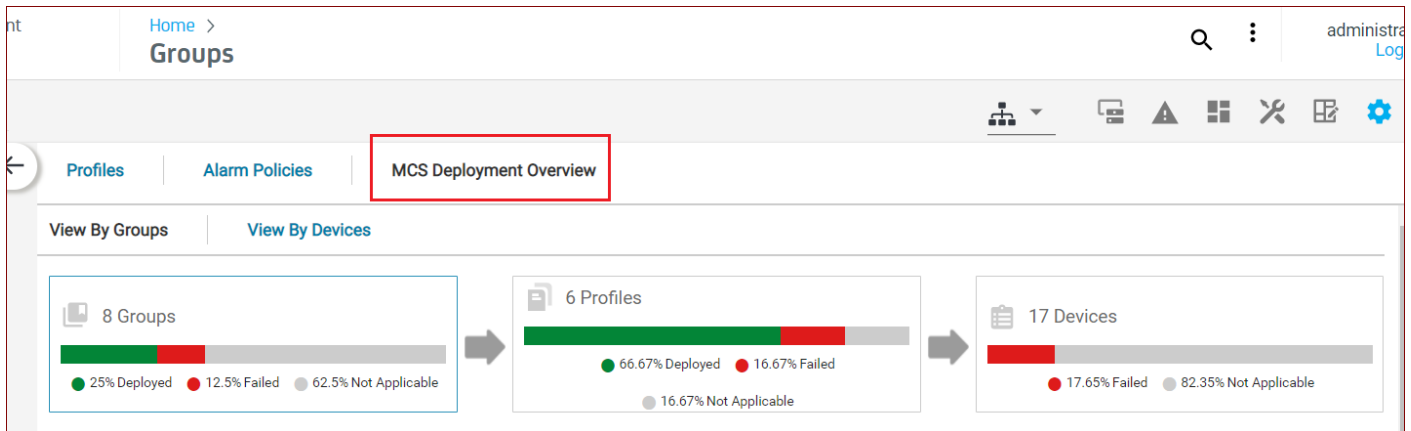
### In-Context Linking of Profiles to MCS Deployment Dashboard

The MCS Deployment Overview tab provides an in-context linking of the profiles to MCS Deployment Dashboard. You can access this tab through the same Monitoring Config icon (gear icon) that you use to access the Profiles and Alarm Policies tabs.

#### Follow these steps:

1. Click the Monitoring Config icon in the top-right menu.

2. Locate the **MCS Deployment Overview** tab next to the **Alarm Policies** tab.



3. Click the **MCS Deployment Overview** tab.
4. Review the information in the **View By Groups** tab and **View By Devices** tab, as required.

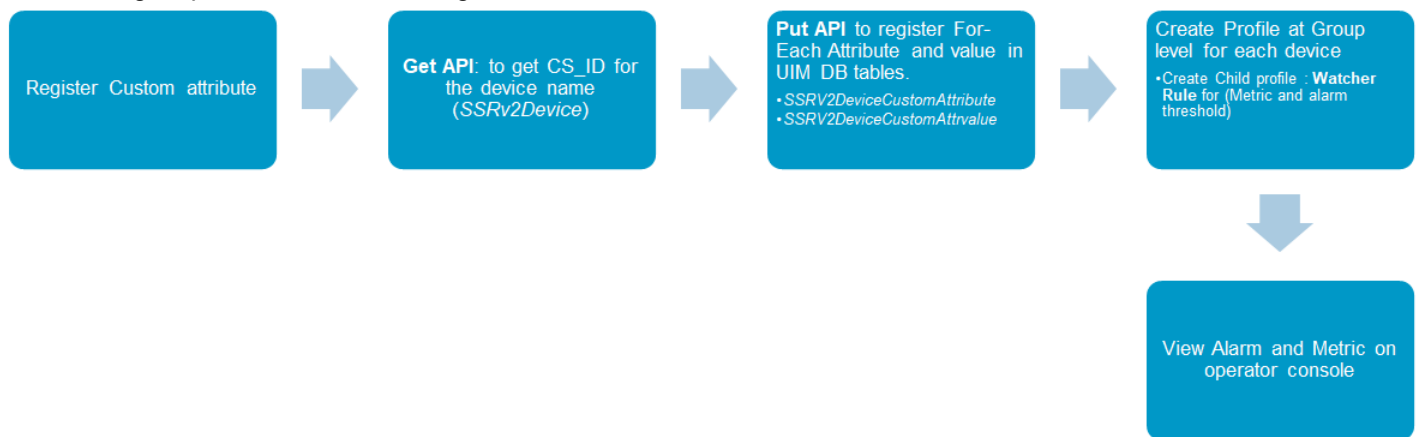
### For-Each Profiles

The For-Each profiles feature is available in the Profiles section of the Monitoring Config in the Operator Console. For-Each functionality supports the Bulk deployment of the profiles at a group level based on custom attribute for each of the devices available in SSRV2DeviceCustomAttribute table. Using this feature, you can create For-Each profile at a group level. While creating the profile, you need to specify on which custom attribute you want to iterate over.

If a device in a group have one instance of Oracle, on another device in the same group have 2 instances of Oracle and so on. In this case, you need to select the Oracle device instance (device.custom.oracleInstance) variable, and can create a profile for every instance of Oracle on the device in the group. If a device has 10 instances, it will create 10 profiles, if a device has 1 instance it will create 1 profile and so on.

### Process to use For-Each profiles

The following steps are needed for using the For-Each feature



1. Register a Custom attribute for a device in database on which the values can be iterated to create profile should be present.  
Device custom attributes can be present in ssrv2devicecustomattribute, and ssrv2devicecustomattrvalue tables.

2. If the Device custom attributes are not present, they can be created using manual sql scripts or uimapi (<http://<uimserver>/uimapi>) under DeviceOperations (/PUT /deviceoperations/{identifier}). Sample device payload to insert with custom attributes is given below as an example which can be executed through UIMAPI.

- a. Perform GET API call to get the device payload using name
- b. Modify the payload and add the custom attribute elements. Sample payload is shown below:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<device>
 <cs_id>1</cs_id>
 <device_id>1</device_id>
 <csdev_id>D86221456EEA5CF0ABEE4A804860767FF</csdev_id>
 <name>pp671588-win1</name>
 <status>modified</status>
 <custom1>device.name</custom1>
 <origin>pp671588-win1_hub</origin>
 <os_type>Windows</os_type>
 <nimbus_type>2</nimbus_type>
 <ip>10.17.165.209</ip>
 <cs_type>A</cs_type>
 <customattribute>
 <name>custom.instance</name>
 <scope>default</scope>
 <value>4</value>
 <value>D:\testdr</value>
 <encrypted>true</encrypted>
 </customattribute>
 <customattribute>
 <name>custom.pandu.instance</name>
 <scope>default</scope>
 <value>5</value>
 <value>E:\testdr</value>
 <encrypted>true</encrypted>
 </customattribute>
 <customattribute>
 <name>device.usertag1</name>
 <scope>default</scope>
 <encrypted>true</encrypted>
 <modified>0</modified>
 </customattribute>
 <customattribute>
 <name>device.usertag2</name>
 <scope>default</scope>
 <encrypted>true</encrypted>
 <modified>0</modified>
 </customattribute>
 <customattribute>
 <name>device.origin</name>
 <scope>default</scope>
 <value>pp671588-win1_hub</value>
 <encrypted>true</encrypted>
 <modified>0</modified>
 </customattribute>
 <customattribute>

```

```
<name>device.ipaddress</name>
<scope>default</scope>
<value>10.17.165.209</value>
<encrypted>true</encrypted>
<modified>0</modified>
</customattribute>
<customattribute>
 <name>device.name</name>
 <scope>default</scope>
 <value>pp671588-win1</value>
 <encrypted>true</encrypted>
 <modified>0</modified>
</customattribute>
<customattribute>
 <name>device.os_type</name>
 <scope>default</scope>
 <value>Windows</value>
 <encrypted>true</encrypted>
 <modified>0</modified>
</customattribute>
<deviceattribute>
 <name>Origin</name>
 <scope>default</scope>
 <value>pp671588-win1_hub</value>
</deviceattribute>
<deviceattribute>
 <name>RobotInstanceId</name>
 <scope>default</scope>
 <value>D86221456EEA5CF0ABEE4A804860767FF</value>
</deviceattribute>
<deviceattribute>
 <name>DisplayAlias</name>
 <scope>default</scope>
 <value>pp671588-win1</value>
</deviceattribute>
<deviceattribute>
 <name>PrimaryIPV4Address</name>
 <scope>default</scope>
 <value>10.17.165.209</value>
</deviceattribute>
<deviceattribute>
 <name>typeName</name>
 <scope>default</scope>
 <value>ComputerSystem</value>
</deviceattribute>
<deviceattribute>
 <name>PrimaryRole</name>
 <scope>default</scope>
 <value>Host</value>
</deviceattribute>
<deviceattribute>
 <name>Roles</name>
 <scope>default</scope>
```

```
<value>Device</value>
<value>Host</value>
</deviceattribute>
<deviceattribute>
 <name>label</name>
 <scope>default</scope>
 <value>pp671588-win1</value>
</deviceattribute>
<deviceattribute>
 <name>PrimaryOSType</name>
 <scope>default</scope>
 <value>WindowsServer-2012-R2</value>
</deviceattribute>
<deviceattribute>
 <name>RobotName</name>
 <scope>default</scope>
 <value>pp671588-win1</value>
</deviceattribute>
<deviceattribute>
 <name>CorrelationNames</name>
 <scope>default</scope>
 <value>pp671588-win1</value>
</deviceattribute>
<deviceattribute>
 <name>DisplayName</name>
 <scope>default</scope>
 <value>pp671588-win1</value>
</deviceattribute>
<deviceattribute>
 <name>CorrelationId</name>
 <scope>default</scope>
 <value>D86221456EEA5CF0ABEE4A804860767FF</value>
</deviceattribute>
<deviceattribute>
 <name>OSDescription</name>
 <scope>default</scope>
 <value>Service Pack 0 Build 9600</value>
</deviceattribute>
<deviceattribute>
 <name>PrimaryOSVersion</name>
 <scope>default</scope>
 <value>6.3.9600</value>
</deviceattribute>
<deviceattribute>
 <name>PrimaryMacAddress</name>
 <scope>default</scope>
 <value>00-50-56-8D-E9-0A</value>
</deviceattribute>
<deviceattribute>
 <name>RobotVersion</name>
 <scope>default</scope>
 <value>9.2</value>
</deviceattribute>
```

```
</device>
```

3. Perform PUT operation /PUT/deviceoperations/{identifier} using the modified payload containing the device custom attributes.

The device custom attributes and their values are populated in `ssrv2devicecustomattribute`, `ssrv2devicecustomattrvalue` tables respectively. For a device, there are three entries in `ssrv2devicecustomattribute`, `ssrv2devicecustomattrvalue` tables and monitoring the log files `C:\Test\Log1.log`, `C:\Test\Log2.log`, `C:\Test\Log3.log`, `C:\Test\Log4.log`, `C:\Test\Log5.log`, `C:\Test\Log6.log`. The for-each profile is created for each of the values of log file directories with custom attribute `{device.logfilepath}` defined in database.

4. Once For-Each profile is created at group level, the device attribute values selected are iterated to create profiles at device level and alarms are raised matching the threshold.
  - a. The below are the operations performed using For-Each profiles.
    - a. Monitors all log files on a particular device.
    - b. Notifies if "error" string exist in each log file (If "error" is selected while profile creation).
    - c. Count of string "error" from the log files.
    - d. Alert if the count is greater than the specified values in the Metric Definition as per the defined Alarm severity.

### **For-Each Profile Creation Example**

With this example, you can create a For-Each profile using the logmon template to raise alarms when the text "error" is found in the log files .

- Click on the Log Monitoring (Enhanced) profile under Monitoring Config of a group and click + icon. Select For-Each deployment as 'yes' .

"For-Each Value of" specifies the attribute on which the For-Each profile is created.

#### **For-Each Deployment**

Enable

Yes

For-Each Group Profile Name

Log Monitoring (Enhanced)

For-Each Value Of

device.logfilepath

Matching Expression

#### **Group Profile Settings**

- Provide the Profile Name details as `FED{foreach-instance}`  
In this example, `{foreach-instance}` is substituted with value of `{device.logfilepath}` for the device.



## Log Profile

Active

Profile Name

FED{foreach-instance}

*{Variables} are substituted with actual values.*

Mode

cat

Log File or Command \*

{foreach-instance}

*{Variables} are substituted with actual values.*

Log File/Command Encoding

Default

- Click on save after setting the alarm message to match.
- Create watcher rule in the Enhanced Profile to match the pattern for creating alarm on log file. Search for the string 'error' and configure thresholds.

## Log Monitoring Watcher Rule Definition

Active

Profile Name  
FindError

---

Pattern to Match  
error

---

Severity  
Major

---

Alarm Message on Match

---

Suppression Key

- Click on save for creating the For-Each profile at a group level.
- The profiles are created at device level for each of the custom attributes configured for the device. In this case we will have 6 profiles created as below.

|  |                    |                           |        |       |
|--|--------------------|---------------------------|--------|-------|
|  | FEDC\Test\Log1.log | Log Monitoring (Enhanced) | 4.15.1 | Group |
|  | FEDC\Test\Log2.log | Log Monitoring (Enhanced) | 4.15.1 | Group |
|  | FEDC\Test\Log3.log | Log Monitoring (Enhanced) | 4.15.1 | Group |
|  | FEDC\Test\Log4.log | Log Monitoring (Enhanced) | 4.15.1 | Group |
|  | FEDC\Test\Log5.log | Log Monitoring (Enhanced) | 4.15.1 | Group |
|  | FEDC\Test\Log6.log | Log Monitoring (Enhanced) | 4.15.1 | Group |

- The instance variables are substituted at device level for profile name.
- The alarms are raised once the string "error" is matched in log files.

| <input type="checkbox"/> |  | Device Name | Actions | Alarm Type | Owner      | Alarm Message       |
|--------------------------|--|-------------|---------|------------|------------|---------------------|
| <input type="checkbox"/> |  | ibnqa003721 | ⋮       | Alarm      | Unassigned | FEDC:\Test\Log6.log |
| <input type="checkbox"/> |  | ibnqa003721 | ⋮       | Alarm      | Unassigned | FEDC:\Test\Log3.log |
| <input type="checkbox"/> |  | ibnqa003721 | ⋮       | Alarm      | Unassigned | FEDC:\Test\Log4.log |
| <input type="checkbox"/> |  | ibnqa003721 | ⋮       | Alarm      | Unassigned | FEDC:\Test\Log2.log |
| <input type="checkbox"/> |  | ibnqa003721 | ⋮       | Alarm      | Unassigned | FEDC:\Test\Log1.log |

## Considerations

- For-Each does not create default alarm policies. As a pre-requisite, disable the flag `policy_mode_enabled = false` in `mon_config_service` probe under `configure/timed` section. The thresholds are configured at template level.
- For-Each profile is not supported at child template level, but sub profiles can be created. For-Each attribute is enabled at group level for parent templates having maximum profile count as `> 1`.
- For-Each flag is visible in the UI for those templates which do not have parent template. Maximum profiles that can be created are more than 1.

## Enable Read-Only Access to MCS Profiles

UIM now allows users to have read-only access to the MCS profiles. This ensures that only relevant users are allowed to perform the required operations on the profiles. To enable this functionality, a new permission (MCS Read-Only Access) is now available. Users with this permission can only view the profile; they cannot edit, create, or delete it. You must add the permission to the ACL list.

### Follow these steps:

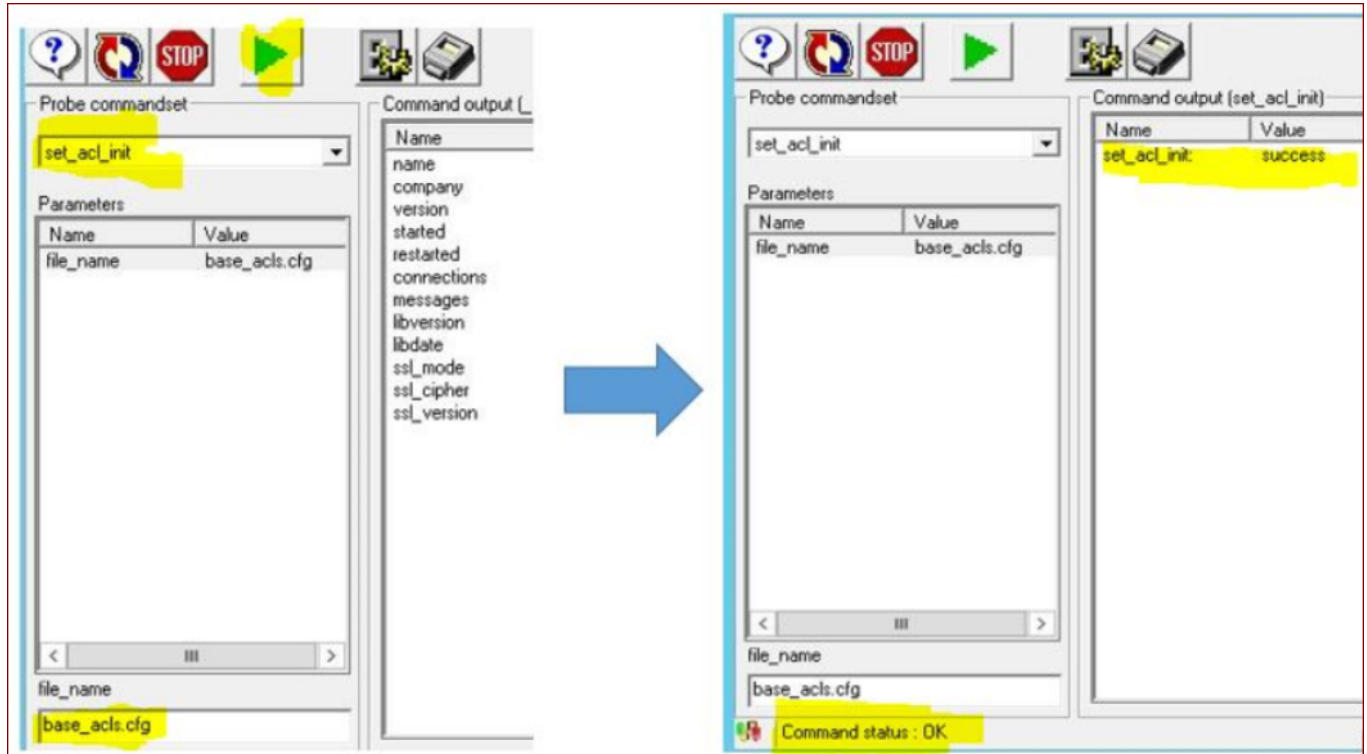
1. Add the permission (MCS Read-Only Access) to the ACL list.
  - a. Access the primary hub and open the `..\Nimsoft\probes\service\distsrv\base_acs.cfg` file in a text editor.
  - b. Add the permission section to the file.

The following snippet shows that the `<MCS Read-Only Access>` section is added to the file:

```
<MCS Read-Only Access>
 name = MCS Read-Only Access
 desc = Read-only view access for any MCS profiles
 type = UMP
 access = read
</MCS Read-Only Access>
```

- c. In Infrastructure Manager, navigate to the `distsrv` probe on the primary hub.
- d. With the `distsrv` probe selected, press `Ctrl-P` to open the probe Utility (pu).
- e. In the probe commandset, select the `set_acl_init` callback with the parameter value as `base_acs.cfg`. The callback updates the `security.cfg` with the ACLs; it does not delete or change any ACLs.

The following screenshot shows the required information:

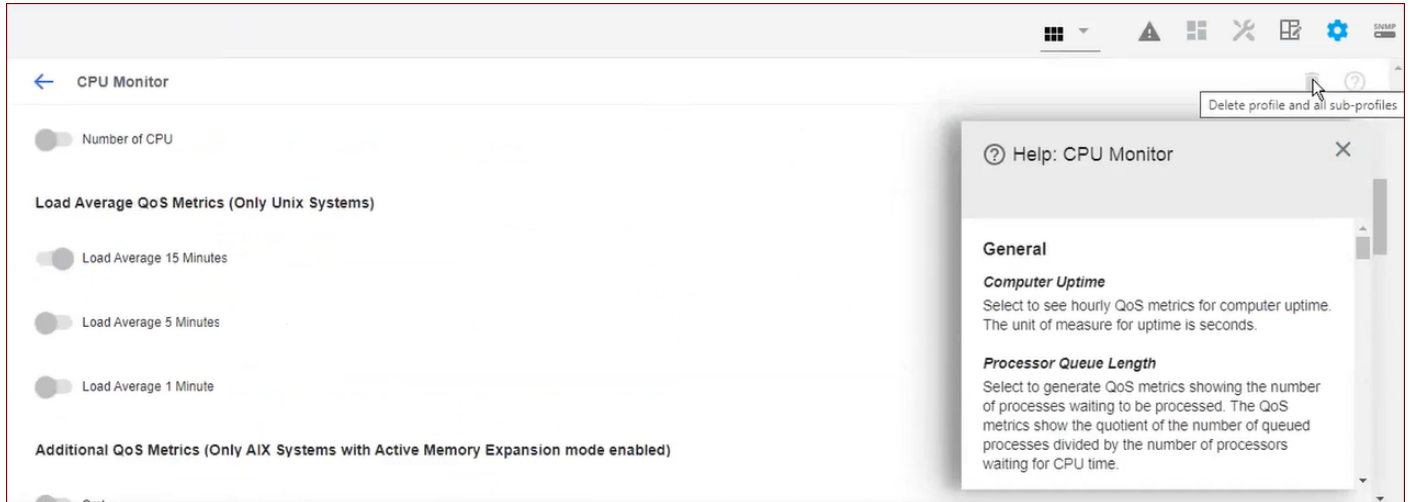


- f. In infrastructure manager, open **Security, Manage Access Control List**.
  - g. Verify that the ACL list has the required permission added to it.
2. Ensure that the write permission (OC Monitoring Configuration Service) is cleared and the read-only permission (MCS Read-Only Access) is selected for the user.
  3. Log in to the OC UI using the required user credentials.
  4. Access the MCS profile.
  5. Verify that the user can only view the profile information and configuration settings. Review the following points in the UI:
    - a. User cannot add a new profile.
    - b. User cannot edit the existing profile configuration settings.
    - c. User cannot delete the existing profile.

The following example screenshot shows that the add option is disabled for this user:

| State | Profile name               | Template Name              | Template version | Profile type | Alarm Policy                             |
|-------|----------------------------|----------------------------|------------------|--------------|------------------------------------------|
|       | CPU Monitor                | CPU Monitor                | 2.54             | Device       |                                          |
|       | CPU Monitor (Enhanced)     | CPU Monitor (Enhanced)     | 6.50.1           | Device       | CPU Monitor (Device: sg036804W12VM2)     |
|       | Default Disk(s) (Enhanced) | Default Disk(s) (Enhanced) | 6.50.1           | Device       | Default Disk(s) (Device: sg036804W12VM2) |
|       | Disk IO Monitors           | Disk IO Monitors           | 1.15             | Device       |                                          |

The following example screenshot shows that the delete option and configuration settings are disabled:

**NOTE**

The same behavior is also applicable for the sub-profiles.

You have successfully provided the read-only access to users for viewing the MCS profiles.

## How to Copy and Apply Profiles in MCS

This article describes the best practices for copying and applying profiles in Monitoring Configuration Services (MCS). This document also gives some business use case examples. The examples demonstrate best practices.

Using MCS, you can copy a device or a group profile (the source) and apply the copied profile to a device or a group profile (the target). When you apply a profile at the group level, MCS applies this profile to all devices within the group. Device level configuration overrides the group level configuration. When you copy and apply a profile, MCS analyzes the source against the target. What MCS does after analyzing the source against the target depends on whether the group has a previously configured group profile.

### Copy and Apply a Profile

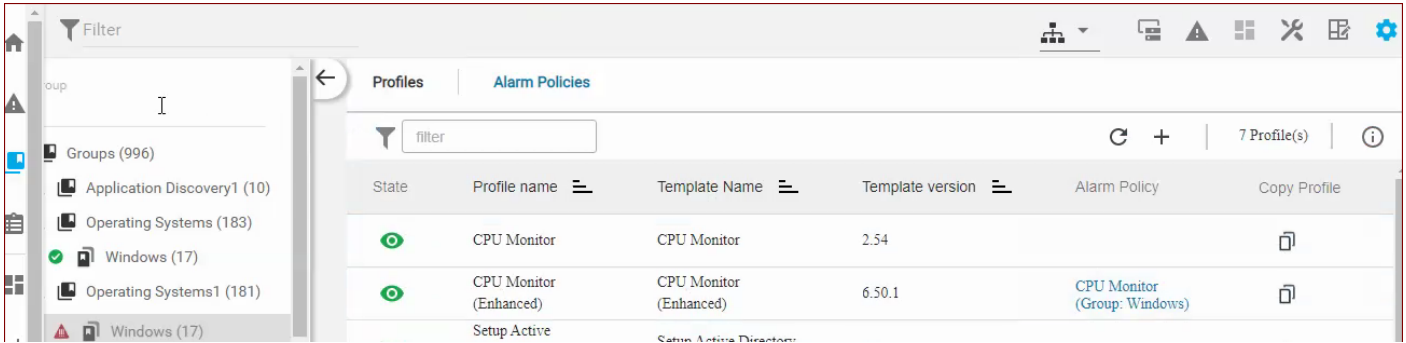
This procedure includes high-level steps that help you understand how you can copy and apply profiles.

**NOTE**

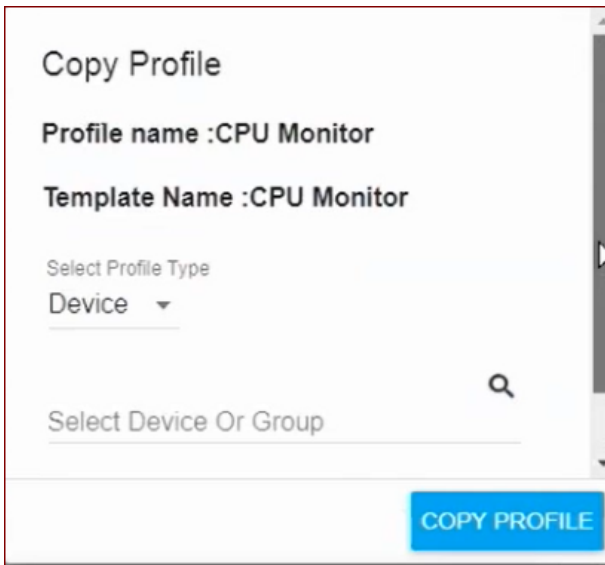
For detailed information about specific scenarios and best practices, see the Best Practices and Examples sections.

#### **Follow these steps:**

1. From the Inventory view or Group view, navigate to the appropriate group or device.
2. Click the Monitoring Config icon (gear icon) available in the top-right corner.
3. Locate the group or device profile (as applicable) that you want to copy and apply.

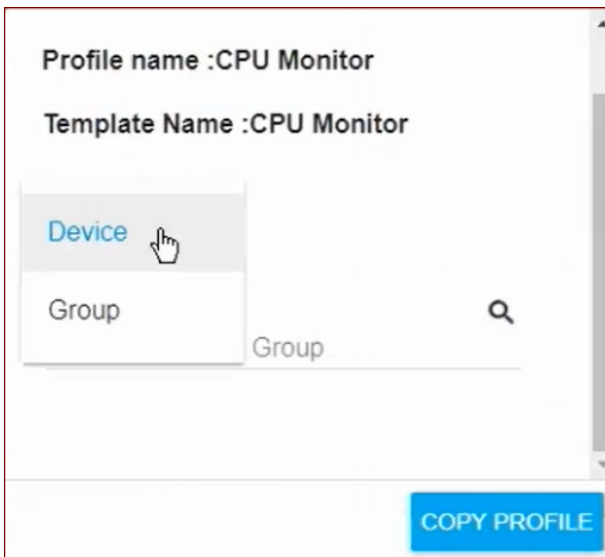


4. Click the **Copy Profile** option.

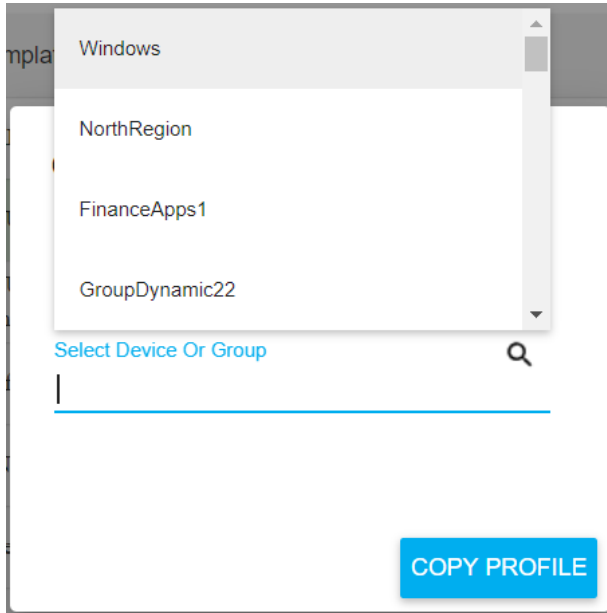


The **Copy Profile** dialog opens.

5. Select whether you want to apply the profile to a group or device.



Depending on your selection, the **Search Device Or Group** field is populated with a list of related devices or groups. Click the field to view the list



6. From the list, select the required group or device (as applicable) where you want to apply the profile.
7. Click the **Copy Profile** button.  
The profile is applied to the intended device or group.

### **Best Practices**

When using MCS, it is most efficient to first create a device profile. Then, you can test it and can modify it as needed. Only copy and apply tested device profiles to a device or group in a production environment. When you monitor with MCS, we recommend that you follow this process:

1. Create and configure a device profile.
2. Modify and test the device profile in an isolated test environment.
3. Determine how you want to group your devices.
4. Copy and apply the device profile to the desired devices or groups.
5. Repeat steps 1-4 as you make configuration changes to your production environment.

### **Examples**

These examples show some common use cases.

#### **Copy and Apply a Device Profile to a Group (Not Having a Group Profile)**

When you copy and apply a profile to a group that does not have a group profile:

- The applied profile becomes the group profile.
- All devices inherit the group profile.
- The group profile is the effective configuration for all the devices in the group.

This enables you to start with one device profile and then to standardize it for a group profile.

In this example, you are setting up a new call center. You create a group that is named Call Center 2. The Call Center 2 group does not have a group profile.

In your Call Center 2 group, you have three devices:

- **Accounts 2**

The device Accounts 2 does not have a device profile.

- **Brokerage 2**

The device Brokerage 2 has a device profile.

- **Fraud 2**

The device Fraud 2 does not have a device profile.

You want to create a device profile in your test environment and, after testing it, apply it to the Call Center 2 group.

Following best practices, you use a test server to develop the new CPU Monitor device profile. In this example, we assume that you have a test server that is named Fraud Test 2.

**Follow these steps:**

1. Create a CPU Monitor device profile on Fraud Test 2.
2. Modify and test the CPU Monitor device profile on Fraud Test 2.
3. Copy the CPU Monitor device profile from Fraud Test 2.
4. Apply the CPU Monitor device profile to the Call Center 2 group profile in your production environment.

When you apply the CPU Monitor device profile to the Call Center 2 group in your production environment:

- The source, the CPU Monitor device profile from Fraud Test 2, becomes the group profile for the Call Center 2 group.
- The Accounts 2 device, which did not have a device profile, now inherits the group profile for the Call Center 2 group.
- The Brokerage 2 device, which had a device profile, retains the device profile.
- The Fraud 2 device, which did not have a device profile, now inherits the Call Center 2 group profile.

**Copy and Apply a Device Profile to a Device (Inheriting a Group Profile)**

In this example, you have a group that is named Factory. The Factory group has a CPU Monitor group profile. In the Factory group you have two devices:

- **Manufacturing**

The Manufacturing device has a CPU Monitor device profile that it inherits from the Factory group profile. You have not modified the inherited profile for Manufacturing. It is therefore identical to the Factory group profile.

- **Distributing**

The Distributing device has a CPU Monitor device profile that it inherits from the Factory group profile. You have not modified the inherited profile for Manufacturing. It is therefore identical to the Factory group profile.

You want to modify the configuration for the Distributing device. You want the Distributing device profile to include metrics from the Factory group profile and more metrics. You also plan to add many more devices to the Factory group. You want these many devices to inherit the configuration from the Factory group profile.

Following best practices, you:

1. Use a test server to develop the new CPU Monitor device profile for the Distributing device.  
In this example, we assume that you have a test server that is named Distributing Test.
2. Copy the CPU Monitor device profile from the Distributing device in your production environment.
3. Apply the CPU Monitor device profile to the Distributing Test device in your test environment.
4. Modify and test the CPU Monitor device profile on Distributing Test.
5. Copy the CPU Monitor device profile from Distributing Test.
6. Apply the CPU Monitor device profile to the Distributing device in your production environment.

When you apply CPU Monitor device profile to the Distribution device in your production environment:

- The Distributing Test profile becomes the device profile for only the Distributing device. It affects no other devices within the group.
- The effective profile for the Distributing device is a merge of the device profile and the Factory group profile. Device level configuration takes precedence over group level configuration. Therefore:



- MCS ignores the data in any field that is identical for the group profile and the new device profile.
- MCS overrides the data in any field where there is a difference between the group profile and the new device profile.

### **Copy and Apply a Device Profile to a Device (Not Inheriting a Group Profile)**

In this example, you have a group that is named Development. The Development group does not have a group profile. Within the Development group, you have two devices.

- **Engineering**  
The Engineering device does not have a device profile.
- **QA**  
The QA device does not have a device profile.

You want to create a CPU Monitor device profile for the QA device. You want to include a few metrics for the QA device that you do not want to apply to any other device in the Development group. You also plan to add many more devices to the Development group. You do not want these many devices to use the QA device profile.

You decide to create, test, and apply a CPU Monitor device profile to the QA device.

Following best practices, you:

1. Use a test server to develop the new CPU Monitor device profile for the QA device.  
In this example, we assume that you have a test server that is named QA Test.
2. Create a CPU Monitor device profile on QA Test.
3. Modify and test the device profile on QA Test.
4. Copy the device profile from QA Test.
5. Apply the device profile to the QA device in your production environment.

When you apply the device profile to the QA device in your production environment:

- The QA Test profile becomes the device profile for only the QA device.
- The Engineering device still does not have a device profile.
- The Development group still does not have a group profile.

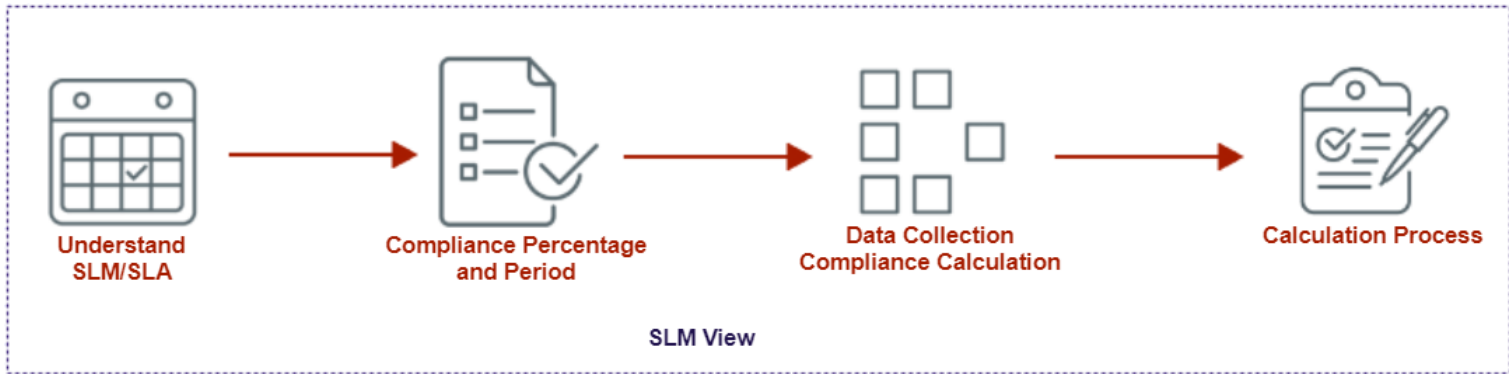
## **The SLM View**

(From 20.3.1) In the Service-Level Management (SLM) view, you create service-level agreements (SLAs) and their component service-level objectives (SLOs) and quality of service (QoS) constraints. With this tool, you can build powerful, extensible, and measurable agreements with clients. Once you define SLAs in the SLM view, data is recorded and compliance is computed automatically.

### **NOTE**

You must have the SLM Admin permission set in the Access Control List (ACL) to view the contents of the SLM interface. If you do not have permissions or you are an account user, regardless of permissions, a "Permission Denied" message appears when you try to open the SLM view.

The following illustration provides an overview of the information covered in this article:



### **About SLM and SLAs**

SLM is an industry-standard framework that is used for the primary management of network and application services. SLM uses a hierarchical set of measurable criteria to monitor and ensure the validity of SLAs between customers and service providers. Among other aspects, SLAs typically define a service provider's hours of operation, maintenance windows, up-time guarantees, timeliness in responding to issues, recovery aspects, and service performance.

The components of SLM form the following hierarchy:

- Service level agreements (SLAs). SLAs typically define a service provider's hours of operation, maintenance windows, uptime guarantees, timeliness in responding to issues, recovery aspects, and service performance. Operational aspects of SLAs are defined in one or more SLOs.
  - Service level objectives (SLOs). SLOs are specific measurable characteristics of the SLA, such as availability, throughput, frequency, response time, or quality. System component measurements that support SLOs are defined in one or more quality of service (QoS) constraints.
    - Quality of Service (QoS) constraints. QoS constraints specify source, target, threshold, and operating period settings, and are combined to produce the SLO achievement value.

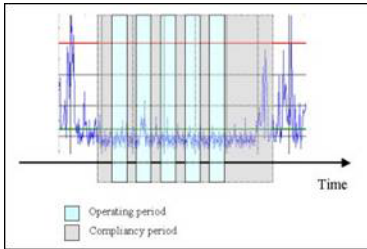
### **Compliance Percentage and Compliance Period**

A compliance percentage is the percentage of time that QoS constraints meet defined thresholds for the QoS object and its SLA. SLM checks each data sample for a defined QoS object, compares the value to the defined threshold, summarizes it as failed or successful, and calculates the percentage of samples that exceed ("breach") the threshold.

Compliance percentage is calculated according to the threshold appropriate to the QoS object: Some QoS constraints require a minimum performance measure (such as speed), a maximum performance measure (such as capacity), or a numerical performance measure (such as queue length). Thresholds can be calculated according to different calculation methods: best value, worst value, mean value, or number.

Compliance is tracked over time in two ways: the compliance period and the operating period. The compliance period is the overall contract period for the SLA, measured in days, weeks, or months. The operating period is the business-critical period within the compliance period, such as active business hours, and is defined in hours during calendar days. Operating periods are defined at the QoS object level. If no operating period is defined, the operating period and the compliance period are the same.

SLM creates a graph for each QoS metric defined in the SLA, including the sampled data, compliance threshold, and compliance period. In the following example, the red line represents the threshold value, the blue line represents the actual sample values, and the green line represents the average value of the data samples throughout the compliance and operating periods.



In this example, none of the samples breach the threshold line within the operating periods, which means that compliance is 100%. Samples that exceed the threshold value fall outside of the compliance period. Those samples can be specifically excluded from the compliance period for system maintenance or other foreseen downtime.

When a QoS metric breaches the object threshold, the compliance percentage is reduced according to the percentage of time that the threshold is breached. For example, if the total number of samples within the operating period is 129 and 9 samples breach the threshold, 6.98% ( $9 * 100/129$ ) of the samples would be out of compliance.

Compliance values for multiple QoS objects are summed for their assigned SLOs and compliance values for multiple SLOs are summed for their assigned SLAs. In this example, if this QoS object is the only one defined in the SLA and the SLA required 98.50% or better compliance, the SLA would be breached due to a QoS compliance percentage of 93.02% ( $100\% - 6.98\%$ ).

### **Calculation Terms and Conditions for the QoS Object**

The QoS reflects the data series that is measured by monitoring probes. The compliance percentage is calculated for each QoS object, and the results are presented to the SLO.

The compliance percentage for a QoS object is calculated based on the following settings:

- **Threshold value** - A threshold defines a maximum or minimum value for each QoS object. Each sample in the data series that a probe collects is evaluated to determine whether it meets or exceeds the threshold.
- **Operating period** - The operating period defines the time interval for a compliance percentage. Only data samples from within the operating period influence the compliance percentage.
- **Calculation method** - The Calculation method is the way the compliance percentage is calculated for the QoS object.

These settings are set in the **Quality of Service Constraints** dialog.

### **Calculation Terms and Conditions for the SLO**

The SLO receives the compliance calculations from the associated QoS objects. The compliance percentage is calculated on each SLO, and the result is presented to the SLA.

The compliance percentage on the SLO is calculated, based on three different parameters:

- **Excluded period** - Data collected within an excluded period is not considered when compliance is calculated for an SLO. For example, excluded periods might be days and times when the monitored system shut down for maintenance.
- **Calculation method** - The calculation method that you select determines how the compliance percentage is calculated.

Select between two different types of calculation methods: **Formula** or **Profile**:

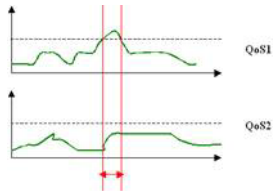
- **Formula** - Select a mathematical formula to calculate the compliance percentage based on the input from a QoS:
  - **Average** - Calculates the average value of the input from the monitoring probes.
  - **Best** - Looks for the QoS object with the best result and selects this result.
  - **Sequential** - The difference between 100% and the achieved compliance for each QoS object is summarized and then extracted from 100%.

**Example:** The SLO receives the compliance calculations from two QoS objects with compliance of 70% and 90%.

Calculated compliance:  $100\% - ((100\% - 70\%) + (100\% - 90\%)) = 60\%$ .

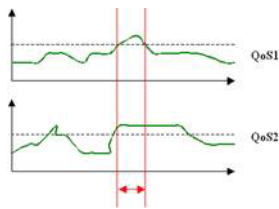
- **Weight** - Weights the relative importance of the different QoS objects.
- **Worst** - Looks for the QoS object with the worst result and selects this result.
- **Profile** - Select one or more conditions to determine compliance:
  - **AND** - The values of **all** samples in **all** QoS objects must meet or be better than the QoS threshold values for the SLO to be in compliance.
  - **OR** - The values of **all** samples in **any single** QoS object must meet or be better than its threshold value for the SLO to be in compliance.

#### Example Using AND



In the preceding example using AND, both data series must be equal to or better than the expected value. This condition is achieved except for the period marked red.

#### Example Using OR



In the preceding example using OR, at least one of the data series must be equal to or better than the expected value. In the previous example, this condition is achieved except for the period marked red.

### Calculation Terms and Conditions for the SLA

The SLA receives the compliance calculations from the associated SLOs and calculates the total compliance percentage based on three different parameters:

- **Operating period** - The operating period defines the critical days and times that compliance is measured (for example, Monday to Friday from 08:00 - 17:00). Only data series gathered within this period determine compliance percentages.
- **Weight** - Weight is the relative importance of the different SLOs to SLA compliance.
- **Calculation method** - The calculation method is the mathematical formula for calculating the SLA compliance percentage from SLOs:
  - **Average** - Calculates the average value of the input from the SLOs.
  - **Best** - Looks for the SLO with the best result and selects this result.
  - **Sequential** - The difference between 100% and achieved compliance for each SLO is summarized and extracted from 100%.

**Example:** The SLA receives the compliance calculations from two SLOs with compliance of 70% and 80%.

Calculated compliance:  $100\% - ((100\% - 70\%) + (100\% - 80\%)) = 50\%$ .

- **Weight** - Weighs the relative importance of the different SLOs.
- **Worst** - Looks for the QoS with the worst result and selects this result.

## Data Collection and Compliance Calculation

QoS-enabled probes monitor and report changes and threshold breaches. QoS-enabled probes, such as cdm (the CPU, Disk, and Memory monitoring probe), generate messages for QoS objects that contain sampled data.

The data\_engine probe subscribes to the primary hub to receive messages that are collected by QoS-enabled probes. QoS-enabled probes initiate themselves during startup by sending a QOS\_DEFINITION message. The data\_engine probe picks up and decodes this message, and then inserts it into the database.

The sla\_engine probe retrieves the data that the data\_engine probe inserts into the database. The sla\_engine probe performs calculations according to the SLA settings and writes the results back into the database. Calculation jobs are automatically started and run on a schedule that is specified in the sla\_engine probe UI.

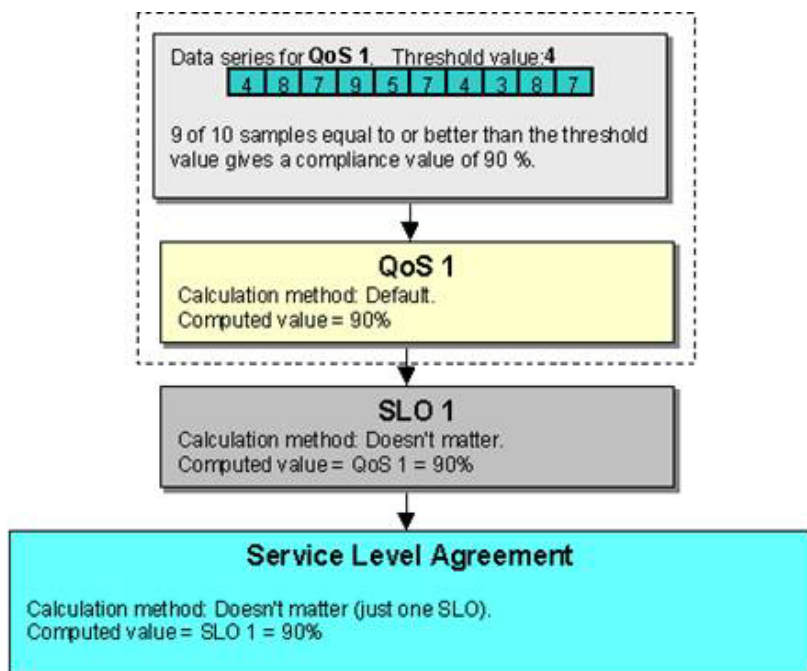
Calculation jobs also can be started manually.

## Calculation Process

The high-level process for calculating SLA compliance includes calculations at each level in the heirarchy, from bottom to top.

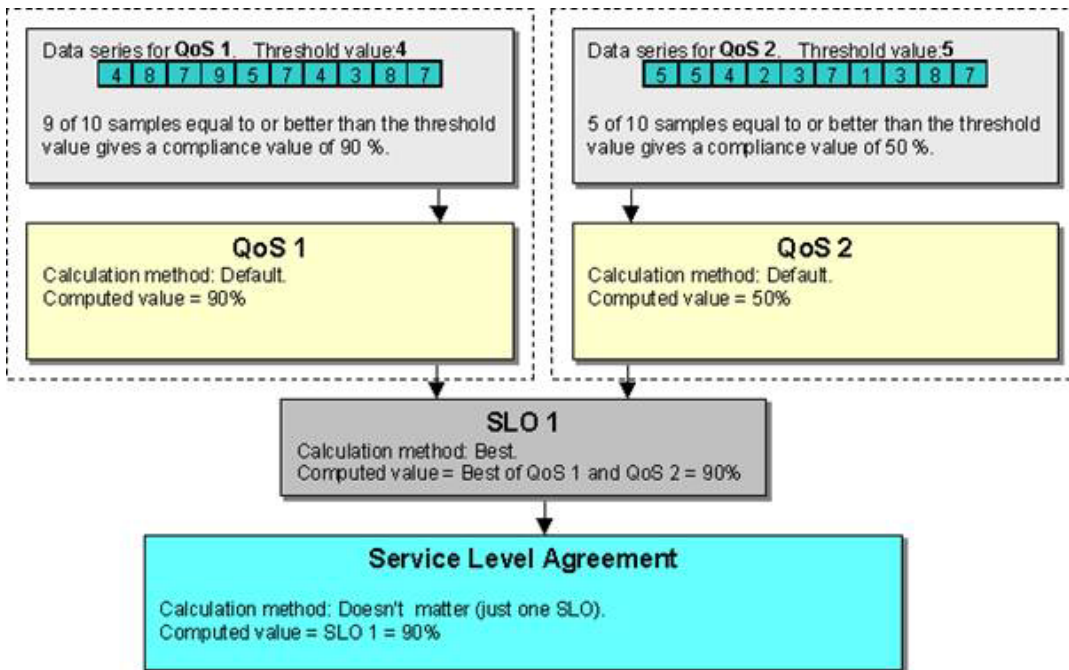
1. Each of the QoS constraints compares the collected data values from the probes with the defined threshold value and calculates the compliance percentage.
2. The SLO collects the compliance values from the QoS constraints and computes the compliance percentage based on a selected calculation method (selects the best value, the worst value, the average value, etc.).
3. The SLA collects the compliance value from the SLOs and calculates the total compliance value, also based on a selected calculation method.

### Example 1: One QoS and One SLO

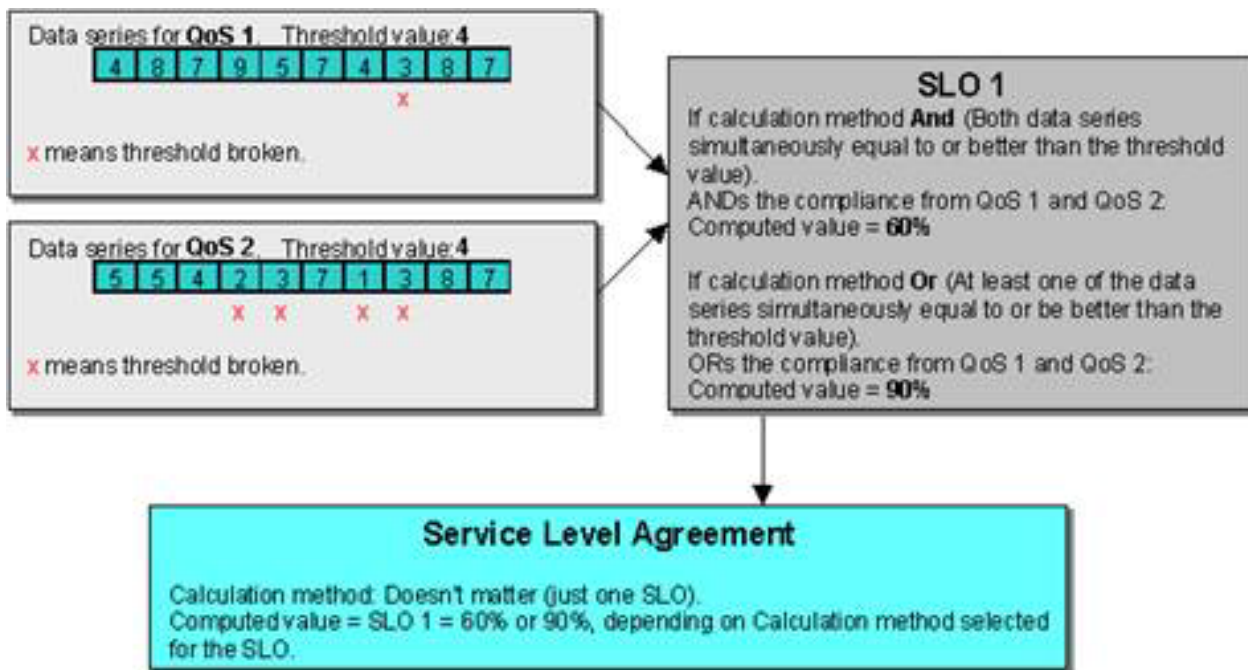


### Example 2: Two QoSs and One SLO

If using a calculation method other than Default for the QoS.



**Example 3: Two QoSs and One SLO, Using Calculation Method AND or OR**

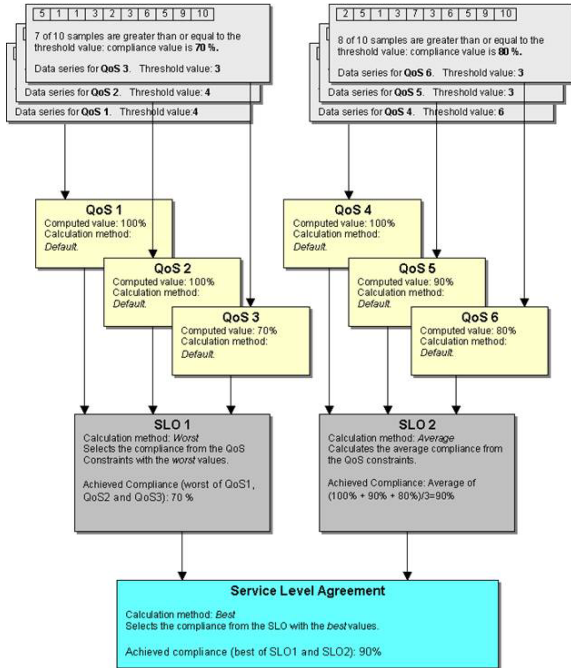


**Example 4: Two SLOs, Each with Three QoS**

This example uses a calculation method other than Default for the QoS.  
 In the following figure:

- SLO 1: - Calculating the compliance percentage from QoS 1, 2, and 3 using calculation method Worst yields a compliance percentage of 70%.
- SLO 2: - Calculating the compliance percentage from QoS 4, 5, and 6 using calculation method Average yields a compliance percentage of 90%.

The table below the figure shows the total SLA compliance percentage, using different calculation methods for the SLA.



The table shows the SLA compliance percentage for the previous example, selecting different calculation methods for the SLA:

| Calculation method | Achieved compliance | Explanation                                                                                                                                             |
|--------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Average            | 80%                 | The average value of the two SLOs (70% + 90%)/2                                                                                                         |
| Best               | 90%                 | The best value of the two SLOs (70% and 90%)                                                                                                            |
| Worst              | 70%                 | The worst value of the two SLOs (70% and 90%)                                                                                                           |
| Sequential         | 60%                 | The difference between 100 % and achieved compliance for each SLO is summarized and extracted from 100%:<br>$100\% - ((100\% - 70\%) + (100\% - 90\%))$ |
| Weight             | 82%                 | Assuming that the weight distribution between SLO 1 and SLO 2 is set to 40 / 60 for the SLA:<br>$(70\% * 40/100) + (90\% * 60/100)$                     |

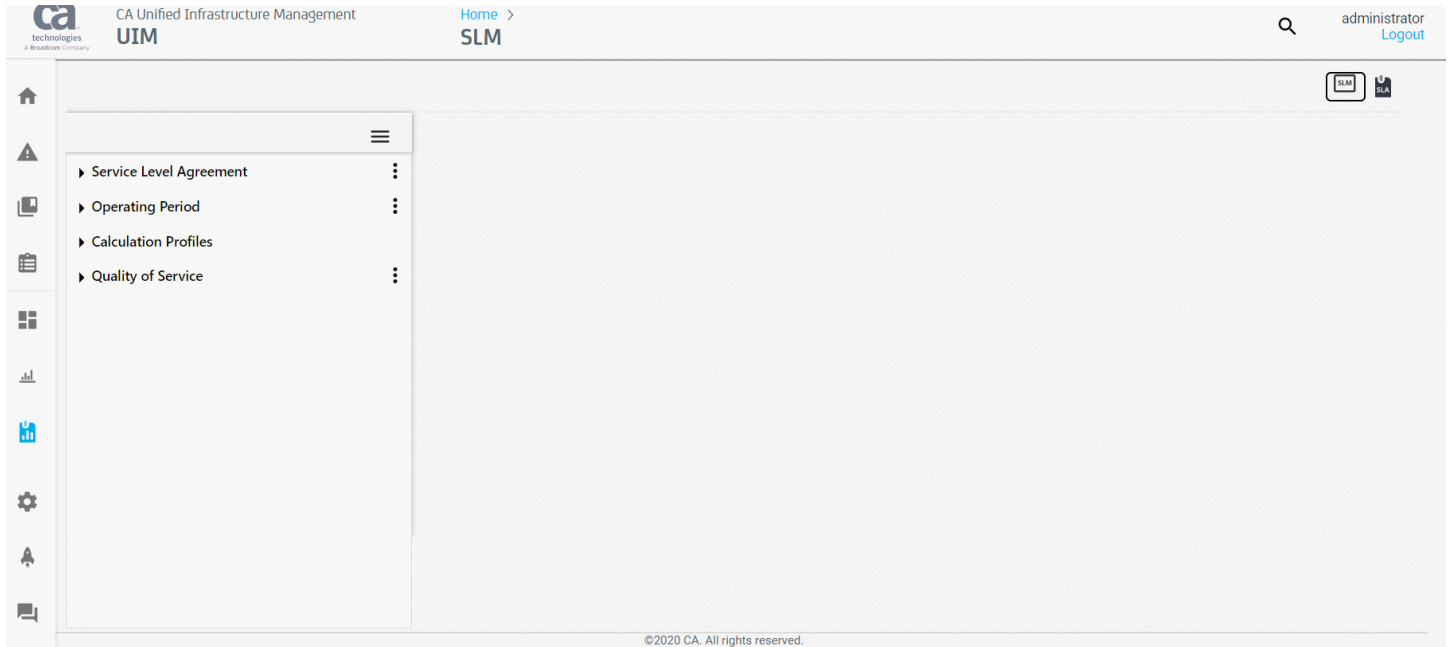
## SLM Interface Reference

### Contents

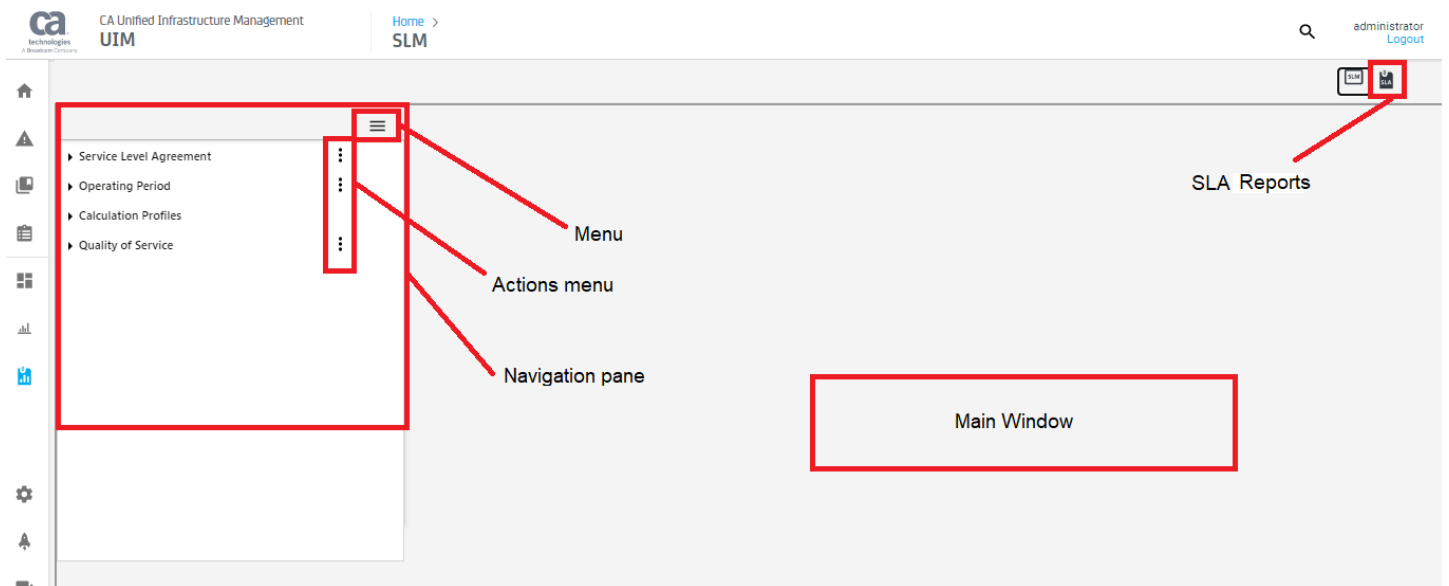
The Service Level Management application window consists of the following main parts:

- Menu
- Navigator pane
- Main window
- SLA Reports

The following video shows the different options that are available in the SLM interface:



This illustration highlights the appropriate sections of the UI:



### The Menu Bar

This section gives a short description of the different functions and tools that are found in the menu line. Note that some of the menus are partly restricted, depending whether your user is classified as an operator or a super-user.



- **Actions menu**

This option can be used when defining a new:

- **Service Level Agreement**  
Opens the Service Level Agreement dialog in which you can create SLAs.
- **Operating Period**  
Opens the Operating Period dialog; see description in the section Creating an Operating Period in [Create a New Service Level Agreement](#).
- **Quality of Service**  
Opens the QoS Definition dialog in which you can define a new Quality of Service object.

- **Menu**

This option can be used to perform multiple functionalities in SLM:

- **Database Status**  
Opens the Database Status window. The window contains relevant database information, such as:
  - A list of QoS objects in existing SLAs.
  - A list of the probes responsible for generating QoS messages in existing SLAs.

**NOTE**

The database table D\_QOS\_PROBES that populates the Probes tab is not populated by default. To re-enable the population of D\_QOS\_PROBES, in Account Admin, select the Raw Configure option for the data\_engine probe and, in setup, set the qos\_probes parameter to yes.

- **Data Management**  
Opens the Data Management dialog. You can configure the data\_engine to perform automatic clean-up procedures or open the Data Management dialog to perform manual data management.
- **Export QoS data**  
Opens the Export QoS data window. You can export the selected QoS object.
- **View SLM Alarms**  
Displays alarms that are related to Service Level Management in the OC view in a new page. This provides you with a way to identify devices generating alarms and further information on the alarms.
- **SQL Query**  
Opens the SQL Query dialog, allowing you to send SQL queries to the database. This is useful if you want to view database contents.
- **Wizards**  
Lets you start a wizard for creating SLAs.
  - Creating a SLAs based on a selected service.
  - Adding an excluded period. You can create excluded periods in the SLA and SLO forms or, with this wizard, you can add an excluded period and can attach the period to the newly created SLAs and SLOs.

## **The Navigator Pane**

The Navigator pane is at the left of the screen. The pane contains a tree-like structure, showing the various nodes and elements in the UIM Service Level Management product suite.

## **SLA Reports**

The SLA Reports is at the top right of the screen. You can select any existing SLA and can view the reports that are related to the SLA.

## **Service Level Agreements**

This node lists all defined SLAs. The SLAs might appear as:

- Single SLAs
- Grouped SLAs - The SLAs can be placed in one group or in subgroups on multiple levels under the main group. SLAs can be moved between groups using drag-and-drop.
- Accounts - A list of all accounts created through the Account Admin view. You can assign an account to a new or existing SLA or can create an SLA from an account. You can also create SLA groups under accounts and move SLAs to them using drag-and-drop.

#### NOTE

You cannot create or delete an account in this node. To create or delete an account, go to the instructions in [Using Account Admin](#).

Click the **Actions menu**



icon beside Service Level Agreement in the Navigation pane to define new SLAs or SLA groups.

- **New Service Level Agreement**  
Opens an empty SLA dialog, where you can define a new SLA.
- **New Group**  
Opens a New Group dialog where you can define a new SLA group. Give a name to the new group and (optionally) a description.
- **Refresh**  
Updates the Service Level Manager to reflect the latest modifications.

When an SLA group or an Account is selected, these options appear:

- **View**  
Opens the current group in edit mode. You can view or edit the desired group details and save it.
- **New Group**  
Opens a New Group dialog, where you can define a new SLA group. Give a name to the new group and (optionally) a description.
- **New Service Level Agreement**  
Opens an empty SLA dialog, where can define a new SLA.
- **Delete** (for SLA groups only)  
Deletes the selected SLA group, including all SLAs in that group.
- **Recalculate**  
Starts a new calculation job for all SLAs in the selected group.  
Clicking the Recalculate option of a SLA group does not open the Job Properties dialog. To see the Job Properties dialog, select the Recalculate option of individual SLA within the group.

When an SLA is selected, these options appear:

- **View**  
Opens the current SLA in edit mode. You can view or edit the desired SLA details and save it.
- **New Based On**  
Starts the SLM wizard, so that you can create a SLA based on settings in the selected SLA except for specific management fields, such as Notes and Excluded Periods. Note that some input fields are not editable. Assigning an account to an SLA inserts the SLA under the Account name in the Navigator pane.
- **Delete**  
Deletes the selected SLA.
- **Recalculate**  
Starts a new calculation job for the selected SLA. The Job Properties dialog is opened, allowing you to edit the job parameters.

## Operating Periods

This node lists the defined operating periods. Operating Periods are used to constrain the measured QoS values to specific hours of any day (the period in which the QoS constraint is valid.)

The operating period is defined to be a collection of time periods and is used when we define new SLAs. Use the Operating Periods when defining the QoS constraints (see the section Create an Operating Period in the article [Create a New Service Level Agreement](#)). The samples falling outside these time specifications does not influence the SLA and SLO compliance requirements.

### Follow these steps:

- Click the **Actions menu**

(  )

icon beside **Operating Period** to define a new Operating Period.


- **New Operating Period**

Opens an empty dialog, enabling you to define a new Operating Period.

- **Refresh**

Updates the Service Level Manager to reflect the latest modifications to the Operating Period.

- Click the **Actions menu**

(  )

icon beside any defined Operating Period to open menu options:

- **View**

Opens the existing Operating Period in edit mode. You can view or edit the existing Operating Period and save it.

- **New**

Opens an empty dialog, enabling you to define a new Operating Period.

- **Delete**

Deletes the selected Operating Period.

## Calculation Profiles

This option allows you to define your own calculation profiles.

These calculation profiles are used when defining the calculation properties for Service Level Objects and Quality of Service Constraints (see the section Create a Calculation Profile in the article [Create a New Service Level Agreement](#)).

When defining calculation profiles, the profiles are grouped either as SLO calculations or as QoS calculations, depending on the selected plug-in supports single-data or multi-data series.

### Follow these steps:

1. Click the **Actions menu**

(  )

icon beside the **SLO Calculation** subnode, and select **New** to define a new SLO Calculation profile.

**OR**

2. Click the **Actions menu**

(  ) icon

beside the **QoS Calculation** subnode, and select **New** to define a new QoS Calculation profile.

When any existing SLO Calculation or QoS Calculation is selected, these options appear:

- **View**

- Opens the existing Operating Period in edit mode. You can view or edit the existing Operating Period and save it.
- **New**  
Opens an empty dialog, enabling you to define a new Operating Period.
- **Delete**  
Deletes the selected Operating Period.

### **Quality of Service**

Under this node, available registered QoS objects are grouped into logical groups based on the description field in the QoS object. This view enables you to browse the database for a particular data series.

Click the **Actions menu**



icon in the QoS node to open a small menu containing four options:

- **Order by QoS group**  
All QoS objects are presented in their logical groups.  
In addition, see the section Properties for information about sorting and organizing QoS objects in folders.
- **Order by QoS**  
All QoS objects are listed alphabetically (and not grouped).  
In addition, see the section Properties for information about sorting and organizing QoS objects in folders.
- **Refresh**  
Updates the Service Level Manager to reflect the latest modifications.

When any existing QoS object is selected, these options appear:

- **Properties**  
Opens the existing QoS object in edit mode. You can view or edit the existing QoS object and save it.
- **New**  
Opens an empty dialog, enabling you to define a new QoS object.
- **Delete**  
Deletes the selected QoS object.
- **Refresh**  
Updates the Service Level Manager to reflect the latest modifications.

### **The Main Window**

This is the application frame. All child windows are contained within the frame of the main window. The main window icons are:

- **Save**  
Lets you save new definitions, or any modifications to existing definitions.

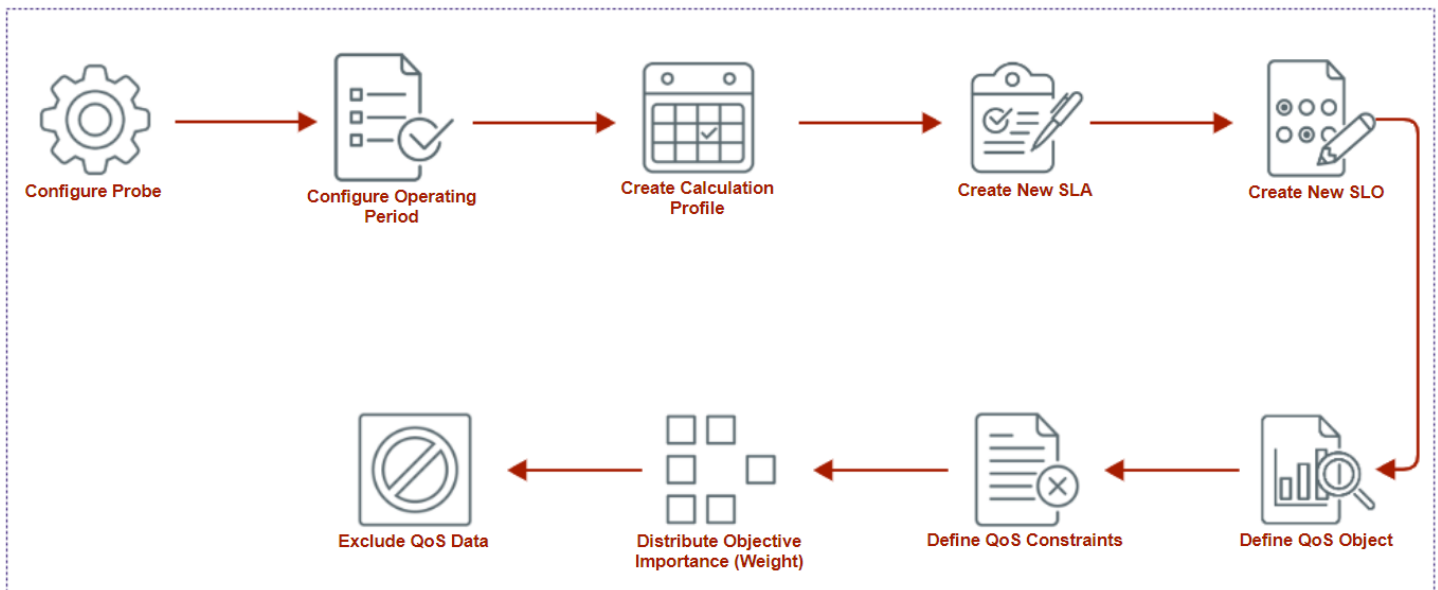
#### **NOTE**

Save SLA, SLO, and QoS views as you create them. If you close a window (for instance, a new or revised SLO within an SLA) without saving it, information and settings are not saved.

## **Create a New Service Level Agreement**

A Service Level Agreement (SLA) consists of Service Level Objectives (SLOs), quality of service (QoS) objectives, and QoS constraints. These are nested elements. However, before the SLA can be fully defined, monitoring probes must be installed and launched to collect metrics and operating periods and service calculations should be created so that they can be applied to QoS objectives.

The following diagram shows the high-level process to create SLAs:



The tasks outlined in the illustration are as follows:

### **Set Up a Probe to Deliver Quality of Service Data**

Configure a monitoring probe to generate QoS data for use in an SLA either through Infrastructure Manager or Admin Console. Configuration options differ from probe-to-probe, but the following steps for the cdm probe are typical.

#### **NOTE**

You must have UIM administrator rights to configure probes.

#### **Follow these steps in Admin Console:**

1. Launch Admin Console.
2. On the robot running monitoring probes, open the **Configuration** option for the cdm probe.
3. In the navigation pane, view the settings for **Disks**, **Memory**, and **Processor** to verify that the sampling interval supports the QoS objectives for the SLA.
4. In the navigation pane, open the folders for the QoS items to be used in the SLA, verify the thresholds for each metric, and click the box beside **Publish Data**.
5. Click the **Save** button at the upper-right corner and the **OK** button on the Success dialog.

#### **Follow these steps in Infrastructure Manager:**

1. Launch Infrastructure Manager on your system.
2. On the robot running monitoring probes, open the properties window of the cdm probe.
3. Under the **Setup** tab, verify that the sampling intervals for **Disk**, **Memory & Paging**, and **CPU** support the QoS objectives for the SLA.
4. Under the **Advanced** tab, check the boxes for the QoS messages that will be available to the SLA.
5. Click the **Update** button.
6. The QoS definitions for disk properties are located under the **Status** tab. Double-click the disk that you are interested in, check the boxes for **Disk Usage QoS Message** (in Mb, percentage, or both) in the dialog box that appears, and click the **OK** button.
7. In the **Status** tab, click the **Apply** button to apply the changes.

8. Reply **Yes** when prompted for a restart.
9. In the **Status** tab, click the **OK** button to close the properties window of the cdm probe.

The probe initially sends a QOS\_DEFINITION message to the data\_engine, causing the SLM system to recognize the new QoS object.

Repeat this general procedure for each probe that returns QoS data for the SLA.

### **Create an Operating Period**

Once probes have been configured to return data to the SLM, open the SLM in the Operator Console (OC) to define SLAs, SLOs, and QoS objects.

Operating periods are used to constrain the measured values to specific hours of any day. By defining operating periods now, the periods will appear as options in a pull-down menu when defining SLOs.

Samples falling outside these time specifications will not influence the SLO or SLA compliance requirements.

#### **Follow these steps:**

1. Click the **Action menu**



icon beside the **Operating Period** node in the Navigator pane and select **New Operating Period** option.

2. Name the operating period and enter a description (optional).
3. Click the **New** button in the dialog to add days and time specifications.  
For example, you can create an operating period called Business Hours to define the client's work-hours and define work hours as Monday-Friday, from 0700 to 1700.

#### **NOTE**

Enter time for a 24-hour clock.

4. To edit an entry in the list, simply select the entry and click on **Edit** button.
5. Click the **OK** button to create and save the operating period.

#### **NOTE**

The compliance period (the overall measurement period) is defined elsewhere in the SLA. Excluded periods—for instance, for system maintenance or business holidays—are defined in the SLA.

Operating periods are weekly periods and are not calendar-specific. Set a calendar-specific compliance period within the SLA form.

### **Create a Calculation Profile**

Calculation profiles define the conditions for SLO and QoS compliance. A calculation profile can be assigned to any SLO or QoS object. By defining calculations now, the calculations appear as options in a pull-down menu when defining SLOs.

#### **Follow these steps:**

1. Expand the **Calculation Profiles** node in the Navigator pane.
2. Click the **Actions menu**



icon beside the **SLO Calculations** or **QoS Calculations** subnodes and select **New**.

You can also expand the folders for SLO and QoS calculations to view the list of calculations already created. Click the **down** icon beside the name of any existing calculation to create a new one.

The profiles are based on built-in plug-ins that are distributed with the SLA application.

- **Name**  
Enter the new Calculation profile name in this field.
- **Description**  
Give a short description of the Calculation profile in this field.
- **Calculation**  
You can select one of the available calculation plug-ins from the pull-down list.  
Available plug-ins in the list depend on whether you have opened the dialog for a SLO calculation (multi-series calculations) or opened the list for a QoS calculation (single-series calculations).
- **Variable Configuration**  
Fields are associated with the Calculation selection.

These plug-ins are available:

- **For QoS calculations:**
  - **Calculate availability from the average of all samples.**  
Finds the average value of all samples and compares this value against the defined threshold value.  
If the average value of all samples meets the constraints, the availability for that QoS is 100%. If the average value of all samples does not meet the constraints, the availability for that QoS is by default set to 0%. You can set the Breach Value in the Variables Configuration and the percentage on breach to a value other than 0%.  
You can also define the way NULL values are handled. The NULL value typically occurs if a probe does not measure a value from the target due to a timeout—for example, there is no answer to a ping. In the case of Null value samples in the data series, you have the following options for treating these samples . If none of the options are selected, a NULL sample is treated as a non-compliant value.
    - **Ignore**  
The samples are ignored and do not influence on the compliance percentage. The value “0” is entered in the Value column.
    - **Min**  
The samples are set to the same value as the minimum sample value found in the data series. The value “1” is entered in the Value column.
    - **Max**  
The samples are set to the same value as the maximum sample value found in the data series. The value “2” is entered in the Value column.

**Example:**  
Threshold: Greater than or equal to 5  
Samples: 5, 4, 8, 6, 2, and one NULL sample.  
Define NULL sample as ignored and Breach Value as 35% using the Variables Configuration.  
Availability: The NULL sample is ignored, giving an average value of  $(5+4+8+6+2)/5= 4.6$ .  
This value is below the threshold of 5 and is therefore a breach condition (set to 35%).
  - **Calculate availability from number of samples that meet the constraints.**  
This profile calculates the availability by finding the percentage of samples that meet the constraints.  
Note that you can, using the Variables Configuration, define how missing samples should be treated: ignored (and not influencing the availability) or treated as samples not meeting the constraints.
 

**Example:**  
Threshold: Greater than or equal to 5  
Samples: 5, 4, 8, 6, 2, with one sample missing.  
Define missing samples as ignored using the Variables Configuration.  
Availability: One sample missing (ignored) and three of four samples meets the constraints, yielding an availability of 75%.
  - **Calculate availability from the median.**  
The median value is found by sorting the values in a row in descending order. The value found in the middle of the row is the median value.
 

**Example:**  
Threshold: Greater than or equal to 5

Samples: 5, 4, 8, 6, 2.

Sorted in ascending order: 2, 4, 5, 6, and 8.

The value in the middle of the row is 5, which means that the median value is 5.

Availability: The median value 5 means that the threshold value is not breached. This value indicates 100% availability.

Note that, using the Variables Configuration, you are allowed to define floor and ceiling values. Values below the floor value and above the ceiling value are ignored and not counted when calculating the median value.

– **Calculate availability from the N'th percentile of all samples.**

The value for a percentile that you specify is evaluated to determine whether it meets the QoS constraints. For example, if you specify the 50th percentile, the value that corresponds to the 50th percentile of the data samples that are evaluated. If the value meets the constraints, the availability is 100%. If it does not meet the constraints, the availability is 0%.

Use the Variable Configuration table to specify the percentile.

**Example:**

Threshold: Greater than or equal to 5

Samples: 5, 4, 8, 6, 2

Percentile: 50th

Availability: First, the data is sorted in ascending order: 2, 4, 5, 6, and 8. The position in the data array for the percentile is calculated as:  $(\text{number of data samples} \times \text{percentile})/100$ . In this example, the calculation is  $(5 \times 50)/100=2.5$ . However, decimal places are ignored and values are rounded down, so the result is 2. This means the data sample in the second position in the array is used: in this case, 4. Because 4 does not exceed the threshold of 5, the availability is 100%.

The Calculation Profile is assigned to a QoS as a Calculation Method for an SLO QoS object. Options are available only if the SLO **Calculations Type** under the **Calculation Settings** tab is set to **Formula**.

• **For SLO calculations:**

- **Calculate availability by AND-ing or OR-ing the data series.**
- **Calculate availability by logical expression.**

These options require that the QoS object type and order is known. Either create the SLA, SLOs, and QoS objects and then return to the Calculation Profiles node to define the calculation or create the calculation and then view it when creating QoS objects in an SLO.

For setting the logical expression in the profile, set the value of the **Expression** field. For setting an expression, use following guidelines; otherwise, an expression parser error occurs.

- – Use AND, OR, and NOT operators either in upper or lower case.
- QOS is represented by an integer number from the SLO definition window.
- Each expression must be enclosed in brackets.
- Each token in the expression must be separated by a space.

Some valid examples of logical expressions are:

- – ( 1 OR 2 )
- ( 1 AND 2 )
- ( 1 AND ( NOT 2 ) )
- ( 1 AND 2 ) OR ( 3 AND ( NOT 4 ) )
- **Set the treatment in the Missing samples field.**
- **Ignore** sets a flag to exclude missing samples from compliance calculations.
- **Down** (for a non-responding server) sets a flag to treat missing samples as non-compliant.
- If none of the options are selected, a NULL sample is treated as a non-compliant value.

The Calculation Profile is assigned to an SLO as a **Calculation Method** under the **Calculations Settings** tab of the **Quality of Service** table. Options are available only if the SLO **Calculations Type** is set to **Profile**.



## Create a New SLA

You can create a new SLA in the following ways:

- Click the **Action menu**



icon beside the **Service Level Agreement** node in the Navigator pane and select **New Service Level Agreement** option.

- At the top of the Navigator pane, click **Menu** icon > **Wizards** > **Create SLA By Service**. See information at [Create an SLA Using the SLA Wizard](#).
- Expand the **Service Level Agreement** node and select any existing SLA and select **Create SLA Based On The Selected SLA**.

To create a new SLA group, click the **Actions menu** icon in the Service Level Agreement node of the Navigator pane and select **New Group**.

### Follow these steps:

- Give the new SLA a name and a description.
- Assign an account to the SLA.

#### NOTE

Assigning an account to an SLA inserts the SLA under the Account name in the Navigator pane when the SLA is saved.

- Select a **Calculation Method** from the pull-down menu.

#### NOTE

The calculation method is applied to the SLA based on the compliance selection of component SLOs. For the Weighted option, the Weight Properties dialog is activated once at least two SLOs are created. To reassign relative weights as further SLOs are defined, click the Weighted button to open the Weight Properties dialog.

- Click the **Compliance period** button for **Compliance Period** options. This period is the period over which the service level is measured and your committed compliance level (measured as a percentage). If you choose the Day option, the SLA defaults to the current day.

#### NOTE

The starting day for a weekly operating period defaults to the first Monday of the current week or the first day of the current month, regardless of the day that you select in the calendar.

- Select the time zone for the compliance period. You can leave the **Timezone** field empty if your OC server is located in the same time zone as the server that collects SLA data.
- Click **OK** to save the settings.
- Set the compliance percentage in the **Percentage** field at the right.

#### NOTE

The Compliance Period and percentage is passed to new SLOs. If you change the percentage in the SLA, save the settings and refresh the browser to see the new percentage in the SLOs.

To reopen an existing SLA, Select an SLA from the SLA screen on the top right of the SLM view or click the **Actions menu** icon beside the SLA in the Navigator pane and select the **View** option.

## **Create a New Service Level Objective**

On the SLA form, you can create a new SLO as follows:

1. Open the SLA window by selecting SLA name in the Navigator pane.
2. In the SLA form with the **Objectives (SLO)** tab selected, click the **New** button at the bottom of the table.

The Service Level Objective form appears.


### **Service Level Objective Form**

An SLO is built around one or more QoS objects. The combination of source, target, threshold, and operating period sets the constraints for each QoS object. As with SLAs, you can set alarms for SLO breaches. If necessary, you can exclude an SLO from certain periods, such as scheduled down-time for maintenance or business closure dates and times.

The following fields or messages appear in the upper portion of the SLO form:

- **Name**  
Use this field to provide a short name for the SLO.
- **Description**  
Use this field for descriptive text, such as the purpose of the SLO.
- **Status**  
This message provides the current date and time.
- **The current period**  
Shows the current period defined in the Compliance Period settings of the SLA form.
- **Achieved compliance**  
Shows the current compliance percentage values.
- **Expected compliance**  
Shows the expected compliance percentage values from the SLA form.

You can create one or more SLOs without defining QoS objects. The SLOs appear in the SLA form once they are created.

To save a new SLO, click the **Save** button on the bottom of the table. To close the SLO form, click the **close** () icon at the top-right corner. To add or amend QoS settings, double-click the SLO name or select the SLO name and click the **Edit** button on the bottom of the table.

The following tabs appear in both the SLA and SLO forms. You can use them to define parameters for SLAs or the individual SLOs within an SLA.

### **Objectives Tab (SLA Form)**

The list of SLOs in the SLA.

### **The Quality of Service Tab (SLO Form)**

The columns appear under the Quality of Service tab.

- **QoS Name**  
The name of the Quality of Service object.
- **Source**  
Shows the source device of the QoS data.
- **Target**  
Shows the target device of the QoS data.
- **Weight**

Shows the assigned weight of the QoS constraint in relation to the other QoS objects within the selected SLO. The possible values are **Auto** or a percentage value defined under the **Calculations Settings** tab. The default **Auto** option weighs the QoS objects equally.

- **Fulfilled**  
Shows the percentage of fulfillment of the QoS constraint. **100%** indicates complete fulfillment.
- **Operator**  
The operator code for the value comparison.
- **Threshold**  
Shows the value set as the expected QoS value.
- **Op. Period**  
Shows the defined operating period for the QoS constraint.
- **Total**  
Defines the data samples used for calculations.
- **Accuracy**  
The measured value of the object.
- **Calculation Method**  
The method for calculating accuracy.
- **Order**  
The order of objects in the list. This value is used when defining AND or OR conditions for SLO compliance.

The following buttons appear:

- **New** button  
Creates a new QoS constraint within the current SLO.
- **Edit** button  
Edits the selected QoS constraint.
- **Delete** button  
Removes the selected QoS constraint from the current SLO.
- **Save** button  
Saves the settings. The **Save** button is enabled as soon as you enter text or change any selections to QoS definitions.

### **Alarm Notification Tab (SLA and SLO Forms)**

SLM generates alarms whenever an SLA or SLO breaches the defined compliance settings. Like others, these alarms can be forwarded to email, paging, etc.

- **Alarm when compliance is breached**  
Check this option to be notified of an SLA breach. A standard alarm is issued when the compliance breaches the value you specify in the **Expected** field.
  - **Severity Level**  
Select the appropriate severity level.
  - **Alarm Message**  
Enter the message to be generated when compliance is breached.
  - **Subsystem**  
Select the subsystem in which alarms appear in the Alarm SubConsole of Infrastructure Manager. The IM table gives more information about the alarms.
- **Alarm when warning threshold is breached**  
Check this option to be notified when approaching an SLO breach.
  - **Severity Level**  
Select the appropriate severity level.
  - **Alarm Message**  
Enter the message to be generated when the warning threshold is breached.

The **Save** button is enabled when you enter text or change any selections in the Alarm Notification tab.

### **Notes Tab (SLA and SLO Forms)**

The Notes tab lets you record relevant information pertaining to an SLA. For example, a system administrator can leave a note about an event that affected SLA compliance.

- **Date**  
Ties the note to a specific date and time.
- **Title**  
Descriptive text explaining the circumstances for the note.
- **Official**  
Indicates that the note will appear on published reports. Select the checkbox to enable this.
- **Text**  
The body of the note.

Buttons at the bottom let you create, edit, delete or save a note. The **Save** button is enabled as soon as you add a new note or make changes to an existing note.

### **Excluded Periods Tab (SLA and SLO Forms)**

The periods for which QoS data are not included in compliance calculation for either the SLA or individual SLO.

The following fields pertain to excluded periods in SLOs.

- **From date**  
Start of the exclusion period.
- **To date**  
End of the exclusion period.
- **Note Editor**  
The text of a note to be included with the exclusion period, such as an explanation of the period. Add Note will open the pop-up to enter the notes.
- **Official**  
Sets the note to be included in any published reports. Select the checkbox to enable this.

Exclusion periods can be added, changed, or deleted through the buttons to the right of the table. The **OK** button is enabled when you create a new period or make changes to an existing period.

### **Calculation Tab (SLA Form)**

The Calculation Settings tab shows the last calculations that are performed to set the compliance status.

### **Calculation Settings Tab (SLO Form)**

The Calculation Settings tab allows you to select how the compliance for an SLO is computed.

The following fields appear under the Calculation Settings tab of the SLO form:

- **Calculation Type**  
Use the radio buttons to select **Formula** or **Profile**. This selection affects the options available in the **Calculation Method** pull-down list.
- **Calculation Method**  
The options in the **Calculation Method** pull-down list depend on the **Calculation Type** you select - **Formula** or **Profile**.  
If you select **Formula**, you can select one of the following methods from the pull-down list:
  - **Average**

Calculates the average compliance percentage from the QoS constraints.

– **Best**

Selects and uses the compliance percentage from the QoS constraint with the best compliance.

– **Sequential**

Summarizes the periods when the expected value is not met for all QoS constraints and calculates the compliance. The difference between 100% and achieved compliance for each QoS is summarized and subtracted from 100%.

– **Weight**

Weights the compliance from the different QoS constraints according to importance. When **Weight** is selected, the Weight Properties dialog opens, enabling you to set the relative importance of the different QoS constraints. To change the relative weight, select the weight in the Weight Properties dialog and adjust the weighting at the top. Once saved, to reopen the dialog, select Weight as the Calculation Method and click the **Modify** button underneath the Calculation Type.

– **Worst**

Selects and uses the compliance percentage from the QoS constraint with the worst compliance.

If you select **Profile**, you can select one of the defined profiles in the pull-down list under **Calculation Method**.

Methods are listed under **Calculation Profiles > SLO Calculations** in the Navigator pane. New profiles are defined there also.

The **Save** button is enabled when you make changes to the dialog.

### **Define a Quality of Service Object**

On startup, all QoS-enabled probes send a QOS\_DEFINITION message to the data engine regarding a Quality of Service object in the database. The object is created automatically in the database with the provided information. You can select the objects in the **Quality of Service constraints** window.

You can also create the QOS object manually through the Service Level Manager by expanding **Quality of Service > New** from the Navigator pane. The following table describes the various fields in the dialog form.

| Field                             | Description                                                   |
|-----------------------------------|---------------------------------------------------------------|
| Name                              | The actual object name on the form QoS_XXX.                   |
| Description                       | A short descriptive text.                                     |
| Group                             | The group to which the object belongs.                        |
| Unit                              | A string stating the unit (e.g., Milliseconds or Centimeter). |
| Unit abbreviation                 | Used by reports and views (e.g., ms, cm)                      |
| Use specific data type properties | Activates the following fields.                               |
| Has maximum value                 | Defines the object with a maximum value.                      |
| Is of type Boolean                | Sets the type of the object to be Boolean (True/False).       |
| Object type                       | Presents a list of object type in the pull-down menu.         |

#### **NOTE**

The **Quality of Service > New** option exists for users who write and install their own probes. Information entered into the form depends on the parameters of the installed probe.

Once the QoS has been created, it is available to the SLO form and can be selected in the **Quality of Service constraints** window.

### **Define QoS Constraints**

The Quality of Service data itself has no value to the service objective unless it is constrained to a time-period, source, and target and meets rules to for the actual sample values.

Click the **New** button in the SLO form to display the QoS constraint dialog.

The QoS constraint dialog has the following fields:

- **Object**  
The Quality of Service object.
- **Source**  
Where the sample value originates.
- **Target**  
The target name of the sample, such as a disk or URL.
- **Expect Quality of Service to be**  
Set a threshold operator for the QoS. Sample values that meet the threshold criteria are considered to be in compliance for the QoS. Select an operator and then a Value and Unit.
- **Value**  
The threshold value. Depending on the QoS Object selected, a default value appears. Change this value as needed. Other default selections can be taken from a pull-down list for this field:
  - **Low**  
Smallest value during the operating period.
  - **Average**  
Average value for the operating period.
  - **High**  
Highest value in the sample range.
  - **Maximum**  
The QoS definition states that a maximum value exists for this QoS object, such as a disk sample.
- **Unit**  
A QoS definition describes a unit for the QoS value (e.g., %, MB, or count). This unit is the default unit for the QoS object selected.  
The pull-down list lets you select another unit, if available.  
If you change the unit, the value is automatically converted. For example, if the value initially is 1 second and you change the unit to milliseconds, the value automatically changes to 1000.
- **In operating period**  
Select the time period for which the compliance percentage is measured. Data from outside this period does not affect the compliance percentage.
  - **Always**  
All QoS measurements within the SLA compliance period (defined in the SLA) are included in the compliance percentage.
  - **<Custom>**  
Any custom operating periods created in the **Operating Periods** node of the Navigator pane. Only data that are collected during the specified period is included in the compliance percentage for the QoS. If you define custom operating periods in that node, they are listed in the pull-down menu. For example, you can create an operating period named Business Hours for Monday through Friday from 08:00 to 17:00 to measure compliance for the QoS during these hours only.
- **Calculation Method**  
Select the calculation method to use to determine the compliance percentage for the QoS. Expand **Calculation Profiles > QoS Calculations** option in the Navigator pane.
  - **Default**  
The Interval method is currently the default method.
  - **Average**  
Calculates the average of the data sample values and evaluates whether that average meets the threshold (sum of sample values/number of non-null samples).  
**Example:**  
Threshold: Greater than or equal to 5

Samples: 5, 4, 8, 6, and 2

The total of the sample values is 25, and the number of samples is 5, so the average is 5 (25/5). This meets the threshold, so compliance is 100%. If the average does not meet the threshold, the compliance percentage is 0.

– **Interval**

Calculates the compliance percentage by finding the percentage of samples that meet the threshold (number of compliant samples/total number of samples).

**Example:**

Threshold: Greater than or equal to 5

Samples: 5, 4, 8, 6, and 2

Three of five samples meet the threshold, so the compliance percentage for the operating period is 3/5 or 60%.

– **Median**

Calculated by determining the median value (the value in the middle of the sample range) and evaluating whether that value meets the threshold.

**Example:**

Threshold: Greater than or equal to 5

Samples: 5, 4, 8, 6, and 2

The median value (the value in the middle) is 5. A value of 5 means that the threshold is met, therefore compliance is 100%. If the median value does not meet the threshold, the compliance percentage is 0.

– **<Custom>**

You can define custom calculation profiles in the **Calculation Profiles** node of the Navigator pane, which allows you to set advanced properties for the calculation method. If you defined calculation profiles in that node, they are listed in the pull-down menu.

For example, if you defined a custom calculation profile and select **Median** as the calculation method, you can use **Variable Configuration** to set a Floor value and a Ceiling value. Values below the Floor and above the Ceiling are ignored when calculating the median value. Or, if you select **Average** as the calculation method, you can set the Breach Value to a value other than 0%, and you can define how null values are handled.

– **Percentile**

This option is listed on the pull-down menu if you have created a custom calculation profile using the calculation method **Calculate availability from the N<sup>th</sup> percentile of all samples**.

The value for a percentile you specify is evaluated to determine whether it meets the QoS constraints. For example, if you specify the 50th percentile, the value that corresponds to the 50th percentile of the data samples is evaluated. If the value meets the constraints, the availability is 100%. If it does not meet the constraints, the availability is 0%. Use the Variable Configuration table to specify the percentile.

**Example:**

Threshold: Greater than or equal to 5

Samples: 5, 4, 8, 6, and 2

Percentile: 50th

Availability: First the data is sorted in ascending order: 2, 4, 5, 6, 8. The position in the data array for the percentile is calculated as (number of data samples x percentile)/100. In the example, this is (5 x 50)/100=2.5. However, any decimal places are ignored, so the result is 2. This means the data sample in the second position in the array is used, in this case 4. Because 4 does not exceed the threshold, the availability is 100%.

**NOTE**

Use the QoS sample browser to determine the best possible values for your QoS threshold settings.

**Distribute Objective Importance (Weight)**

When setting up service level agreements and objectives, some objectives are more important than others. The same applies to QoS constraints. The weight distribution feature will help the user to either automatically or manually set up importance (measured in percent) for SLO or QoS constraints.

In **Calculations Settings** tab, select **Weight** as the **Calculation Method**. The weight dialog opens, showing a pie chart representing the importance as percentages. Modify the settings and save the dialog. To reopen the dialog, select **Weight** as the **Calculation Method** and click the **Modify** button underneath the Calculation Type.

### **Automatic Weight Distribution**

Click the **Auto** for automatic distribution of weight. The weight is computed automatically based on the number of objects available (objectives or constraints). This method is the default method.

### **Manual Weight Distribution**

This mode enables you to distribute weight manually using the selected object and the slider. Distributed weights must equal 100%. The defined weight is displayed in the **Weight(%)** column in QoS tab.

### **Exclude Quality of Service Data**

Data backup, hardware/software upgrades, and other maintenance tasks are normal system administrative tasks that make the systems unavailable for periods of time. Normally these procedures are performed during off-hours, such as evenings and weekends, but scheduled maintenance can be covered by the agreement between the service provider and the customer.

You can define exclusion periods for an SLA or for individual SLOs within an SLA. Separate exclusion periods for SLOs are useful for defining down times for individual servers or systems within a larger SLA. You can create multiple excluded periods for any SLA or SLO.

Excluded periods can be created in the following way:

- In an SLA by or SLO window

### **Create an Exclude Period for a Single SLA or SLO**

You can create an excluded period for a specific SLA or SLO from an open SLA or SLO window.

#### **Follow these steps:**

1. Selecting the **Excluded Periods** tab in the SLA or SLO window.
2. Click the **New** button.

The Exclude Period dialog appears. Ticking the **Add Note** option expands the dialog to enter an explanation for the period, such as a maintenance window or business holiday.

- **From**  
Defines the start date/time for the exclude period.
- **To**  
Defines the end date/time for the exclude period.
- **Add note**  
Checking this option expands the dialog to display the Note section, which otherwise is hidden. The textual note explains the reason for the exclude period and any other information.
- **Official note**  
If this option is checked the text of the note appears on published reports. If the box is not checked, the note does not appear on published reports.
- **Title and text**  
Title and text fields for describing the reason for the excluded period.

Click **OK** or **Cancel**. The dialog disappears



## Create an SLA Using the Wizard

Two different SLA wizards are available:

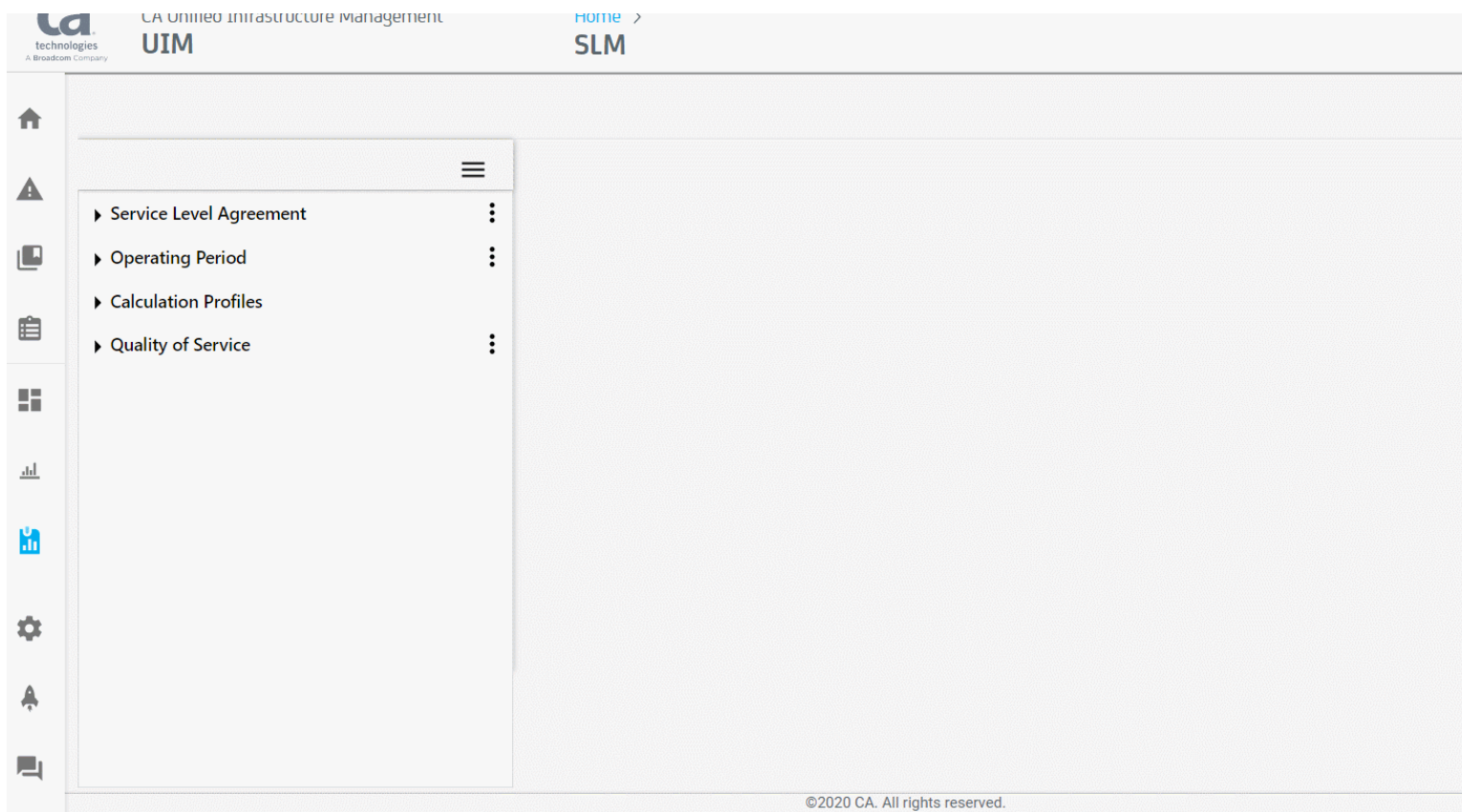
- Creating SLA based on a service
- Creating SLA based on an existing SLA

To create an SLA based on a service, launch the SLA Wizard by clicking "Create SLA By Service" from Wizards in the menu (three horizontal bars) at the top right of the Navigator pane in the SLM view. To create an SLA based on an existing SLA, select Create SLA Based On The Selected SLA from the Actions menu of an existing SLA (Service Level Agreement, <Existing SLA>, Actions menu).

### Contents

#### Example - Creating an SLA Based on a Service

This wizard creates an SLA group containing one or more SLAs, based on your selections through this wizard (one SLA for each selected source computer). Each SLA consists of one SLO with one or more QoS constraints, according to your selections.



1. In the Navigation pane, click the menu, and select Wizards, Create SLA BY Service to launch the wizard.
2. First select the type of SLA you want to create. You have two options:  
 Server SLA - Creating SLAs computing data from server-related probes  
 Network SLA - Creating SLAs using the net\_connect probe
3. Make your selection and click the **Next** button to continue.  
 When selecting source in the wizard, it means:

- The device (for example, a router) for the interface\_traffic probe.
- The robot hosting the probe for the net\_connect probe.

In this example, we describe a Server SLA.

4. Click the **Next** button to continue.

Step 1 prompts you for the following information:

- **Group Name** (required)  
This is the name of the created SLA group.
- **Description** (optional)  
This is a short informative description of the SLA. This information is displayed in the Description field of each of the SLAs created through this wizard.
- **Account** (optional)  
Select the Account under which the SLA Group is created.

Select Compliance percentage, Compliance period, QoS calculation method, and QoS Operating Period as described in the chapter Creating Service Level Agreement.

5. Click the **Next** button to continue.

Step 2 enables you to select the cdm properties for the SLAs. You can select:

- CPU usage, Memory usage, and Disk usage.
- disks to include
- none of these (select **Do not include**).

6. Click the **Next** button to continue.

Step 3 enables you to select the ntservices properties for the SLAs. You can select:

- One or more of the services listed.
- Whether you want to skip the services part (select **Do not include**).

7. Click the **Next** button to continue.

Step 4 enables you to select the processes properties for the SLAs. You can select:

- One or more of the processes listed.
- Whether you want to skip the processes part (select **Do not include**).

8. Click the **Next** button to continue.

Finally you can select one or more QoS Sources. One SLA is created for each of the selected QoS sources, and the SLAs are placed in the SLA group that is created with the name specified in step 1.

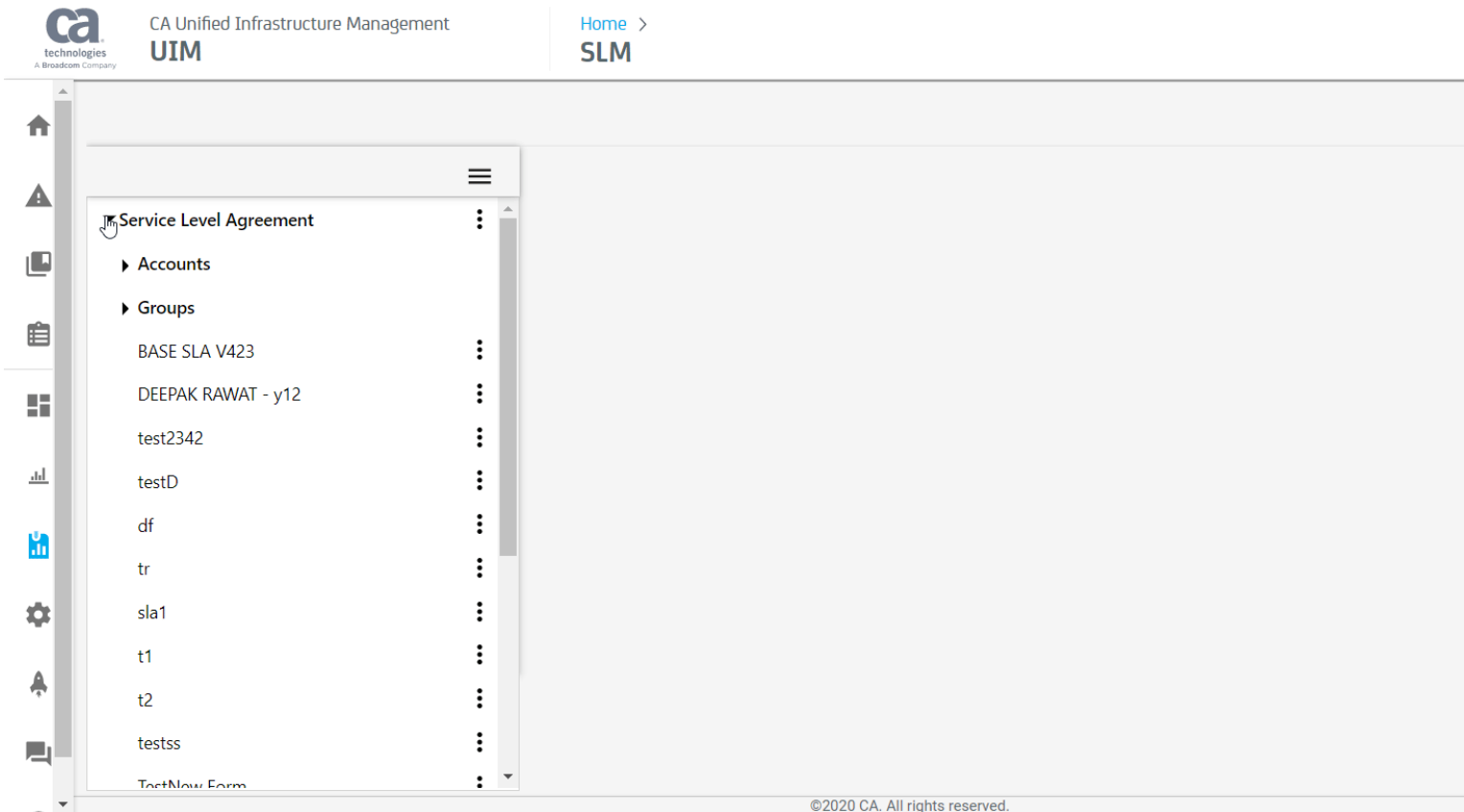
9. Click the **Finish** button.

The wizard is now finished. When you click the Finish button, the SLA group is created with one or more SLAs, depending on your selections.

Each of the SLAs contains one SLO with one or more QoS objects according to your selections.

### **Example - Creating an SLA Based on the Selected SLA**

This wizard creates an SLA, based on an SLA selected in the Navigator pane. The underlying SLOs and QoS definitions for the selected SLA is used as a template.



1. Launch the wizard by selecting **Create SLA Based On The Selected SLA** from the **Actions menu**

(  
⋮  
)

beside the existing SLA .

2. Give the new SLA a name and an optional short description.  
The SLA Description field initially contains the description of the SLA that we use as basis for the new SLA.  
The Based on field contains the name of the SLA you have selected to use as a template.
3. Select an account from the drop-down list at the bottom of the dialog if you want to attach the new SLA to an account, otherwise leave the field empty.
4. Click the **Next** button to continue.  
The next dialogs allow you to change the source and a target for each of the QoS definitions that are defined for the template SLA. You may skip any of the QoS definitions that you don't want in the new SLA.
5. Click the **Next** button to continue.
6. Click the **Finish** button, and the newly defined SLA appears in the Navigator pane.  
If the new SLA is based on a SLA in a SLA group, the new SLA is placed in the same group.

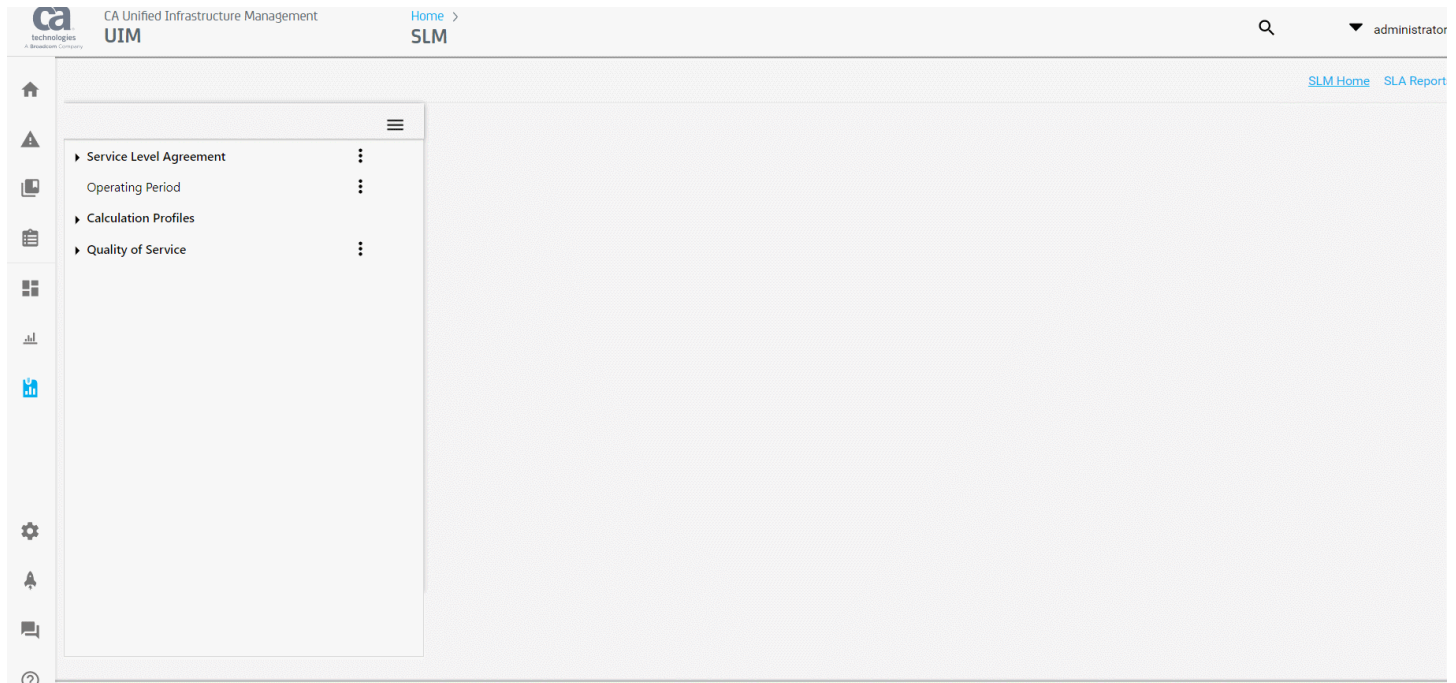
## Create a QoS Monitoring Profile

### WARNING

This feature requires the qos\_engine probe, which is no longer available as of the 7.6 release of Nimsoft Monitor. This functionality can be replicated using the [Time Over Threshold event rule](#) in the Probes Documentation Space.

## Send SQL Queries to the UIM Database

The SLM view includes a SQL Query Editor tool that you can use to enter custom SQL queries for testing and verification. From the SLM, select **SQL Query Editor** from the **Menu** at the top right of the Navigator pane to access the tool.



### WARNING

The SQL Query Editor tool in SLM is intended for experienced users only.

Select a query from the pull-down box and click the **Start Query Editor** button to execute the query.

SQL Query Editor
✕

START QUERY
STOP QUERY

SELECT \* FROM S\_SLA\_DEFINITION;

RECORDSET #1 (2 ROWS)

EXPORT

| SLA_ID | NAME                | DESCRIPTION | PERIOD_CODE | PERIOD_START          | PERIOD_NUMBER | PERIOD_BEGIN          | PERIOD_END            | C |
|--------|---------------------|-------------|-------------|-----------------------|---------------|-----------------------|-----------------------|---|
| 2      | My2ndTest           | Test 1 2 3  | m           | 2021-02-28 21:00:00.0 | 1             | 2021-03-27 21:00:00.0 | 2021-04-27 21:00:00.0 | 1 |
| 5      | System Availability |             | m           | 2021-02-28 10:30:00.0 | 1             | 2021-03-28 00:00:00.0 | 2021-04-28 00:00:00.0 | 9 |

With the SQL Query Editor tool, you can:

- Use any SQL command.
- Enter carriage returns.
- Enter queries that consist of multiple statements.

#### NOTE

To use multiple statements, separate each statement with a semicolon.

- Run queries with multiple statements *and* a query selected from the combo box simultaneously.
- Enter multiple statements, then highlight one or more of the statements to run only the highlighted statements.
- Stop a query that is running by clicking the **Stop Query** button.

The result of a query appears in a table under the **Recordset** tab. When you run a query that consists of multiple statements, a separate **Recordset** tab appears for each statement. The number of rows found is displayed in the tab header.

The SQL Query Editor also alerts you if enter the incorrect syntax and/or invalid database objects.

### **Size Limits for SQL Queries**

In environments with extensive monitoring, database tables can contain a large number of rows. To maintain OC response time, SLM SQL queries in OC version 20.3 and later are now limited to 1000 rows and columns to 1024 bytes.

To override the limits, edit the **<slm>** section of `wasp.cfg`, add the following parameters, and restart the wasp probe:

- **max\_rows** The maximum number of rows returned
- **max\_field** The maximum length of any column

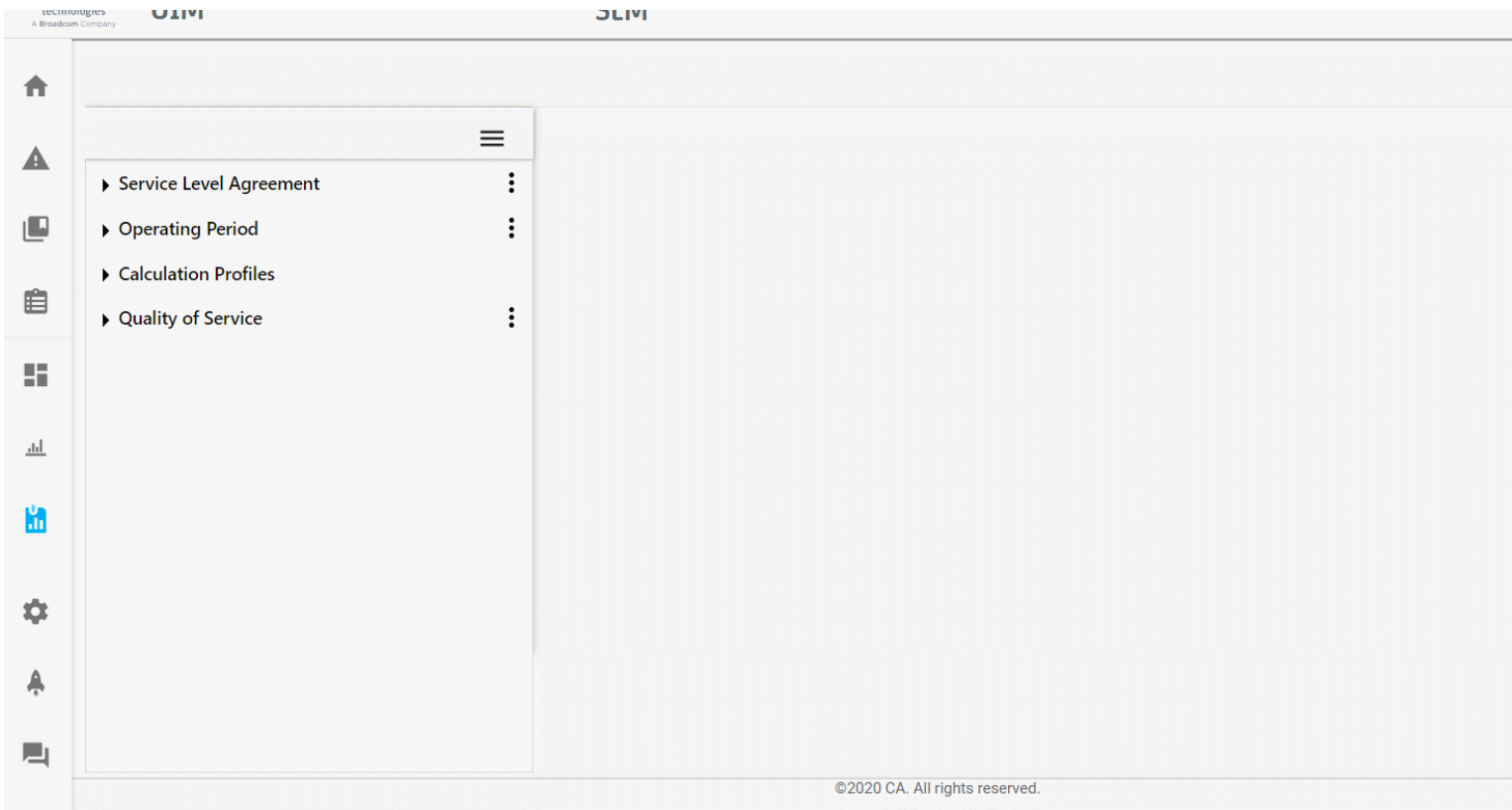
#### **For example**

```
<slm>
 reloadable = true
 cross_context = true
 load_on_startup = true
 unpack_war = true
 path = /slm
 max_rows = 10
 max_field = 2048
</slm>
```

## **SLM Data Management**

The `data_engine` receives all QoS data and inserts it into the database. The `data_engine` can be configured to perform automatic clean-up procedures by configuring the data management section of the `data_engine`.

To perform manual data-management in SLM, click the **Menu** at the top right of the Navigator pane and select the **Database Status** option.



## Contents

### View Database Usage

The Database Status window displays information that is related to the QoS data stored in your database. To view the window, click the **Menu** at the top right of the Navigator pane and select the **Database Status**.

The Database Status window contains the following tabs:

- Active Objects
- QoS Definition

The tabs represent various ways of getting information regarding database usage.

### The Active Objects Tab

The Active Objects Tab shows all available QoS objects registered within the database structure. You can filter the view, view information for individual QoS objects, and can change QoS display through individual objects in the Quality of Service list.

The followings columns appear in the Database Status view when the Active Objects tab is selected:

- **Quality of Service**  
The name of the QoS object.
- **Source**  
The source from which the sample originates.
- **Target**  
The target of the sample.
- **Table id**

An ID number is assigned to each of the QoS objects registered within the database structure.

- **Host**  
The IP-address of the host of the probe from which the sample originates.
- **Robot**  
The name of the robot from which the sample originates.
- **Probe**  
The name of the probe from which the sample originates.
- **Origin**  
This is the origin of the QoS sample. All messages that received by a given hub are stamped with an origin element. The default origin name is the HUB name.

Objects can be filtered by QoS, Source, Target, Host, Robot, Probe, and Origin.

Options in the **Actions** icon menu are:

- **View Data**

Opens a view of the data for the current compliance period as a graph or as a table.

- **Get Statistics**

Displays the statistics of the selected QoS object.

- **Delete Data**

Opens the Data Management dialog for the selected QoS constraint, allowing you to delete the complete QoS data series or only for a selected period. The QoS object is not deleted selecting this option, and data for the selected QoS constraint remains stored in the database table.

- **Export Data**

Opens the Export QoS Data wizard, enabling you to export the data series for the selected QoS constraint dialog to a file.

- **Delete Object(s)**

Deletes both the selected QoS objects and data series from the database. The deleted QoS object disappears from the database and is recreated when the probe is restarted.

- **Merge Objects**

Allows you to merge two QoS selected objects of the same type.

A dialog box appears with the objects assigned as Source and Destination and the direction of the merge shown as an arrow between them. You can switch the direction of the merge operation by clicking the arrow in the middle of the dialog.

You also can delete the “source” QoS after the merge operation. The deleted QoS object disappears from the database and is recreated when the probe is restarted.

- **Change origin**

Select one or more entries in the list, click the Actions menu icon and select Change Origin to change the origin for the selected entries. Available origins are listed in the dialog.

You can also create a new origin by clicking the **Add** button. Note that when you try to add an origin, you need to press Enter after entering the origin name, select the newly added name in the list, and click **OK**. Otherwise, the new origin is not saved to the list.

#### **NOTE**

All messages that are received by a given hub are stamped with an origin element. The default origin name is the HUB name.

## **QoS Definition Tab**

The QoS definition tab shows a list of QoS definitions and their properties. You can create new QoS definitions, edit, or delete existing QoS definitions.

- **Name**  
Name of the QoS.
- **Group**  
Group to which the QoS belongs. This determines how QoS are grouped in the tree in Navigator pane.
- **Unit**  
Unit of measurement for the QoS.
- **Abbreviation**  
Abbreviation for the unit of measurement for the QoS. For example, if the unit is **Bytes/sec** the abbreviation is **B/s**. You can use either the **Unit** or the **Abbreviation** when creating reports.
- **Is Boolean**  
Whether the value for the QoS is Boolean.
- **Has Max**  
Whether there is a maximum value for the QoS.
- **Type**  
Data type of the QoS.
- **Objects**  
Number of objects this QoS definition is assigned to.
- **Rows**  
Number of rows in the database with entries for the QoS.
- **Size (KB)**  
Size, in kilobytes, of the rows with entries for the QoS.
- **Historic**  
Number of measurements in the historic database for the QoS.
- **Size (KB)**  
Size, in kilobytes, of the historic measurements for the QoS.

Options in the **Actions** icon menu for each QoS are:

- **New**  
Opens an empty dialog, enabling you to define a new QoS object.
- **Delete**  
Deletes the selected QoS object.
- **Edit**  
Open the QoS Definition dialog to edit the description information. Only the **Description** field is available for editing. All other fields are in the disabled state and cannot be edited.

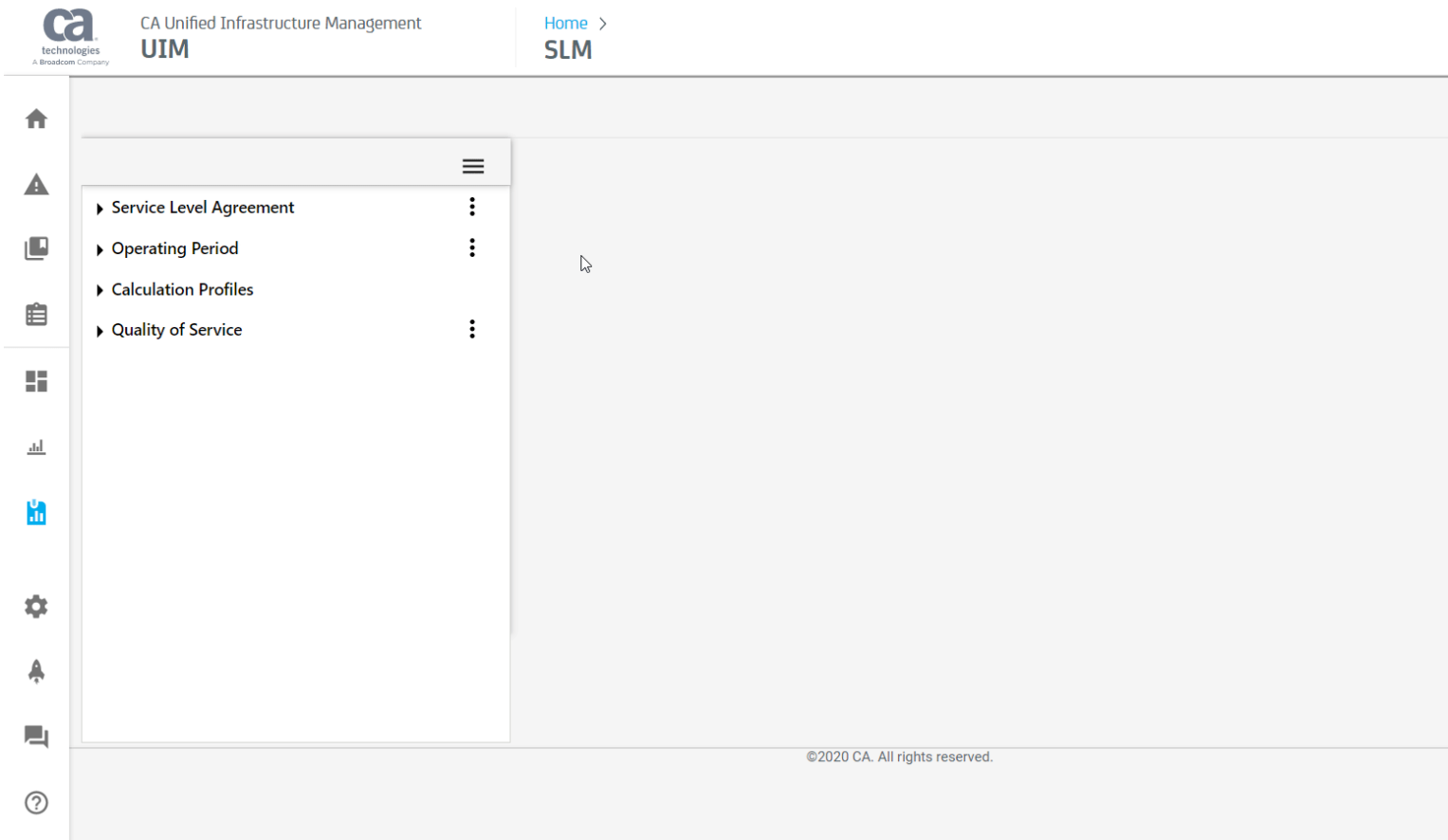
## **Manage QoS Data**

You can change the period settings for QoS data to exclude a specific period or ignore all period constraints. You can also delete data for a QoS constraint when it is not needed. When a contract expires or constraints are redefined, you can delete an object, SLO, or SLA.

### **Change Data Collection Periods and Delete Data**

Use the Data Management dialog to change period settings or delete data. Select the tools menu, Data Management option from the top of the pane.





The Data Management dialog opens. The various fields in the dialog are:

### Quality of Service Object

- **Object**  
Select a QoS object name from the pull-down menu.
- **Source**  
The source of the QoS data: for example, computer or device. Select a source from the pull-down menu.
- **Target**  
The target of the QoS data: for example: the disk, network service, or CPU. Select a target from the pull-down menu.

### Operation

- **Delete Data**  
Select this option to delete the QoS data that is related to the source and target settings. This option deletes only the raw data.
- **Invalidate Data**  
Select this option to invalidate the QoS data that is related to the source and target settings. This option replaces the raw data with NULL.
- **Delete Historic data**  
Select this option to delete the historic data for this QoS constraint. This option deletes only the aggregated (hourly and daily) data.

#### NOTE

Once deleted, data cannot be recovered.

---

## Period settings

- **Ignore**  
Select this option to ignore period constraints and send all data to the database.
- **In selected period**  
Select this option to delete or invalidate all data within the chosen period.

## Delete Objects, SLOs, and SLAs

Once a QoS object, SLO, or SLA is no longer needed, it can be deleted.

### **NOTE**

Deleting a QoS object also deletes data for that object. Once deleted, the data, object, SLO, or SLA cannot be recovered.

### **Follow these steps:**

1. From the Navigator pane, select an SLA, SLO, or QoS object from the Service Level Agreement node or Quality of Service node.
2. Hover over the name and click the **down** icon.
3. Select the Delete option from the pull-down menu.

## **View and Export Quality of Service (QoS) Data**

The Navigator pane contains the Quality of Service node. All QoS objects are listed under this node. Browse the node for one or more data-series, view the data in chart and table formats, and export the data to a csv file on the server running the SLM view.

### **Contents**

#### **View QoS Data**

You can view QoS data by opening a QoS object from the Quality of Service node in the Navigator pane. The Quality of Service node lists all QoS objects that by source and target and provides filtering options.



©2020 CA. All rights reserved.

**Follow these steps:**

1. Go to the **Quality of Service** node in the Navigator pane.
2. Expand the the node and select a QoS object:
  - QoS Group
  - QoS
3. Click on the tree navigation to expand the top-level directories.
- 4.

Click the **Actions menu** (  ) beside the QoS object and click **Details**.

Data reflects the time period chosen for the QoS. You can select a different period from the Select Period pull-down list.

**NOTE**

In the graph, any gray area represents the portion of the current period that has not yet been sampled. To update the graph with the latest data, click the **Get Data** button.

Click the **Table View** tab to view data in table form.

**Export a QoS Data Series**

You can export QoS tabular data to a file from two places:

- The **Menu** of the Navigator pane options,
- The list of **Active Objects** in the **Database Status** window, and

All two options launch a set of dialog boxes.

**Follow these steps:**

1. In the Navigator pane, click the **Menu** to open a pull-down menu.

2. Select **Export QoS Data**.

### Export QoS Data

Configure QoS source and targets

First, please configure the data source used for the export

Object ▼

---

Source ▼

---

Target ▼

---

EXPORT
CLOSE

**OR**

1. In the **Database Status > Active Objects** window, click the box to select a QoS.
2. Click the **Action menu** icon.
3. Select the **Export Data** option.

|                                                                                                                                                                       | ACTIVE OBJECTS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | QOS DEFINITION           |                       |          |              |             |               |       |       |                                     |               |             |                     |   |              |             |               |                          |               |             |                      |   |              |             |               |                          |               |             |                       |   |              |             |               |                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-----------------------|----------|--------------|-------------|---------------|-------|-------|-------------------------------------|---------------|-------------|---------------------|---|--------------|-------------|---------------|--------------------------|---------------|-------------|----------------------|---|--------------|-------------|---------------|--------------------------|---------------|-------------|-----------------------|---|--------------|-------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▶ Service Level Agreement</li> <li>▶ Operating Period</li> <li>▶ Calculation Profiles</li> <li>▶ Quality of Service</li> </ul> | <p>Total Active Objects : 33138</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th><input type="checkbox"/></th> <th>Qua...</th> <th>Source</th> <th>Target</th> <th>Table id</th> <th>Host</th> <th>Robot</th> <th>Probe</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>QOS_MCS_RE...</td> <td>lvnqa012407</td> <td>Average amount o...</td> <td>3</td> <td>10.74.90.146</td> <td>lvnqa012407</td> <td>mon_config...</td> </tr> <tr> <td><input type="checkbox"/></td> <td>QOS_MCS_PR...</td> <td>lvnqa012407</td> <td>Template: Configu...</td> <td>4</td> <td>10.74.90.146</td> <td>lvnqa012407</td> <td>mon_config...</td> </tr> <tr> <td><input type="checkbox"/></td> <td>QOS_MCS_DE...</td> <td>lvnqa012407</td> <td>Overall Device Cou...</td> <td>5</td> <td>10.74.90.146</td> <td>lvnqa012407</td> <td>mon_config...</td> </tr> </tbody> </table> | <input type="checkbox"/> | Qua...                | Source   | Target       | Table id    | Host          | Robot | Probe | <input checked="" type="checkbox"/> | QOS_MCS_RE... | lvnqa012407 | Average amount o... | 3 | 10.74.90.146 | lvnqa012407 | mon_config... | <input type="checkbox"/> | QOS_MCS_PR... | lvnqa012407 | Template: Configu... | 4 | 10.74.90.146 | lvnqa012407 | mon_config... | <input type="checkbox"/> | QOS_MCS_DE... | lvnqa012407 | Overall Device Cou... | 5 | 10.74.90.146 | lvnqa012407 | mon_config... | <ul style="list-style-type: none"> <li>Get Statistics</li> <li>Delete Data</li> <li>Export Data</li> <li>Merge Objects</li> </ul> |
| <input type="checkbox"/>                                                                                                                                              | Qua...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Source                   | Target                | Table id | Host         | Robot       | Probe         |       |       |                                     |               |             |                     |   |              |             |               |                          |               |             |                      |   |              |             |               |                          |               |             |                       |   |              |             |               |                                                                                                                                   |
| <input checked="" type="checkbox"/>                                                                                                                                   | QOS_MCS_RE...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | lvnqa012407              | Average amount o...   | 3        | 10.74.90.146 | lvnqa012407 | mon_config... |       |       |                                     |               |             |                     |   |              |             |               |                          |               |             |                      |   |              |             |               |                          |               |             |                       |   |              |             |               |                                                                                                                                   |
| <input type="checkbox"/>                                                                                                                                              | QOS_MCS_PR...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | lvnqa012407              | Template: Configu...  | 4        | 10.74.90.146 | lvnqa012407 | mon_config... |       |       |                                     |               |             |                     |   |              |             |               |                          |               |             |                      |   |              |             |               |                          |               |             |                       |   |              |             |               |                                                                                                                                   |
| <input type="checkbox"/>                                                                                                                                              | QOS_MCS_DE...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | lvnqa012407              | Overall Device Cou... | 5        | 10.74.90.146 | lvnqa012407 | mon_config... |       |       |                                     |               |             |                     |   |              |             |               |                          |               |             |                      |   |              |             |               |                          |               |             |                       |   |              |             |               |                                                                                                                                   |

The **Menu > Export QoS Data** option opens a set of boxes. Identify the QoS, source, and target for the data export. Based on your selection, the other two export options are selected automatically.

**Follow these steps:**

1. Select the QoS, source, and target for data export, if necessary.
2. Select the period of interest.
3. Select configuration options for the export file.
4. Click the **Export** button to export the data.

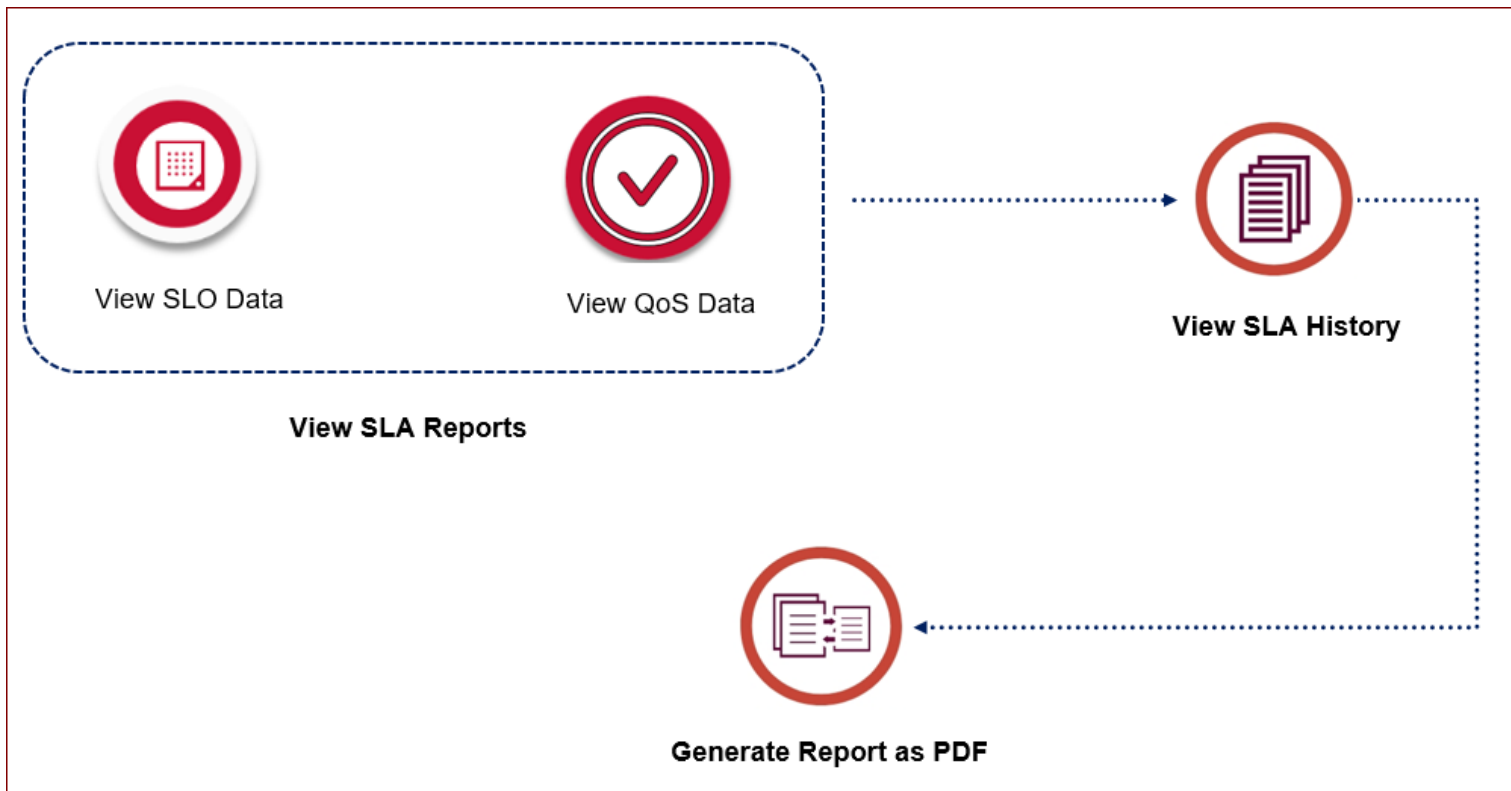
A dialog box opens with the destination of the export file. By default, the file is sent to the C:\ drive of the server running the SLM.

## The SLA Reports

The SLA Reports display performance information for service level agreements (SLAs) defined in the SLM view.

- An SLA is an agreement between a client and a service provider that specifies the service to be provided, times, priorities, responsibilities, guarantees, and warranties.
- SLAs consist of one or more service level objectives (SLOs), which are specific measurable characteristics of the SLA such as availability, throughput, frequency, response time, or quality.
- SLOs are composed of one or more QoS objects that are combined to produce the SLO achievement value. For example, an availability SLO may depend on multiple components, each of which has a quality of service (QoS) availability measurement. QoS objects specify the source, target, threshold, and operating period settings for the QoS measurement.

SLA Reports display performance information for all three levels of the SLA.



## Contents

### View SLA Reports

The SLA Reports can be accessed from the top right of the SLM view in the Operator Console.

#### **NOTE**

If you do not have the SLM View permission set in the Access Control List (ACL), you see a "Permission Denied" message when you try to open the SLA Reports.

When you open the SLA Reports, a selection dialog appears listing SLAs created in the SLM. Select an SLA from the window by typing the name of an SLA, and then click **OK**.

#### **NOTE**

If the selected SLA contains no QoS objects, a dialog appears to indicate an invalid SLA. The selection box disappears; to open it again, click on the **Open SLA**



icon at the upper right of the window.

The SLA appears as a graph showing the compliance and non-compliance averages and a table of SLO and their individual compliance rates.

The screenshot shows the UIM interface for an SLA named 'qoscharts\_6oct'. At the top, it displays the current period as 'Thu Oct 01 2020 to Tue Dec 01 2020 (2 month(s))' with a current compliance of 100.00% and a goal of 59.00%. A green gauge chart shows the current compliance level. Below this, a table lists the SLOs:

| State | Objective | Description | Weight | Achieved | Expected | Notes |
|-------|-----------|-------------|--------|----------|----------|-------|
|       | slo1      | hhy         | auto   | 100      | 100      |       |

Icons next to the SLO names represent the state of compliance:



- SLO in compliance



- SLO compliance breached

Entries in the Achieved and Expected columns give more detailed information about the state of the SLO.

Icons at the upper right corner are:



- View historical data for the selected SLA in a separate window.



- Save the current window to a PDF file that can be saved and printed.



- Open an SLA.

### View SLO Data

You can view information for SLOs that is similar to information for SLAs. Click on an SLO in the SLA table.

A table appears, listing the QoS objects, the source, and target of each and their rate of compliance. Icons reflect the compliance state of the SLOs.

goscharts 6oct | slo1

The current period is Thu Oct 01 2020 to Tue Dec 01 2020. Current compliance is 100%, the goal is 100%.

**Quality of Service (Summary)**  
 The following Quality of Service objects (QoS) are defined in this SLO. Each QoS is listed with its weight and the percentage of fulfillment. The fulfillment is the relationship between the weight and the compliance for the constrained Quality of Service.

| State | Object                | Source        | Target        | Weight(%) | Achieved(%) | Expected(%) |
|-------|-----------------------|---------------|---------------|-----------|-------------|-------------|
|       | QOS_MEMORY_PERC_USAGE | lvntest015309 | lvntest015309 | 0         | 100         | 100         |

### View QoS Data

You can view charts for QoSs for SLOs. Click on a QoS name in the SLO table.

A graph appears, listing the QoS objects, the source, and target of each and their rate of compliance. An icon next to the QoS name reflects its compliance state.

CA Unified Infrastructure Management  
UIM

Home

administrator  
Logout

goscharts 6oct | slo1 | QOS\_MEMORY\_PERC\_USAGE

Object: QOS\_MEMORY\_PERC\_USAGE  
 Source: lvntest015309  
 Target: lvntest015309  
 Compliance: 100%  
 Threshold: <=> 53%  
 Operating Period: OP-MONDAY

Legend: ■ % - Threshold

Data is displayed for the time period for the QoS.

#### NOTE

In the graph, any gray area without data represents the portion of the current period that has not yet been sampled. This data is automatically updated.





If there were no QoS objects assigned to the SLA or if the probe was unable to collect data, an Unavailability Report appears below the graph. The Unavailability Report lists the periods for the breach or lack of data. The State column indicates the cause for the unavailability:

- 
- breach
- unavailable service

**Unavailability Report**

The report summarizes the periods with threshold breaches and where the service is unavailable. A service is considered unavailable if it is impossible to determine the state of the service. A breach is defined to be where the sample value does not meet the compliance criteria.

Total Unavailability: 20 Mins

| State                                                                             | Period Start             | Period End               | Minutes |
|-----------------------------------------------------------------------------------|--------------------------|--------------------------|---------|
|  | Mon Oct 05 2020 08:20:00 | Mon Oct 05 2020 08:25:00 | 5       |
|  | Mon Oct 12 2020 02:10:00 | Mon Oct 12 2020 02:15:00 | 5       |
|  | Mon Oct 12 2020 04:10:00 | Mon Oct 12 2020 04:15:00 | 5       |
|  | Mon Oct 12 2020 05:00:00 | Mon Oct 12 2020 05:05:00 | 5       |

To view other QoS charts, you can navigate back to the SLO view or to the SLA view through the named links at the upper left of the window.

**View SLA History**

The SLA History chart shows historical information about the SLA and provides an easy way to view the SLA report for different compliance periods.

1. Click the **History**



icon.


The SLA History chart is displayed. Compliance periods where the SLA objectives were met are shown as green columns, while compliance periods where SLA objectives were not met are shown as red columns. Hover over a column to see a pop-up window with the dates of the compliance period and the compliance percentage. The trend line for the data is shown in blue, and the compliance objective is shown as a red line. Click the Maximize icon to enlarge the SLA History chart.

2. Click a column in the history chart to view the SLA report for that compliance period.

**Generate a Report as a PDF**

You can view an SLA Report as a PDF that can be printed or saved. You can set the PDF to include pages for all views of the report: the SLA, SLOs, and all QoS charts.

**Follow these steps:**

1. Click the **View as PDF**  icon. The PDF Preferences dialog opens.
2. In the PDF Preferences dialog:
  - a. Select the desired orientation and size of the PDF.
  - b. Select the depth (level) of the report and click **OK**.
 A new window opens and displays the PDF.

The PDF version of an SLA Report contains links that you can use to navigate through the pages. These items are as follows:

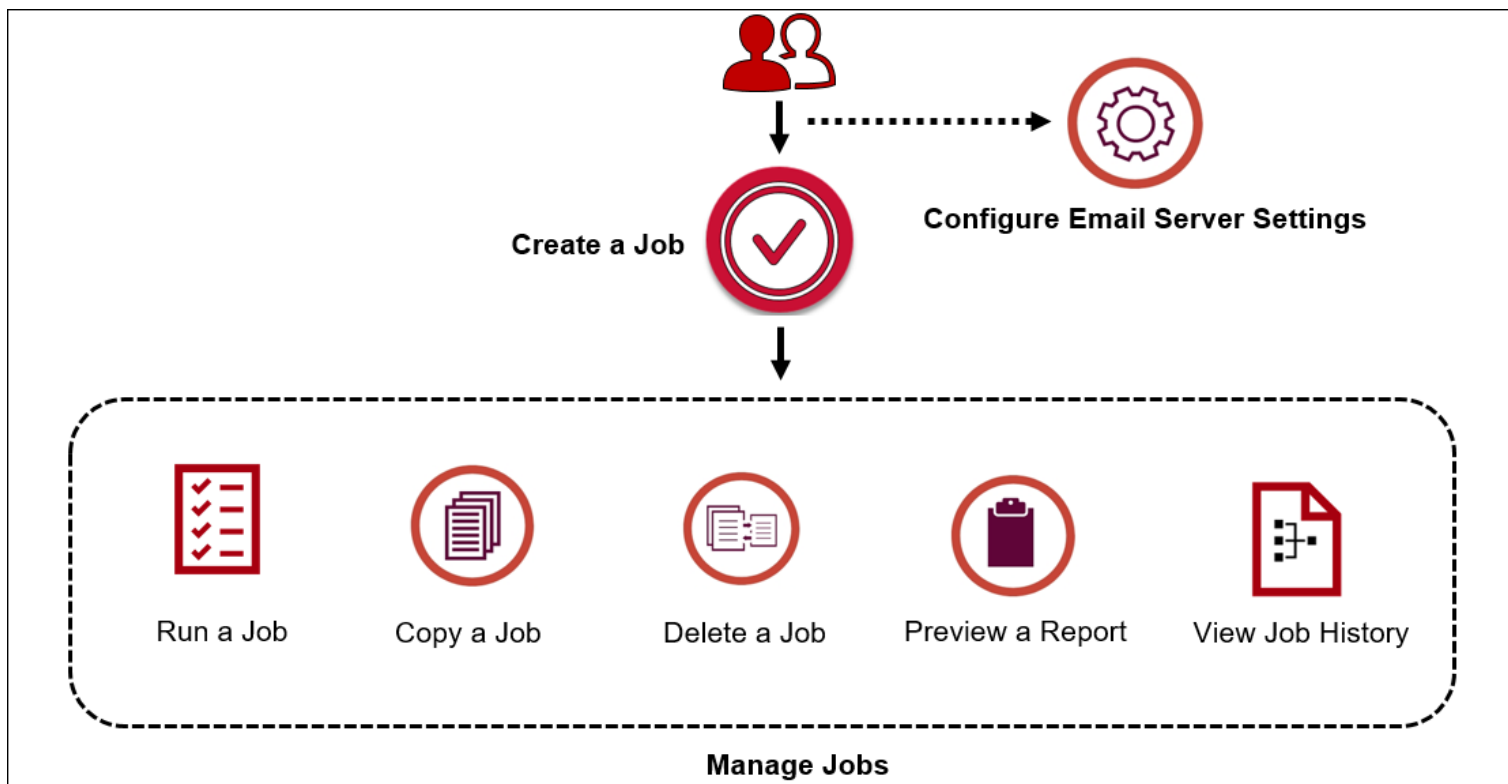
- The SLA summary page contains a table listing the SLOs in the report. You can click on items in the **Objective** column to jump to a page containing details of an SLO.
- The pages displaying details of an SLO contain a table listing QoS objects. You can click on items in the **Object** column to jump to a page containing details of a QoS object.
- At the top of each page displaying details of an SLO or QoS object, the heading provides links that allow you to navigate back up to an SLO or to the SLA summary page.

**Working with Report Scheduler**



(From UIM 20.3.3) You can use Report Scheduler to schedule Metric views or Service Level Agreement (SLA) reports to run at specified times. The reports can be delivered as a PDF through email or FTP, or can be stored on a server. This article explains how you can work with jobs in Report Scheduler. It describes how to create, edit, delete, preview, copy, and run jobs. It also provides information on how to view the history for a job and how to view the log file for each job run.

The following illustration provides an overview:



The following topics provide the required information:

#### NOTE

- You must have the Report Scheduler ACL permission to work with the Report Scheduler functionality.
- For a multi-node OC environment, the Report Scheduler functionality in UIM 20.3.3 no longer supports the `job_refresh_secs` configuration property in the `/webapps/reportscheduler` section of `wasp.cfg`. Now, it supports the `execute_email_action` configuration property in the `/webapps/reportscheduler` section of `wasp.cfg`. The `execute_email_action` property lets you prevent the duplicate reports by stopping the execution of the email actions on one or more OC servers. On each OC server that you want to stop executing email actions, add the `execute_email_actions` property with a value of `false`. Therefore, with this property, you can resolve the issue of users receiving duplicate reports in a multi-node OC environment.

The following illustration helps you quickly understand how you can access and create a report schedule:

CA Unified Infrastructure Management  
UIM

Home > Settings > Report Schedules

Search icon | administrator

Filter | Email Setup | **Create New**

| Job name                   | Type        | Report                  | Next Run (local time)                | Account   | Actions  |
|----------------------------|-------------|-------------------------|--------------------------------------|-----------|----------|
| Windows CPU Report         | Metric View | Metric View 1 - Windows | 3:50 PM on Wednesday, Apr 7th, 2021  |           | ▶ 📄 🗑️ ⋮ |
| Copy Of Windows CPU Report | Metric View | Metric View 1 - Windows | 3:50 PM on Wednesday, Apr 7th, 2021  |           | ▶ 📄 🗑️ ⋮ |
| New Schedule 1             | Metric View | Metric View 1 -         | 10:59 AM on Wednesday, Apr 7th, 2021 | CustomerA | ▶ 📄 🗑️ ⋮ |
| Demo Job                   | Metric View | Metric View 1 - Windows | 8:00 PM on Tuesday, Apr 6th, 2021    |           | ▶ 📄 🗑️ ⋮ |
| 17mar1                     | Metric View | Metric View 1 - Windows | 1:41 PM on Wednesday, Apr 7th, 2021  |           | ▶ 📄 🗑️ ⋮ |
| 17mar77777                 | Metric View | Metric View 1 - Windows | 1:42 PM on Wednesday, Mar 16th, 2022 |           | ▶ 📄 🗑️ ⋮ |
| Copy Of Demo Job           | Metric View | Metric View 1 - Windows | 8:00 PM on Tuesday, Apr 6th, 2021    |           | ▶ 📄 🗑️ ⋮ |
| Copy Of 17mar77777         | Metric View | Metric View 1 - Windows | 1:42 PM on Wednesday, Mar 16th, 2022 |           | ▶ 📄 🗑️ ⋮ |
| New Schedule 1_wweklu      | SLA         | My2ndTest               | 2:52 PM on Friday, Apr 9th, 2021     |           | ▶ 📄 🗑️ ⋮ |

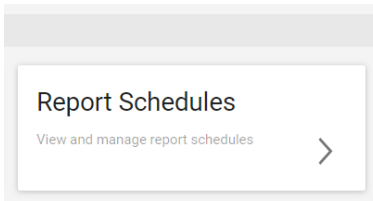
©2021 CA. All rights reserved.

### Create a Job

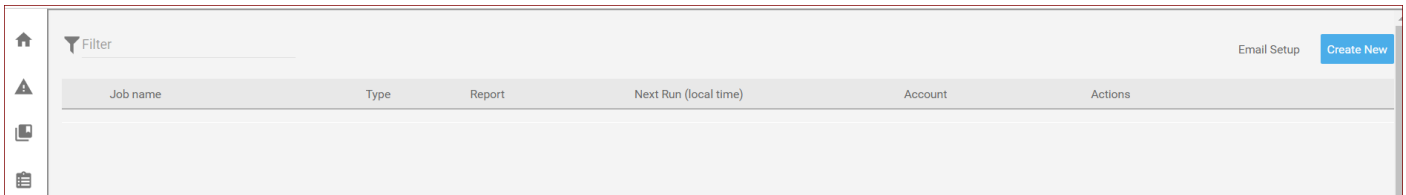
To schedule a report, you must create a job. The complete job creation process includes three steps: configure schedule details, specify when to schedule the job, and provide information about the delivery mechanism.

#### Follow these steps:

1. Access the **Settings** option in the OC UI.
2. Click the **Report Schedules** tile.



The **Report Schedules** page opens.



3. Click the **Create New** button.  
The **Create Schedule** dialog opens.

Create Schedule
✕

---

Schedule Details
Step 1 of 3

---

Save As
Required

Schedule\_Create

Enabled

Description  

This is a schedule.

Account  

IT
▼

---

Report Type  

Performance
▼

Report
Required

Metric\_View\_Create
▼

4. Provide the following information in the **Schedule Details** section:
  - a. Enter a name for the report in the **Save As** field.
  - b. Select the **Enabled** option to allow the job to run.
  - c. Enter a meaningful description in the **Description** field.
  - d. Assign the job to an account from the **Account** drop-down list.
  - e. Select the type of report from the **Report Type** drop-down list. You can select Metric Views or SLA.
  - f. Select the required report from the **Report** drop-down list.
  - g. If you selected the report type as SLA, make a selection from the **SLA Depth** drop-down list. The default is Full SLA. Similarly, if you selected the report type as Metric Views, make a selection from the **Report Time Frame** drop-down list. The default is Last Full Day.
 

**NOTE**

The **Full SLA** option provides the most detail, but is more resource intensive than the other options.
  - h. (For Metric Views) If necessary, select a different data **Aggregation Interval**. The default is Automatic. To print the job at the report settings, you must change the **Report Time Frame** value to match the report time frame and the **Aggregation Interval** value to match the report aggregation interval.

**NOTE**

You can change the data aggregation interval for each new job. This will not change the aggregation interval in the saved report. Saving a job saves the time frame and aggregation interval selections for that job.

- i. Click **Next**.

The **Scheduling** section is displayed.

Create Schedule
✕

---

Scheduling
Step 2 of 3

---

Run
Required

Daily ▼

---

Run On

Every

1

Day(s)

Start Date

1/28/2021

13:45

End Date

1/28/2021

13:45

No end date

Time Zone

Asia/Calcutta (UTC+05:30) ▼

CANCEL
BACK
NEXT

5. Provide the following information in the **Scheduling** section:
- Select an option from the **Run** drop-down list. The **Run On** area updates dynamically based on your selection.
  - Specify the time and date to run the report. Use the **Time Zone** drop-down list to select the time zone for the report. The time zone that you select determines when the job is executed, and which time zone the report displays. If you do not select a time zone, the local time zone is used by default.

**NOTE**

The job will run at the first specified time after the starting time you set.

- c. Click **Next**.

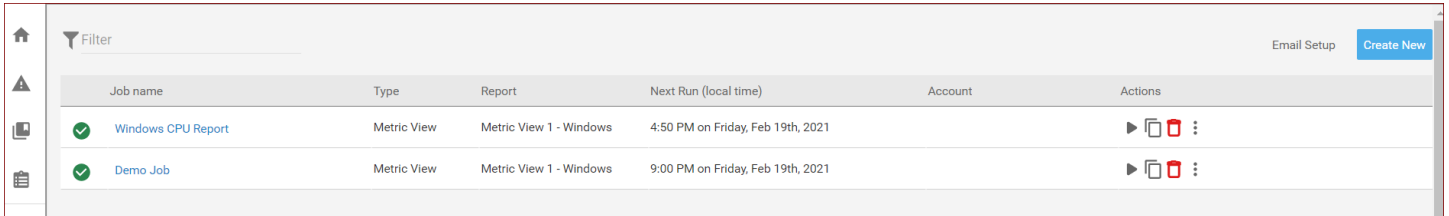
The **Delivery** section is displayed.

6. Provide the following information in the **Delivery** section:
  - a. If you select **Email**, enter information in the **To**, **Subject**, and **Message** fields. Also, ensure that the [SMTP server settings](#) are already configured.
  - b. If you select **FTP**, enter information in the required fields. You can use the **FTP Location** field to specify a subdirectory in which to save the report. For example, enter reports/monthly to save the report in a subdirectory named monthly. The **FTP Passive** option allows you to set passive or active FTP mode. The passive mode is recommended if the OC server and FTP server are separated by a firewall. Click **Test Connection** to validate the FTP connection.
  - c. Select **Store on server** if you want to save the reports on the OC server (..\webapps\reportscheduler\archive). You can also [configure the report storage location](#) on a server.
  - d. Select the layout orientation for the report from the **Report Orientation** drop-down list.
  - e. Select the layout size for the report from the **Report Size** drop-down list.
7. Click **Create**.

The job is created and is listed in the Report Schedules jobs table.

### **View the Report Schedules Table**

The Report Schedules jobs table lists the jobs that you create.



| Job name           | Type        | Report                  | Next Run (local time)             | Account | Actions  |
|--------------------|-------------|-------------------------|-----------------------------------|---------|----------|
| Windows CPU Report | Metric View | Metric View 1 - Windows | 4:50 PM on Friday, Feb 19th, 2021 |         | ▶ 📄 🗑️ ⋮ |
| Demo Job           | Metric View | Metric View 1 - Windows | 9:00 PM on Friday, Feb 19th, 2021 |         | ▶ 📄 🗑️ ⋮ |

Click a column heading to sort the list of jobs by that column, and click again to switch between ascending and descending order. You can also enter text in the filter field to find the relevant job. This icon



indicates that the job is enabled. This icon



indicates that the job is disabled.

You can perform appropriate operations on the created jobs based on your requirements.

### **Configure Storage Location on a Server**

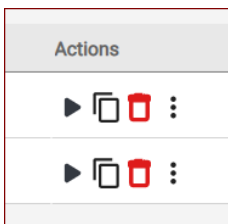
One of the delivery options in Report Scheduler is to store reports on a server. By default, the reports are stored under the root directory `\webapps\reportscheduler\archive`, but you can define the root directory for storing reports. If the report is associated with an account, the report is stored in a directory with that account name under the specified root directory.

#### **Follow these steps:**

1. Open Infrastructure Manager.
2. Click the robot for the primary hub in the tree view.
3. Click the wasp probe to select it in the top-right pane.
4. Press CTRL and right-click, then select Raw Configure from the popup menu.
5. Expand the webapps folder in the tree view of the Raw Configure window.
6. Click reportscheduler in the tree view. The Report Scheduler keys are displayed in the right pane.
7. Click New Key. The New Key dialog is displayed.
8. Enter `file_store_root` in the Enter key name field.
9. Enter the directory path that you want to use as the root directory for storing reports in the Enter value field.
10. Click OK, then click OK again to close the Raw Configure window.
11. Restart the wasp probe.

### **Manage Jobs**

After you create a job, you can perform various operations on the job to manage them efficiently. The following screenshot shows the options that you can perform as part of managing the jobs:



#### **Follow these steps:**

1. **Run a job**

You can run a job at any time. The report is sent to the specified delivery method(s). Running a job does not affect the regular schedule for the job.

- a. Locate the job that you want to run.
- b. Click the **Run Job** icon (play icon) available in the Actions column.

The job runs and the report is sent to the specified delivery methods. The report is named <job\_name>\_<yearmonthdate>\_<hoursminutessseconds>.pdf. Any invalid symbols or characters in the job name are removed.

## 2. **Copy a job**

You can make a copy of an existing job. This is useful if you want to create another job with similar settings.

- a. Locate the job that you want to copy.
- b. Click the copy job icon.

The copy of the job is created, named as Copy of <job name>, and is listed in the table. You can edit the settings of the copy.

## 3. **Delete a job**

You can delete jobs that you no longer want. When you delete a job, all runs of the job and the job history are also deleted.

- a. Locate the job that you want to delete.
- b. Click the delete job icon (trash icon).
- c. Confirm to delete the job.

The job is deleted and is removed from the table.

## 4. **Preview a report**

You can view a PDF of a report without sending it to the selected delivery methods. This also provides an easy way to save the report on your computer.

- a. Locate the job for which you want to preview the report.
- b. Click the three dots in the Actions column.
- c. Click Preview Report.

A PDF of the report is generated in your browser.

## 5. **View job history**

You can view the job history. For example, you want to view the log file for each run of a job. The log file includes information such as actions taken, time, status, and errors.

- a. Locate the job for which you want to view the history.
- b. Click the three dots in the Actions column.
- c. Click Show History.

The Schedule History dialog opens. It contains the job history. Click the status of the required entry. The log is displayed. You can also access the log file from a message if a job is unsuccessful. The successful/unsuccessful error message along with a link for viewing the log file is displayed.

You have successfully performed the required actions.

## **Configure Email Server Settings**

To deliver reports by email, Report Scheduler must be configured to use your SMTP server.

### **Follow these steps:**

1. Open the Report Scheduler UI.
2. Click the Email Setup option in the top-right section. The **Email Setup** dialog opens.

Email Setup
✕

From Address Required

SMTP Server Required

SMTP Port Required

---

User Name

Password

---

Use authentication

Use STARTTLS

Cancel Done

3. Enter an email address that your SMTP server can use in the **From Address** field.
4. Enter the name (**SMTP Server**) and port number (**SMTP Port**) of your SMTP server.
5. Enter a valid user name (**User Name**) and password (**Password**) for your SMTP server.
6. If necessary, select one or more of the security options:
  - **Use authentication**
  - **Use STARTTLS**
7. Click **Done** to save your changes.

The email server settings are configured successfully.

## The SNMP Device Self-Certification

To view information about the SelfCert webapp, go to the [SNMP Device Self-Certification](#) section of the Probes Documentation Space.

## Dashboards

The Operator Console (OC) comes with predefined views, named Dashboards. To see a Dashboard, click on the Dashboards in the left navigation of OC and select the dashboard that you want to view.



**NOTE**

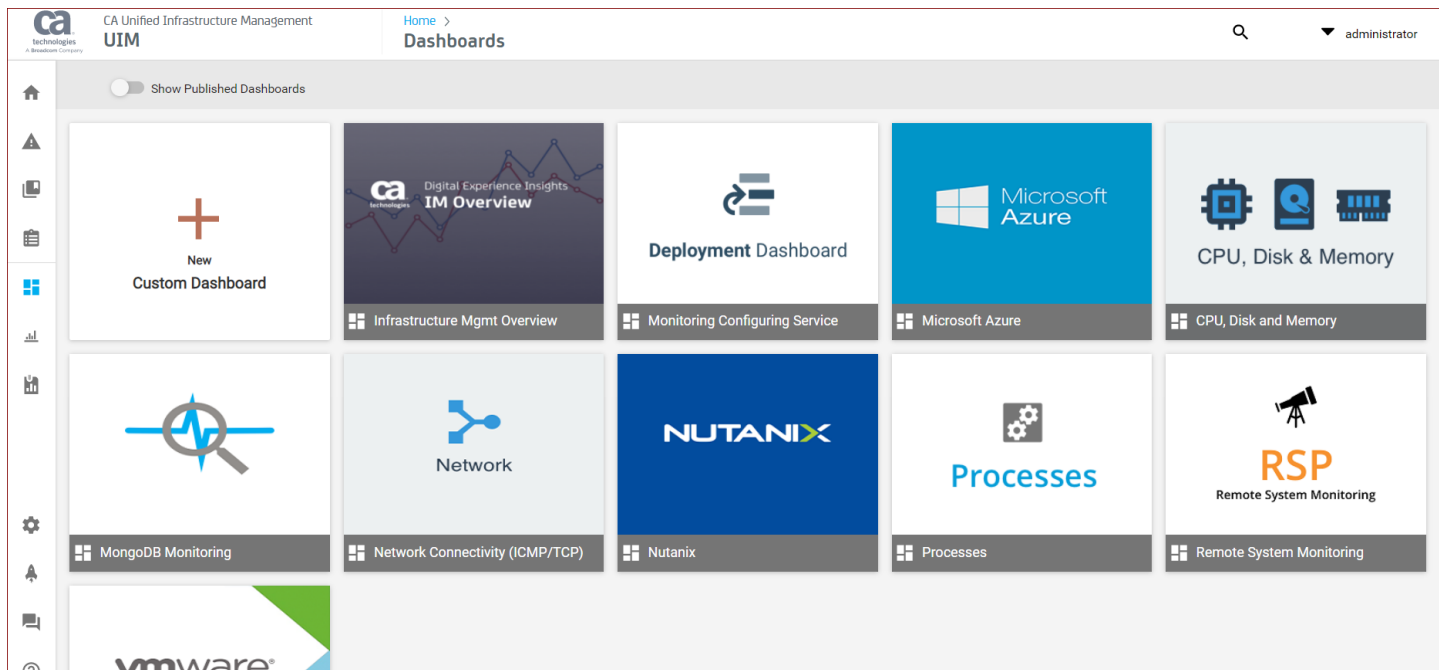
UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

For more information about CABI dashboards, see [CA Business Intelligence with CA UIM](#)

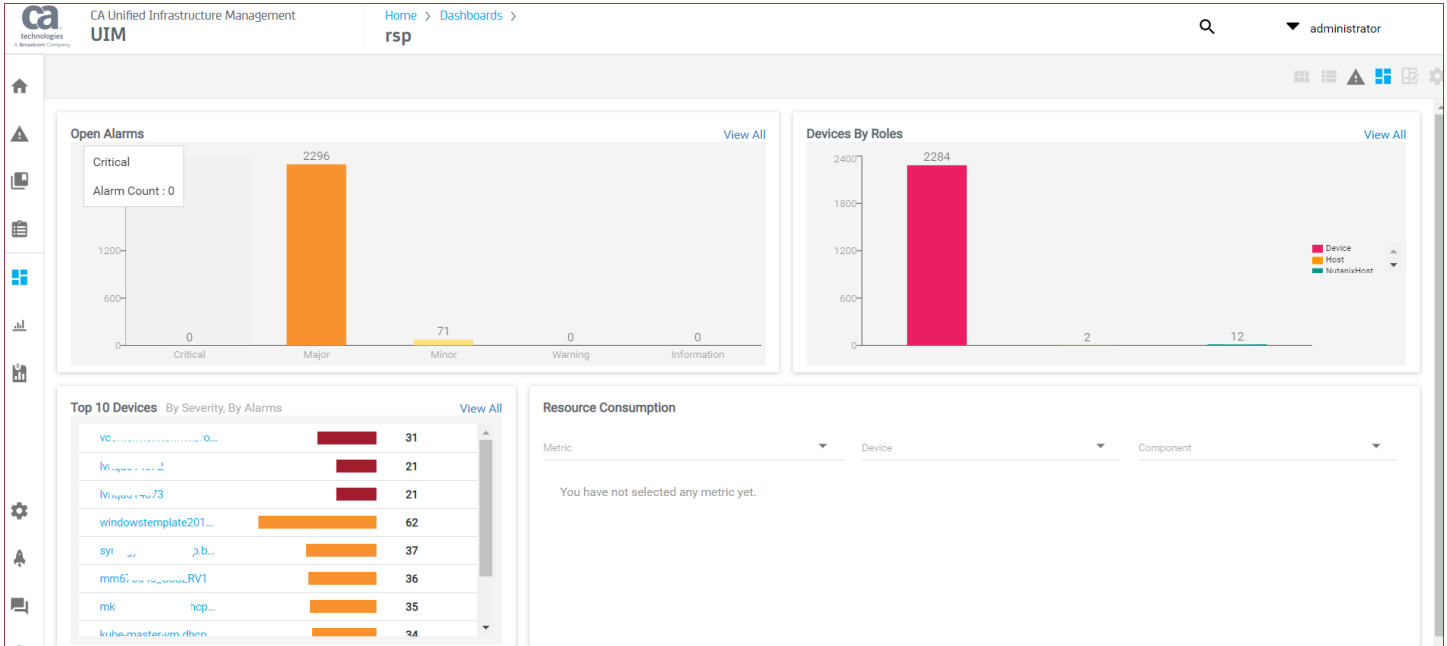
Dashboards view displays the CABI dashboards and the dashboards for the configured probes. Dashboards are displayed of the tenancy and origins as per the user's access and based on the ACL permissions. By Default, Infrastructure Management Overview and the Monitoring Configuring Service dashboards are displayed when there are no probes configured. In UIM 20.3.3, for the monitoring technologies (probes) like cdm, processes, rsp, and so on, the respective dashboard views are rendered by using HTML5 instead of CABI.

You can also create new custom dashboard views using CABI. Published dashboards can be viewed by toggling the "Show Published Dashboards" on the top of the Dashboards view.

The following screenshot shows the Dashboards view in UIM 20.3.3:



In UIM 20.3.3, the dashboard pages for the monitoring technologies (probes) like processes, rsp, cdm, net\_connect, and so on are rendered by using HTML5, not CABI. Therefore, when you click a tile on the main Dashboards page, the dashboard pages for such probes are rendered by using HTML5. The following screenshot shows an example of the cdm probe dashboard page in UIM 20.3.3:



## AD Server Unified Dashboard

### Contents

### AD Server Required Data Sources

The table contains the QoS metrics that are required for the preconfigured AD Server dashboard.

| QoS Required                 | Subkey/Target               |
|------------------------------|-----------------------------|
| QOS_DIRECTORIES              | Directories                 |
| QOS_FILEAGEOLDEST            | File Age Oldest             |
| QOS_FILES                    | Files                       |
| QOS_TOTALSIZE                | Total Size                  |
| QOS %Processor Time          | Perc Processor Time         |
| QOS I/O Data Bytes/sec       | IO Data Bytes Per Sec       |
| QOS_I/O Data Operations/sec  | IO Data Operations Per Sec  |
| QOS_I/O Read Operations/sec  | IO Read Operations Per Sec  |
| QOS_I/O Write Operations/sec | IO Write Operations Per Sec |
| QOS_Page Faults/sec          | Page Faults Per Sec         |

### Directories

| Column      | Description                               |
|-------------|-------------------------------------------|
| Host        | Name of the host where AD Server exists.  |
| Profile     | Target that is being monitored.           |
| Directories | Number of directories in the file system. |

**Oldest File's Age**

| Column          | Description                              |
|-----------------|------------------------------------------|
| Host            | Name of the host where AD Server exists. |
| Profile         | Target that is being monitored.          |
| File Age Oldest | Age of oldest file in the file system.   |

**Files**

| Column  | Description                              |
|---------|------------------------------------------|
| Host    | Name of the host where AD Server exists. |
| Profile | Target that is being monitored.          |
| Files   | Number of files in a file system.        |

**Total Size**

| Column     | Description                              |
|------------|------------------------------------------|
| Host       | Name of the host where AD Server exists. |
| Profile    | Target that is being monitored.          |
| Total Size | Total size of a file system.             |

**Percentage Processor Time**

| Column              | Description                                        |
|---------------------|----------------------------------------------------|
| Host                | Name of the host where AD Server exists.           |
| Profile             | Target that is being monitored.                    |
| Perc Processor Time | % of processor time that is consumed by a process. |

**IO Data Bytes Per Second**

| Column                   | Description                                                 |
|--------------------------|-------------------------------------------------------------|
| Host                     | Name of the host where AD Server exists.                    |
| Profile                  | Target that is being monitored.                             |
| IO Data Bytes Per Second | Data Bytes transferred by process IO operations per second. |

**IO Data Operations Per Second**

| Column                        | Description                                                |
|-------------------------------|------------------------------------------------------------|
| Host                          | Name of the host where AD Server exists.                   |
| Profile                       | Target that is being monitored.                            |
| IO Data Operations Per Second | Number of IO Operations performed by a process per second. |

**IO Read Operations Per Second**

| Column                        | Description                                                  |
|-------------------------------|--------------------------------------------------------------|
| Host                          | Name of the host where AD Server exists.                     |
| Profile                       | Target that is being monitored.                              |
| IO Data Operations Per Second | Number of Read Operations performed by a process per second. |

**IO Write Operations Per Second**

| Column                        | Description                                                            |
|-------------------------------|------------------------------------------------------------------------|
| Host                          | Name of the host where AD Server exists.                               |
| Profile                       | Target that is being monitored.                                        |
| IO Data Operations Per Second | Number of Write Operations that are performed by a process per second. |

**Page Faults Per Second**

| Column                 | Description                              |
|------------------------|------------------------------------------|
| Host                   | Name of the host where AD Server exists. |
| Profile                | Target that is being monitored.          |
| Page Faults Per Second | Number of paging faults per second.      |

**Apache Unified Dashboard**

The Apache Unified Dashboard provides predefined list views for monitoring CPU and HTTP Request.

**Contents****Required Data Sources**

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the Apache dashboard.

| QoS                       | Subkey/Target |
|---------------------------|---------------|
| QOS_APACHE_CPU_LOAD       | *             |
| QOS_APACHE_REQMAXTIME     | *             |
| QOS_APACHE_REQPERSEC      | *             |
| QOS_APACHE_BYTESPERREQ    | *             |
| QOS_APACHE_READINGREQUEST | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

## CPU

This chart displays information about the CPU Load and its usage.

| Column Name | Description                                             |
|-------------|---------------------------------------------------------|
| CPU Load    | CPU Load of the machine where apache server is running. |

## HTTP Request

This chart displays information about the HTTP Request.

| Column Name                | Description                                                   |
|----------------------------|---------------------------------------------------------------|
| Request Maximum Time       | The maximum request processing time in ms.                    |
| Request Per Second         | The number of requests per second on the apache server.       |
| Bytes Per Request          | The average number of bytes per request on the apache server. |
| Connection Reading Request | The connection reading request of the apache server.          |

## AWS Auto Scaling Unified Dashboard

The Amazon Web Services (AWS) Auto Scaling Unified Dashboard provides a predefined list view with key performance indicators for your AWS Auto Scaling environment.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS Auto Scaling Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS Auto Scaling Unified dashboard.

| QoS Name                                    | Subkey/Target |
|---------------------------------------------|---------------|
| QOS_AWS_AUTO_SCALING_STATUSCHECK            | *             |
| QOS_AWS_AUTO_SCALING_STATUSCHECK_INSTANCE   | *             |
| QOS_AWS_AUTO_SCALING_STATUSCHECK_SYSTEM     | *             |
| QOS_AWS_AUTO_SCALING_GROUP_MINIMUM_SIZE     | Average       |
| QOS_AWS_AUTO_SCALING_GROUP_MAXIMUM_SIZE     | Average       |
| QOS_AWS_AUTO_SCALING_GROUP_DESIRED_CAPACITY | Average       |

|                                                  |         |
|--------------------------------------------------|---------|
| QOS_AWS_AUTO_SCALING_GROUP_IN_SERVICE_INSTANCES  | Average |
| QOS_AWS_AUTO_SCALING_GROUP_PENDING_INSTANCES     | Average |
| QOS_AWS_AUTO_SCALING_GROUP_STANDBY_INSTANCES     | Average |
| QOS_AWS_AUTO_SCALING_GROUP_TERMINATING_INSTANCES | Average |
| QOS_AWS_AUTO_SCALING_GROUP_TOTAL_INSTANCES       | Average |
| QOS_AWS_AUTO_SCALING_CPU_UTILIZATION             | Average |
| QOS_AWS_AUTO_SCALING_DISK_READ_OPS               | Average |
| QOS_AWS_AUTO_SCALING_DISK_WRITE_OPS              | Average |
| QOS_AWS_AUTO_SCALING_DISK_READ_BYTES             | Average |
| QOS_AWS_AUTO_SCALING_DISK_WRITE_BYTES            | Average |
| QOS_AWS_AUTO_SCALING_NETWORK_IN                  | Average |
| QOS_AWS_AUTO_SCALING_NETWORK_OUT                 | Average |

### **Auto Scaling Group Summary**

This table displays information about the health and performance of the AWS Auto Scaling groups.

| Column                | Description                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Desired Capacity      | The number of instances that the Auto Scaling group maintains.                                                                                                                              |
| Minimum Size          | The minimum size of the Auto Scaling group.                                                                                                                                                 |
| Maximum Size          | The maximum size of the Auto Scaling group.                                                                                                                                                 |
| Total Instances       | The total number of instances ( <b>in service</b> , <b>pending</b> , and <b>terminating</b> ) in the Auto Scaling group.                                                                    |
| In Service Instances  | The number of instances that are currently <b>executing</b> in the Auto Scaling group.                                                                                                      |
| Pending Instances     | The number of instances that are currently pending in the Auto Scaling group. Amazon defines a pending instance as <b>not yet in service</b> .                                              |
| Standby Instances     | The number of instances that are in Standby state in the Auto Scaling group. Amazon defines an instances as standby when the instance is <b>executing, but is not actively in service</b> . |
| Terminating Instances | The number of instances that are currently <b>terminating</b> in the Auto Scaling group.                                                                                                    |

### **Auto Scaling Health Summary**

This table displays information about the health of the AWS Auto Scaling service.

| Column                       | Description                                                                                                                         |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Status Check Failed          | The operational status of the service as a combination of the Status Check Failed Instance and Status Check Failed System monitors. |
| Status Check Failed Instance | The operational status of the instance.                                                                                             |
| Status Check Failed System   | The operational status of the system.                                                                                               |

### **Auto Scaling Performance Summary**

This table displays information about the performance of the AWS Auto Scaling service.

| Column           | Description                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU Utilization  | The percentage of allocated EC2 compute units that are currently in use on the instance. You can use the information to identify the processing power required to execute an application on the selected instance. |
| Disk Read Ops    | The number of completed read operations from all ephemeral disks available to the instance. You can use the information to identify the rate at which an application reads from a disk.                            |
| Disk Write Ops   | The number of completed write operations to all ephemeral disks available to the instance. You can use the information to identify the rate at which an application writes to a disk.                              |
| Disk Read Bytes  | The number of bytes read from all ephemeral disks available to the instance. You can use the information to determine the volume of data that the application reads from the hard disk of the instance.            |
| Disk Write Bytes | The number of bytes written to all ephemeral disks available to the instance. You can use the information to determine the volume of data that the application writes to the hard disk of the instance.            |

|             |                                                                                                                                                                                           |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network In  | The number of bytes received on all network interfaces by the instance. You can use the information to identify the volume of incoming network traffic to an application on the instance. |
| Network Out | The number of bytes sent on all network interfaces by the instance. You can use the information to identify the volume of outgoing network traffic from an application on the instance.   |

## AWS Billing Unified Dashboard

The Amazon Web Services (AWS) Billing Unified Dashboard provides a predefined list view with estimated charge indicators for your AWS environment.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS Billing Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS Billing Unified dashboard.

| QoS Name                         | Subkey/Target |
|----------------------------------|---------------|
| QOS_AWS_BILLING_ESTIMATED_CHARGE | *             |

### Estimated Charges Summary

This table displays information about the billing charges of configured AWS services.

| Column            | Description                                                  |
|-------------------|--------------------------------------------------------------|
| Estimated Charges | The estimated billing charges of the service, in US Dollars. |

## AWS DynamoDB Unified Dashboard

The Amazon Web Services (AWS) DynamoDB Unified Dashboard provides a predefined list view with key performance indicators for your AWS DynamoDB environment.

### Contents



**NOTE**

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**AWS DynamoDB Required Data Sources**

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS DynamoDB Unified dashboard.

| QoS Name                                                    | Subkey/Target |
|-------------------------------------------------------------|---------------|
| QOS_AWS_DYNAMODB_INDEX_ONLINE_INDEX_CONSUMED_WRITE_CAPACITY | Average       |
| QOS_AWS_DYNAMODB_INDEX_ONLINE_INDEX_PERCENTAGE_PROGRESS     | Average       |
| QOS_AWS_DYNAMODB_INDEX_ONLINE_INDEX_THROTTLE_EVENTS         | Average       |
| QOS_AWS_DYNAMODB_CONSUMED_READ_CAPACITY_UNITS               | Average       |
| QOS_AWS_DYNAMODB_CONSUMED_WRITE_CAPACITY_UNITS              | Average       |
| QOS_AWS_DYNAMODB_PROVISIONED_READ_CAPACITY_UNITS            | Average       |
| QOS_AWS_DYNAMODB_PROVISIONED_WRITE_CAPACITY_UNITS           | Average       |
| QOS_AWS_DYNAMODB_SCAN_SUCCESSFUL_REQUEST_LATENCY            | Average       |
| QOS_AWS_DYNAMODB_SYSTEM_ERRORS                              | Sum           |
| QOS_AWS_DYNAMODB_ONLINE_INDEX_THROTTLE_EVENTS               | Average       |
| QOS_AWS_DYNAMODB_READ_THROTTLE_EVENTS                       | Sum           |
| QOS_AWS_DYNAMODB_PUT_ITEM_THROTTLED_REQUESTS                | Sum           |
| QOS_AWS_DYNAMODB_DELETE_ITEM_THROTTLED_REQUESTS             | Sum           |

|                                                      |         |
|------------------------------------------------------|---------|
| QOS_AWS_DYNAMODB_UPDATE_ITEM_THROTTLED_REQUESTS      | Sum     |
| QOS_AWS_DYNAMODB_GET_ITEM_THROTTLED_REQUESTS         | Sum     |
| QOS_AWS_DYNAMODB_BATCH_GET_ITEM_THROTTLED_REQUESTS   | Sum     |
| QOS_AWS_DYNAMODB_SCAN_THROTTLED_REQUESTS             | Sum     |
| QOS_AWS_DYNAMODB_QUERY_THROTTLED_REQUESTS            | Sum     |
| QOS_AWS_DYNAMODB_BATCH_WRITE_ITEM_THROTTLED_REQUESTS | Average |
| QOS_AWS_DYNAMODB_GET_RECORDS_THROTTLED_REQUESTS      | Sum     |
| QOS_AWS_DYNAMODB_WRITE_THROTTLE_EVENTS               | Average |

### **DynamoDB Index Summary**

This table displays information about the DynamoDB indexes in AWS.

| Column                               | Description                                                                                               |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Online Index Throttle Events         | The number of write throttle events that occur when adding a new global secondary index to a table.       |
| Online Index Consumed Write Capacity | The number of write capacity units of index consumed when adding a new global secondary index to a table. |
| Online Index Percentage Progress     | The percentage of completion when a new global secondary index is being added to a table.                 |

### **DynamoDB Table Operation Summary**

This table displays information about the DynamoDB table operations in AWS.

| Column                        | Description                                                                 |
|-------------------------------|-----------------------------------------------------------------------------|
| Consumed Read Capacity Units  | The number of read capacity units consumed over the specified time period.  |
| Consumed Write Capacity Units | The number of write capacity units consumed over the specified time period. |

|                                  |                                                                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Scan Successful Request Latency  | The elapsed time for successful Scan requests during the specified time period.                                               |
| System Errors                    | The number of requests generating a 500 status code (likely indicating a server error) response in the specified time period. |
| Provisioned Read Capacity Units  | The number of provisioned read capacity units for a table or a global secondary index.                                        |
| Provisioned Write Capacity Units | The number of provisioned write capacity units for a table or a global secondary index                                        |

### **DynamoDB Table Throttled Summary**

This table displays information about the DynamoDB throttled table operations in AWS.

| <b>Column</b>                       | <b>Description</b>                                                                                                                            |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Online Index Throttle Events        | The number of write throttle events that occur when adding a new global secondary index to a table.                                           |
| Read Throttle Events                | The number of read events that exceeded the preset provisioned throughput limits in the specified time period.                                |
| Put Item Throttled Requests         | The number of user requests for PutItem operation that exceeded the preset provisioned throughput limits in the specified time period.        |
| Delete Item Throttled Requests      | The number of user requests for DeleteItem operation that exceeded the preset provisioned throughput limits in the specified time period.     |
| Update Item Throttled Requests      | The number of user requests for UpdateItem operation that exceeded the preset provisioned throughput limits in the specified time period.     |
| Get Item Throttled Requests         | The number of user requests for GetItem operation that exceeded the preset provisioned throughput limits in the specified time period.        |
| Batch Get Item Throttled Requests   | The number of user requests for BatchGetItem operation that exceeded the preset provisioned throughput limits in the specified time period.   |
| Scan Throttled Requests             | The number of user requests for Scan operation that exceeded the preset provisioned throughput limits in the specified time period.           |
| Query Throttled Requests            | The number of user requests for Query operation that exceeded the preset provisioned throughput limits in the specified time period.          |
| Batch Write Item Throttled Requests | The number of user requests for BatchWriteItem operation that exceeded the preset provisioned throughput limits in the specified time period. |
| Get Records Throttled Requests      | The number of user requests for GetRecords operation that exceeded the preset provisioned throughput limits in the specified time period.     |

|                       |                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------|
| Write Throttle Events | The number of write events that exceeded the preset provisioned throughput limits in the specified time period. |
|-----------------------|-----------------------------------------------------------------------------------------------------------------|

## AWS EC2 Unified Dashboard

The Amazon Web Services (AWS) EC2 Unified Dashboard provides a predefined list view with key performance indicators for your AWS EC2 environment.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS EC2 Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS EC2 Unified dashboard.

| QoS Name                     | Subkey/Target |
|------------------------------|---------------|
| QOS_AWS_INSTANCE_POWER_STATE | Average       |
| QOS_AWS_CPU_UTILIZATION      | Average       |
| QOS_AWS_DISK_WRITE_BYTES     | Average       |
| QOS_AWS_DISK_READ_BYTES      | Average       |
| QOS_AWS_DISK_READ_OPS        | Average       |
| QOS_AWS_DISK_WRITE_OPS       | Average       |
| QOS_AWS_NETWORK_IN           | Average       |
| QOS_AWS_NETWORK_OUT          | Average       |
| QOS_AWS_VOLUME_QUEUE_LENGTH  | Average       |

### EC2 Instance Summary

This table displays information about the health and performance of the AWS EC2 instances.

| Column           | Description                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power State      | The current power state of the EC2 instance.                                                                                                                                                                       |
| CPU Utilization  | The percentage of allocated EC2 compute units that are currently in use on the instance. You can use the information to identify the processing power required to execute an application on the selected instance. |
| Disk Write Bytes | The number of bytes written to all ephemeral disks available to the instance. You can use the information to determine the volume of data that the application writes to the hard disk of the instance.            |
| Disk Read Bytes  | The number of bytes read from all ephemeral disks available to the instance. You can use the information to determine the volume of data that the application reads from the hard disk of the instance.            |

|                     |                                                                                                                                                                                           |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disk Read Ops       | The number of completed read operations from all ephemeral disks available to the instance. You can use the information to identify the rate at which an application reads from a disk.   |
| Disk Write Ops      | The number of completed write operations to all ephemeral disks available to the instance. You can use the information to identify the rate at which an application writes to a disk.     |
| Network In          | The number of bytes received on all network interfaces by the instance. You can use the information to identify the volume of incoming network traffic to an application on the instance. |
| Network Out         | The number of bytes sent on all network interfaces by the instance. You can use the information to identify the volume of outgoing network traffic from an application on the instance.   |
| Volume Queue Length | The number of read and write operation requests waiting to be completed in the time period specified in the <b>Start Time</b> field.                                                      |

## AWS ElastiCache Unified Dashboard

The Amazon Web Services (AWS) ElastiCache Unified Dashboard provides a predefined list view with key performance indicators for your AWS ElastiCache environment.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS ElastiCache Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS ElastiCache Unified dashboard.

| QoS Name                                              | Subkey/Target |
|-------------------------------------------------------|---------------|
| QOS_AWS_ELASTICACHE_MEMCACHED_EVICTI<br>ONS           | Average       |
| QOS_AWS_ELASTICACHE_MEMCACHED_GET<br>_HITS            | Average       |
| QOS_AWS_ELASTICACHE_MEMCACHED_GET<br>_MISSES          | Average       |
| QOS_AWS_ELASTICACHE_MEMCACHED_CUR<br>RENT_CONNECTIONS | Average       |
| QOS_AWS_ELASTICACHE_MEMCACHED_UNU<br>SED_MEMORY       | Average       |
| QOS_AWS_ELASTICACHE_REDIS_CURRENT_<br>CONNECTIONS     | Average       |

|                                      |         |
|--------------------------------------|---------|
| QOS_AWS_ELASTICACHE_REDIS_EVICTIIONS | Average |
| QOS_AWS_ELASTICACHE_CPU_UTILIZATION  | Average |
| QOS_AWS_ELASTICACHE_SWAP_USAGE       | Average |

### **ElastiCache Memcached Summary**

This table displays information about the memcached performance of the AWS ElastiCache service.

| Column                  | Description                                                                                                                                                                                                                         |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unused Memory           | The amount of unused memory the cache can use to store items. This is derived from the memcached statistics <code>limit_maxbytes</code> and <code>bytes</code> by subtracting <code>bytes</code> from <code>limit_maxbytes</code> . |
| Memcached Hit Requests  | The number of get requests the cache has received where the key requested was found.                                                                                                                                                |
| Memcached Miss Requests | The number of get requests the cache has received where the key requested was not found.                                                                                                                                            |
| Current Connections     | The number of connections connected to the cache at an instant in time.                                                                                                                                                             |
| Evictions               | The number of non-expired items the cache evicted to allow space for new writes.                                                                                                                                                    |

### **ElastiCache Redis Summary**

This table displays information about the redis performance of the AWS ElastiCache service.

| Column              | Description                                                                 |
|---------------------|-----------------------------------------------------------------------------|
| Current Connections | The number of client connections, excluding connections from read replicas. |
| Evictions           | The number of keys that have been evicted due to the maximum memory limit.  |

## ElastiCache Host Summary

This table displays information about the CPU and memory performance of the AWS ElastiCache service.

| Column          | Description                          |
|-----------------|--------------------------------------|
| CPU Utilization | The percentage of CPU utilization.   |
| Swap Usage      | The amount of swap used on the host. |

## AWS ELB Unified Dashboard

The Amazon Web Services (AWS) ELB Unified Dashboard provides a predefined list view with key performance indicators for your AWS ELB environment.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS ELB Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS ELB Unified dashboard.

| QoS Name                          | Subkey/Target |
|-----------------------------------|---------------|
| QOS_AWS_ELB_REQUEST_COUNT         | Sum           |
| QOS_AWS_ELB_LATENCY               | Average       |
| QOS_AWS_ELB_HTTP_CODE_ELB_4XX     | Sum           |
| QOS_AWS_ELB_HTTP_CODE_ELB_5XX     | Sum           |
| QOS_AWS_ELB_HTTP_CODE_BACKEND_2XX | Sum           |
| QOS_AWS_ELB_HTTP_CODE_BACKEND_3XX | Sum           |
| QOS_AWS_ELB_HTTP_CODE_BACKEND_4XX | Sum           |
| QOS_AWS_ELB_HTTP_CODE_BACKEND_5XX | Sum           |

### ELB Health Summary

This table displays information about the health and performance of the AWS ELB service.

| Column               | Description                                                                                                                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTPCode Backend 2XX | The number of HTTP response codes generated by back-end instances. The 2XX class status codes represent successful actions. This metric does not include any response codes generated by the load balancer. |

|                      |                                                                                                                                                                                                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTPCode Backend 3XX | The number of HTTP response codes generated by back-end instances. The 3XX class status code indicates that the user agent requires action. This metric does not include any response codes generated by the load balancer.                                                                         |
| HTTPCode Backend 4XX | The number of HTTP response codes generated by back-end instances. The 4XX class status code represents client errors. This metric does not include any response codes generated by the load balancer.                                                                                              |
| HTTPCode Backend 5XX | The number of HTTP response codes generated by back-end instances. The 5XX class status code represents back-end server errors. This metric does not include any response codes generated by the load balancer, or if the request rate exceeds the capacity of the instances or the load balancers. |
| HTTPCode ELB 4XX     | The number of HTTP 4XX client error codes generated by the load balancer when the listener is configured to use HTTP or HTTPS protocols. Client errors are generated when a request is malformed or is incomplete.                                                                                  |
| HTTPCode ELB 5XX     | The number of HTTP 5XX server error codes generated by the load balancer when the listener is configured to use HTTP or HTTPS protocols. The metric is reported if there are no back-end instances that are healthy or registered to the load balancer.                                             |



|               |                                                                                             |
|---------------|---------------------------------------------------------------------------------------------|
| Latency       | The time elapsed after the request leaves the load balancer until the response is received. |
| Request Count | The number of completed requests that were received and routed to the back-end instances.   |

## AWS RDS Unified Dashboard

The Amazon Web Services (AWS) RDS Unified Dashboard provides a predefined list view with key performance indicators for your AWS RDS environment.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS RDS Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS RDS Unified dashboard.

| QoS Name                       | Subkey/Target |
|--------------------------------|---------------|
| QOS_AWS_RDS_BIN_LOG_DISK_USAGE | Average       |
| QOS_AWS_RDS_DISK_QUEUE_DEPTH   | Average       |
| QOS_AWS_RDS_FREE_STORAGE_SPACE | Average       |
| QOS_AWS_RDS_READ_IOPS          | Average       |
| QOS_AWS_RDS_WRITE_IOPS         | Average       |
| QOS_AWS_RDS_READ_LATENCY       | Average       |
| QOS_AWS_RDS_WRITE_LATENCY      | Average       |
| QOS_AWS_RDS_READ_THROUGHPUT    | Average       |
| QOS_AWS_RDS_WRITE_THROUGHPUT   | Average       |
| QOS_AWS_RDS_CPU_UTILIZATION    | Average       |
| QOS_AWS_RDS_SWAP_USAGE         | Average       |

|                             |         |
|-----------------------------|---------|
| QOS_AWS_RDS_FREEABLE_MEMORY | Average |
|-----------------------------|---------|

**RDS Disk Summary**

**NOTE**

Values for the **Bin Log Disk Usage** column is only available for non-SQL Server RDS instances.

This table displays information about the disk performance of the AWS RDS service.

| Column             | Description                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------|
| Bin Log Disk Usage | The amount of disk space occupied by binary logs on the master. Applies to MySQL read replicas. |
| Disk Queue Depth   | The number of outstanding IOs (read/write requests) waiting to access the disk.                 |
| Free Storage Space | The amount of available storage space.                                                          |
| Read IOPS          | The average number of disk read I/O operations per second.                                      |
| Read Latency       | The average amount of time taken per disk read I/O operation.                                   |
| Read Throughput    | The average number of bytes read from disk per second.                                          |
| Write IOPS         | The average number of disk write I/O operations per second.                                     |
| Write Latency      | The average amount of time taken per disk write I/O operation.                                  |
| Write Throughput   | The average number of bytes written to disk per second.                                         |

**RDS CPU and Memory Summary**

This table displays information about the CPU and memory performance of the AWS RDS service.

| Column          | Description                                       |
|-----------------|---------------------------------------------------|
| CPU Utilization | The percentage of CPU utilization.                |
| Freeable Memory | The amount of available random access memory.     |
| Swap Usage      | The amount of swap space used on the DB Instance. |

## AWS Route 53 Unified Dashboard

The Amazon Web Services (AWS) Route 53 Unified Dashboard provides a predefined list view with key performance indicators for your AWS Route 53 environment.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS Route 53 Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS Route 53 Unified dashboard.

| QoS Name                                | Subkey/Target |
|-----------------------------------------|---------------|
| QOS_AWS_ROUTE53_CONNECTION_TIME         | Average       |
| QOS_AWS_ROUTE53_HEALTH_CHECK_PERCENTAGE | Average       |
| QOS_AWS_ROUTE53_HEALTH_CHECK_STATUS     | Minimum       |
| QOS_AWS_ROUTE53_SSL_HANDSHAKE_TIME      | Average       |
| QOS_AWS_ROUTE53_TIME_TO_FIRST_BYTE      | Average       |

### Route 53 Health Summary

This table displays information about the health and performance of the AWS Route 53 service.

| Column                  | Description                                                                                             |
|-------------------------|---------------------------------------------------------------------------------------------------------|
| Connection Time         | The time that it takes Amazon Route 53 health checkers to establish a TCP connection with the endpoint. |
| Health Check Percentage | The percentage of Amazon Route 53 health checkers that consider the selected endpoint to be healthy.    |

|                     |                                                                                                                                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Health Check Status | The health status of the service. You can set up the threshold for status using a numeric value between 0 and 1. Each number is assigned a status value, as follows: <ul style="list-style-type: none"> <li>• 0: Unhealthy</li> <li>• 1: Healthy</li> </ul> |
| SSL Handshake Time  | The time that it takes Amazon Route 53 health checkers to complete the SSL handshake.                                                                                                                                                                       |
| Time To First Byte  | The time that it takes Amazon Route 53 health checkers to receive the first byte of the response to an HTTP or HTTPS request.                                                                                                                               |

## AWS S3 Unified Dashboard

The Amazon Web Services (AWS) S3 Unified Dashboard provides a predefined list view with key performance indicators for your AWS S3 environment.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS S3 Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS S3 Unified dashboard.

| QoS Name                  | Subkey/Target |
|---------------------------|---------------|
| QOS_AWS_BUCKET_SIZE       | *             |
| QOS_AWS_NUMBER_OF_OBJECTS | *             |

### S3 Health Summary

This table displays information about the size and number of objects in a bucket of the AWS S3 service.

| Column      | Description                                    |
|-------------|------------------------------------------------|
| Bucket Size | The amount of data that is stored in a bucket. |

|                   |                                                          |
|-------------------|----------------------------------------------------------|
| Number Of Objects | The total number of objects that are stored in a bucket. |
|-------------------|----------------------------------------------------------|

## AWS SNS Unified Dashboard

The Amazon Web Services (AWS) SNS Unified Dashboard provides a predefined list view with key performance indicators for your AWS SNS environment.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS SNS Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS SNS Unified dashboard.

| QoS Name                                             | Subkey/Target |
|------------------------------------------------------|---------------|
| QOS_AWS_SNS_NUMB<br>ER_OF_MESSAGES_PU<br>BLISHED     | Sum           |
| QOS_AWS_SNS_NUMB<br>ER_OF_NOTIFICATION<br>_DELIVERED | Sum           |
| QOS_AWS_SNS_NUMB<br>ER_OF_NOTIFICATION<br>_FAILED    | Sum           |

### SNS Health

This table displays information about the health and performance of the AWS SNS service.

| Column                               | Description                                        |
|--------------------------------------|----------------------------------------------------|
| Number Of Messages<br>Published      | The number of messages published.                  |
| Number Of Notifications<br>Delivered | The number of messages successfully delivered.     |
| Number Of Notifications<br>Failed    | The number of messages that SNS failed to deliver. |

## AWS SQS Unified Dashboard

The Amazon Web Services (AWS) SQS Unified Dashboard provides a predefined list view with key performance indicators for your AWS SQS environment.

### Contents

**NOTE**

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**AWS SQS Required Data Sources**

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the AWS SQS Unified dashboard.

| QoS Name                                             | Subkey/Target |
|------------------------------------------------------|---------------|
| QOS_AWS_SQS_SENT_MESSAGE_SIZE                        | Average       |
| QOS_AWS_SQS_NUMB ER_OF_EMPTY_RECEI VES               | Sum           |
| QOS_AWS_SQS_NUMB ER_OF_MESSAGES_D ELETED             | Sum           |
| QOS_AWS_SQS_APPR OXIMATE_NUMBER_OF _MESSAGES_DELAYED | Average       |
| QOS_AWS_SQS_APPR OXIMATE_NUMBER_OF _MESSAGES_VISIBLE | Average       |

**SQS Health Summary**

This table displays information about the health and performance of the AWS SQS service.

| Column                                 | Description                                                                                                                                                                                                           |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Approximate Number Of Messages Delayed | The number of messages in the queue that are delayed and not available for reading immediately. This can happen when the queue is configured as a delay queue or when a message has been sent with a delay parameter. |
| Approximate Number Of Messages Visible | The number of messages available for retrieval from the queue.                                                                                                                                                        |
| Number Of Empty Receives               | The number of ReceiveMessage API calls that did not return a message.                                                                                                                                                 |
| Number Of Messages Deleted             | The number of messages deleted from the queue.                                                                                                                                                                        |

|                   |                                        |
|-------------------|----------------------------------------|
| Sent Message Size | The size of messages added to a queue. |
|-------------------|----------------------------------------|

## AWS Unified Dashboard

The Amazon Web Services (AWS) Unified Dashboard provides predefined list views with key performance indicators for your AWS environment including EC2 instance performance, S3 storage time, and more.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### AWS Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the AWS dashboard.

| Probe                  | QoS Required                | Subkey/Target                 |
|------------------------|-----------------------------|-------------------------------|
| aws                    | QOS_FILE_READ_TIME          | File Transfer Time            |
|                        | QOS_FILE_WRITE_TIME         | File Transfer Time            |
|                        | QOS_CPU_UTILIZATION         | Minimum<br>Maximum<br>Average |
|                        | QOS_DISK_READ_BYTES         | Average                       |
|                        | QOS_DISK_WRITE_BYTES        | Average                       |
|                        | QOS_DISK_READ_OPS           | Average                       |
|                        | QOS_DISK_WRITE_OPS          | Average                       |
|                        | QOS_NETWORK_IN              | Average                       |
|                        | QOS_NETWORK_OUT             | Average                       |
|                        | QOS_QUEUE_LENGTH            | Average                       |
|                        | QOS_STATUSCHECK             | Average                       |
|                        | QOS_STATUSCHECK_INSTANCE    | Average                       |
|                        | QOS_STATUSCHECK_SYSTEM      | Average                       |
|                        | QOS_MEMCACHED_UNUSED_MEMORY | Average                       |
|                        | QOS_MEMCACHED_HIT_REQUESTS  | Average                       |
|                        | QOS_MEMCACHED_MISS_REQUEST  | Average                       |
|                        | QOS_SENT_MESSAGE_SIZE       | Average                       |
|                        | QOS_MESSAGES_RECEIVED       | Sum                           |
|                        | QOS_EMPTY_MESSAGES_RECEIVED | Sum                           |
|                        | QOS_MESSAGES_DELETED        | Sum                           |
| QOS_MESSAGES_DELAYED   | Average                     |                               |
| QOS_MESSAGES_IN_FLIGHT | Average                     |                               |
| QOS_PUBLISHED_MESSAGES | Sum                         |                               |

|                             |         |
|-----------------------------|---------|
| QOS_DELIVERED_NOTIFICATIONS | Sum     |
| QOS_FAILED_NOTIFICATIONS    | Sum     |
| QOS_READ_IOPS               | Average |
| QOS_WRITE_IOPS              | Average |
| QOS_READ_LATENCY            | Average |
| QOS_WRITE_LATENCY           | Average |
| QOS_READ_THROUGHPT          | Average |
| QOS_WRITE_THROUGHPUT        | Average |
| QOS_SWAP_USAGE              | Average |
| QOS_AVAILABLE_MEMORY        | Average |
| QOS_BIN_LOG_DISK_USAGE      | Average |
| QOS_DISK_QUEUE_DEPTH        | Average |
| QOS_FREE_STORAGE_SPACE      | Average |
| QOS_LATENCY                 | Average |
| QOS_REQUEST_COUNT           | Average |
| QOS_HTTP_BACKEND_RESPONSE   | Sum     |
| QOS_HTTP_RESPONSE           | Sum     |

### **AWS Instance CPU Usage Summary**

The following chart displays details about the CPU Usage by a specific EC2 instance.

| Column          | Description                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EC2 Instance ID | The instance ID provided by Amazon.                                                                                                                                                                                                                                                     |
| CPU Usage       | Gauge displaying the percentage of allocated EC2 compute units that are currently in use on the instance. This metric identifies the processing power that is required to run an application upon a selected instance.<br>0 to 49.99 = Green<br>50 to 79.99 = Orange<br>80 to 100 = Red |

### **AWS Instance File Read/Write Time**

This chart displays information about the Amazon S3 service and the time that is taken by the AWS probe to store and fetch files from the S3 storage bucket.

| Column          | Description                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| EC2 Instance ID | The instance ID provided by Amazon. Click the name of an instance to view a Performance Report of file read/write time data for that instance. |
| Read Time       | Number of seconds to read a file from the S3 storage bucket to the probe.                                                                      |
| Write Time      | Number of seconds to write a file to the S3 storage bucket from the probe.                                                                     |



### **AWS Instance Disk Read/Write Bytes**

The following chart displays information about the disk space (in Bytes) used by the EC2 instance.

| Column          | Description                                                                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EC2 Instance ID | The instance ID provided by Amazon.                                                                                                                                      |
| Read Bytes      | Bytes read from all disks available to the instance. This metric is used to determine the volume of the data the application reads from the hard disk of the instance.   |
| Write Bytes     | Bytes written to all disks available to the instance. This metric is used to determine the volume of the data the application writes onto the hard disk of the instance. |

### **AWS Instance Disk Read/Write Operations**

This chart displays the details about the read and write operations that the EC2 instance performs on a disk.

| Column          | Description                                                                                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EC2 Instance ID | The instance ID provided by Amazon.                                                                                                                                                                                                               |
| Read Ops        | Completed read operations from all disks available to the instances. This metric identifies the rate at which an application reads a disk. This can be used to determine the speed at which an application reads data from a hard disk.           |
| Write Ops       | Completed write operations to all hard disks available to the instance. This metric identifies the rate at which an application writes to a hard disk. This can be used to determine the speed at which an application saves data to a hard disk. |

### **AWS Network In Out**

This chart displays details about the amount of instance data that is transmitted in the network.

| Column      | Description                                                                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network In  | Mini-graph displaying the number of bytes received on all network interfaces by the instance. This metric identifies the volume of incoming network traffic to an application on a single instance. |
| Network Out | Mini-graph displaying the number of bytes sent out on all network interfaces by the instance. This metric identifies the volume of outgoing network traffic to an application on a single instance. |

### **EBS Health**

This chart displays details about the number of Read and Write operations that are completed in a specific time period.

| Column           | Description                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------|
| Queue Length     | The number of read and write operation requests waiting to be completed in the user-defined time period specified. |
| Read Operations  | The number of Read operations in the user-defined time period.                                                     |
| Write Operations | The number of Write operations in the user-defined time period.                                                    |

### **Auto Scaling Summary**

This chart displays the details about the number of read and write operations, the amount of data that is read and written to a disk, status of an EC2 instance, and the amount of data that are sent and received by the EC2 instance.

| Columns          | Description                                                                                                                                                                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU Utilization  | Gauge displaying the percentage of allocated EC2 compute units that are currently in use on the instance. This metric identifies the processing power that is required to run an application upon a selected instance.<br>0 to 49.99 = Green<br>50 to 79.99 = Orange<br>80 to 100 = Red |
| Disk Read Ops    | Completed read operations from all disks available to the instances. This metric identifies the rate at which an application reads a disk. This can be used to determine the speed at which an application reads data from a hard disk.                                                 |
| Disk Write Ops   | Completed write operations to all ephemeral disks available to the instance in a specified period of time.                                                                                                                                                                              |
| Disk Read Bytes  | Bytes read from all ephemeral disks available to the instance.                                                                                                                                                                                                                          |
| Disk Write Bytes | Bytes written to all ephemeral disks available to the instance.                                                                                                                                                                                                                         |
| Network IN       | The number of bytes received on all network interfaces by the instance.                                                                                                                                                                                                                 |
| Network OUT      | The number of bytes sent out on all network interfaces by the instance.                                                                                                                                                                                                                 |

### **Auto Scaling Health**

This chart displays the details about the EC2 instance and system status check.

| Columns              | Description                                                                               |
|----------------------|-------------------------------------------------------------------------------------------|
| StatusCheck          | Tests the status of an EC2 instance.                                                      |
| StatusCheck Instance | Reports whether the instance has passed the EC2 instance status check in the last minute. |
| StatusCheck System   | Reports whether the instance has passed the EC2 system status check in the last minute.   |

### **ElastiCache Health**

This chart displays details about the ElastiCache Memcached data engine status.

| Columns         | Description                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU Utilization | Gauge displaying the percentage of allocated EC2 compute units that are currently in use on the instance. This metric identifies the processing power that is required to run an application upon a selected instance.<br>0 to 49.99 = Green<br>50 to 79.99 = Orange<br>80 to 100 = Red |

|                         |                                                                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Memcached Unused Memory | The amount of unused memory the cache can use to store items. This is derived from the memcached statistics limit_maxbytes and bytes by subtracting bytes from limit_maxbytes. |
| Memcached Hit Request   | The number of get requests the cache has received where the key requested was found.                                                                                           |
| Memcached Miss Request  | The number of get requests the cache has received where the key requested was not found                                                                                        |

### **SQS Health**

This chart displays details about the status of the queue messages.

| Columns                | Description                                                                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Sent Message Size      | The size of messages added to a queue.                                                                                                           |
| Messages Received      | The number of messages that are returned by calls to the ReceiveMessage API action.                                                              |
| Empty Message Receives | The number of ReceiveMessage API calls that did not return a message.                                                                            |
| Messages Deleted       | The number of messages that are deleted from the queue.                                                                                          |
| Message Delayed        | The number of messages in the queue that are delayed and not available for reading immediately.                                                  |
| Message in Flight      | The number of messages that have been sent to a client but have not yet been deleted or have not yet reached the end of their visibility window. |

### **SNS Health**

This chart displays details about the status of the SNS topic messages.

| Columns                 | Description                                              |
|-------------------------|----------------------------------------------------------|
| Published Messages      | The number of messages published                         |
| Delivered Notifications | The number of messages successfully delivered.           |
| Failed Notifications    | The number of messages that SNS topic failed to deliver. |

### **RDS Health 1**

This chart displays details about the RDS service Read/Write operations that are performed on a disk.

| Columns              | Description                                              |
|----------------------|----------------------------------------------------------|
| Read I/O Per Second  | The average number of disk I/O operations per second.    |
| Write I/O Per Second | The average number of disk I/O operations per second.    |
| Read Latency         | The average amount of time taken per disk I/O operation. |
| Write Latency        | The average amount of time taken per disk I/O operation. |
| Read Throughput      | The average number of bytes read from disk per second.   |
| Write Throughput     | The average number of bytes written to disk per second.  |

**RDS Health 2**

This chart displays information about the memory usage by the RDS service.

| Columns               | Description                                                                                                                                                                                                                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU Utilization       | Gauge displaying the percentage of allocated EC2 compute units that are currently in use on the instance. This metric identifies the processing power that is required to run an application upon a selected instance.<br>0 to 49.99 = Green<br>50 to 79.99 = Orange<br>80 to 100 = Red |
| Swap Usage            | The amount of swap space that is used on the DB Instance.                                                                                                                                                                                                                               |
| Available Memory      | The amount of available Random Access Memory.                                                                                                                                                                                                                                           |
| Binary Log Disk Usage | The amount of disk space that is occupied by binary logs on the master. Applies to MySQL read replicas only.                                                                                                                                                                            |
| Disk Queue Depth      | The number of outstanding IOs (read/write requests) waiting to access the disk.                                                                                                                                                                                                         |
| Free Storage Space    | The amount of available storage space.                                                                                                                                                                                                                                                  |

**ELB Summary**

This chart displays the details of the HTTP request that the ELB service receives.

| Columns                   | Description                                                                                                                                                                                                                            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Latency                   | The time elapsed after the request leaves the load balancer until the response is received.                                                                                                                                            |
| Request Count             | The number of completed requests that were received and routed to the back-end instances.                                                                                                                                              |
| 2XX HTTP Backend Response | The number of HTTP response codes that are generated by back-end instances. This metric does not include any response codes that are generated by the load balancer.                                                                   |
| 3XX HTTP Backend Response | The number of HTTP response codes that are generated by back-end instances. This metric does not include any response codes that are generated by the load balancer.                                                                   |
| 4XX HTTP Backend Response | The number of HTTP response codes that are generated by back-end instances. This metric does not include any response codes that are generated by the load balancer.                                                                   |
| 5XX HTTP Backend Response | The number of HTTP response codes that are generated by back-end instances. This metric does not include any response codes that are generated by the load balancer.                                                                   |
| 4XX HTTP Response         | The number of HTTP 4XX client error codes that are generated by the load balancer when the listener is configured to use HTTP or HTTPS protocols.                                                                                      |
| 5XX HTTP Response         | The number of HTTP 5XX server error codes that are generated by the load balancer when the listener is configured to use HTTP or HTTPS protocols. This metric does not include any responses that are generated by back-end instances. |

## Cassandra Unified Dashboard

The Cassandra Unified Dashboard provides predefined list views for monitoring nodes in a Cassandra cluster.

**Note:** If your Unified Dashboard is not populating with data, verify that all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required monitors are active. For more information, see the help topic on required data sources for the Unified Dashboard.

### Required Data Sources

The following table contains the monitors that you must activate in the Cassandra Monitoring probe to see data in the Cassandra Unified Dashboard.

| Dashboard Chart              | Name                    | QoS                                                    |
|------------------------------|-------------------------|--------------------------------------------------------|
| CF Summary                   | CFRecentReadLatency     | QOS_CASSANDRA_CF_LATENCY_RECENTREADLATENCYMICROS       |
| CF Summary                   | CFReadCount             | QOS_CASSANDRA_CF_OPERATION_STATUS_READCOUNT            |
| CF Summary                   | CFTotalWriteLatency     | QOS_CASSANDRA_CF_LATENCY_TOTALWRITELATENCYMICROS       |
| CF Summary                   | CFWriteCount            | QOS_CASSANDRA_CF_OPERATION_STATUS_WRITECOUNT           |
| CF Summary                   | CFPendingTasks          | QOS_CASSANDRA_CF_OPERATION_STATUS_PENDINGTASKS         |
| Node Capacity                | SystemMemoryFree        | QOS_CASSANDRA_SYS_MEM_FREE                             |
| Node Capacity                | SystemMemoryUsed        | QOS_CASSANDRA_SYS_MEM_USED                             |
| Node Capacity                | SystemMemoryUsedPercent | QOS_CASSANDRA_SYS_MEM_USED_PERCENT                     |
| Node Capacity                | FileSystemCapacity      | QOS_CASSANDRA_SYS_IO_TOTAL                             |
| Node Capacity                | DiskReads               | QOS_CASSANDRA_SYS_IO_DISK_READ_BYTES                   |
| Node Capacity                | DiskWrites              | QOS_CASSANDRA_SYS_IO_DISK_WRITE_BYTES                  |
| Node Memory and Task Summary | NodeTotalDiskSpaceUsed  | QOS_CASSANDRA_NODE_SYS_USAGE_TOTALDISKSPACEUSED        |
| Node Memory and Task Summary | NodePhysicalMemTotal    | QOS_CASSANDRA_NODE_SYS_USAGE_TOTAL_PHYSICALMEMORY_SIZE |
| Node Memory and Task Summary | NodePhysicalMemFree     | QOS_CASSANDRA_NODE_SYS_USAGE_FREE_PHYSICALMEMORY_SIZE  |
| Node Memory and Task Summary | NodeSwapSpaceFree       | QOS_CASSANDRA_NODE_SYS_USAGE_FREESWAPSPACE_SIZE        |
| Node Memory and Task Summary | NodeTotalDiskSpaceUsed  | QOS_CASSANDRA_NODE_SYS_USAGE_TOTALDISKSPACEUSED        |
| Node Memory and Task Summary | NodePendingTasksReads   | QOS_CASSANDRA_NODE_PENDING_TASKS_READS                 |
| Node Memory and Task Summary | NodePendingTasksWrites  | QOS_CASSANDRA_NODE_PENDING_TASKS_WRITES                |
| Node Summary                 | NodeOperation           | QOS_CASSANDRA_NODE_OPERATION_OPERATIONMODE             |

|                     |                               |                                                            |
|---------------------|-------------------------------|------------------------------------------------------------|
| Node Summary        | NodeTotalReadCount            | QOS_CASSANDRA_NODE_OPERATION_STATUS_TOTALREADCOUNT         |
| Node Summary        | NodeTotalWriteCount           | QOS_CASSANDRA_NODE_OPERATION_STATUS_TOTALWRITECOUNT        |
| Node Summary        | NodeRecentReadLatencyAverage  | QOS_CASSANDRA_NODE_LATENCY_AVERAGERECENTREADLATENCYMICROS  |
| Node Summary        | NodeRecentWriteLatencyAverage | QOS_CASSANDRA_NODE_LATENCY_AVERAGERECENTWRITELATENCYMICROS |
| Storage Vol Summary | FileSystemCapacity            | QOS_CASSANDRA_SYS_IO_TOTAL                                 |
| Storage Vol Summary | FileSystemUsage               | QOS_CASSANDRA_SYS_IO_USED                                  |
| Storage Vol Summary | FileSystemFree                | QOS_CASSANDRA_SYS_IO_FREE                                  |

### **CF Summary**

This chart allows you to view the availability of keyspaces in a column family. The dashboard data is updated every hour.

| Column           | Description                                                      |
|------------------|------------------------------------------------------------------|
| Column Families  | All keyspace components that are detected on the node            |
| CF Read Latency  | Total amount of latency for the recent read in the column family |
| CF Read Count    | Total number of reads of the column family                       |
| CF Write Latency | Total amount of latency for write in the column family           |
| CF Write Count   | Total number of writes of the column family                      |
| CF Pending Tasks | Total number of pending tasks regarding the column family        |

### **Node Capacity**

This chart allows you to view disk usage by the filesystems mounted on a node. The dashboard data is updated every hour.

| Column               | Description                                               |
|----------------------|-----------------------------------------------------------|
| Target               | All mounted filesystems on the node                       |
| Mem Free             | Total free system memory (For example, Linux plus cached) |
| Mem Used             | Total used system memory                                  |
| Mem Used Percent     | Percent total used system memory                          |
| IO Total             | Total capacity of the physical disk                       |
| IO Read              | Number of physical disk bytes read                        |
| IO Write             | Number of physical disk bytes written                     |
| File System Capacity | Total capacity of the filesystem                          |

### **Node Memory and Task Summary**

This chart allows you to view node disk capacity. The dashboard data is updated every hour.

| Column                | Description                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------|
| Nodes                 | The name or IP address of the Cassandra node. Click this link to view additional information in OC. |
| Total Disk Space Used | Total disk space that is used                                                                       |
| Total Physical Memory | Total physical memory size for the node                                                             |
| Free Physical Memory  | Free physical memory size for the node                                                              |
| Swap Size             | Total disk space used                                                                               |
| Free Swap Size        | Free swap size for the node                                                                         |
| Pending Reads         | Number of pending tasks regarding reads that have been received but are waiting to be processed     |
| Pending Writes        | Number of pending tasks regarding writes that have been received but are waiting to be processed    |

### **Node Summary**

This chart allows you to view the availability of nodes in your Cassandra cluster. The dashboard data is updated every hour.

| Column            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nodes             | The name or IP address of the Cassandra node. Click this link to view additional information in OC.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| State             | The operation mode of the node. Ranges are: <ul style="list-style-type: none"> <li>• Yellow - Starting (0.1 - 0.9)</li> <li>• Green - Normal (1.0 - 1.9)</li> <li>• Blue - Client (2.0 - 2.9)</li> <li>• Yellow - Joining (3.0 - 3.9)</li> <li>• Orange - Leaving (4.0 - 4.9)</li> <li>• Red - Decommissioned (5.0 - 5.9)</li> <li>• Yellow - Moving (6.0 - 6.9)</li> <li>• Orange - Draining (7.0 - 7.9)</li> <li>• Orange - Drained (8.0 - 8.9)</li> <li>• Orange - Relocating (9.0 - 9.9)</li> <li>• Blue - Unknown (10.0)</li> </ul> |
| Total Read Count  | Total number of read requests                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Total Write Count | Total number of write requests                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Avg Read Latency  | Average recent node read round trip times in milliseconds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Avg Write Latency | Average recent node write round trip times in milliseconds                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### **Storage Vol Summary**

This chart allows you to view memory use by the filesystems mounted on a node. The dashboard data is updated every hour.

| Column | Description                         |
|--------|-------------------------------------|
| Target | All mounted filesystems on the node |

|                     |                                        |
|---------------------|----------------------------------------|
| Filesystem Capacity | Total capacity of the filesystem       |
| Filesystem Used     | Total used kilobytes on the filesystem |
| Filesystem Free     | Total free kilobytes on the filesystem |

## Cisco CBQoS Unified Dashboard

The Cisco CBQoS Unified Dashboard provides predefined list views for monitoring information about the CBQoS (Class-Based Quality of Service) policies applied to network interfaces. CBQoS allows specific traffic to be prioritized according to its relative importance and can limit the amount of bandwidth available for certain types of network traffic.

### Contents

#### Required Data Sources in the snmpcollector Probe

The following table contains the monitors that you must activate in the snmpcollector probe to see data in the Cisco CBQoS Unified Dashboard.

| Dashboard Chart                 | QoS                                     | Target/Source |
|---------------------------------|-----------------------------------------|---------------|
| Top CBQoS Class Map Pre-vs-Post | QOS_CBQOSCLASSMAP_PREPOLICYUTILIZATION  | *             |
| Top CBQoS Class Map Pre-vs-Post | QOS_CBQOSCLASSMAP_POSTPOLICYUTILIZATION | *             |
| Top CBQoS Class Map Pre-vs-Post | QOS_CBQOSCLASSMAP_PREPOLICYBITRATE      | *             |
| Top CBQoS Class Map Pre-vs-Post | QOS_CBQOSCLASSMAP_POSTPOLICYBITRATE     | *             |
| Top CBQoS Class Map Pre-vs-Post | QOS_CBQOSCLASSMAP_PREPOLICYPACKETS      | *             |
| Top CBQoS Class Map Pre-vs-Post | QOS_CBQOSCLASSMAP_POSTPOLICYPACKETS     | *             |
| Top CBQoS Class Map Pre-vs-Post | QOS_CBQOSCLASSMAP_DISCARDEDPACKETS      | *             |
| Top CBQoS Police Action         | QOS_CBQOSPOLICER_CONFORMEDBITRATE       | *             |
| Top CBQoS Police Action         | QOS_CBQOSPOLICER_VIOLATEDBITRATE        | *             |
| Top CBQoS Police Action         | QOS_CBQOSPOLICER_CONFORMEDPKTSDROPPED   | *             |
| Top CBQoS Police Action         | QOS_CBQOSPOLICER_EXCEEDEDPKTSDROPPED    | *             |
| Top CBQoS Police Action         | QOS_CBQOSPOLICER_VIOLATEDPKTSDROPPED    | *             |
| Top CBQoS Queuing Statistics    | QOS_CBQOSQUEUEING_CURRENTQUEUE SIZE     | *             |
| Top CBQoS Queuing Statistics    | QOS_CBQOSQUEUEING_PREPOLICYPACKETS      | *             |
| Top CBQoS Queuing Statistics    | QOS_CBQOSQUEUEING_POSTPOLICYPACKETS     | *             |



|                              |                                                    |   |
|------------------------------|----------------------------------------------------|---|
| Top CBQoS Shaping Statistics | QOS_CBQOSTRAFFICSHAPING_SHAPING_QUEUE_SIZE         | * |
| Top CBQoS Shaping Statistics | QOS_CBQOSTRAFFICSHAPING_SHAPING_DELAYED_PACKETS    | * |
| Top CBQoS Shaping Statistics | QOS_CBQOSTRAFFICSHAPING_SHAPING_DROPPED_PACKETS    | * |
| Top CBQoS Shaping Statistics | QOS_CBQOSTRAFFICSHAPING_SHAPING_DELAYED_THROUGHPUT | * |
| Top CBQoS Shaping Statistics | QOS_CBQOSTRAFFICSHAPING_SHAPING_DROPPED_THROUGHPUT | * |
| Top CBQoS RED Statistics     | QOS_CBQOSRED_RED_QUEUE_SIZE                        | * |
| Top CBQoS RED Statistics     | QOS_CBQOSRED_RANDOM_DROP_PACKETS                   | * |
| Top CBQoS RED Statistics     | QOS_CBQOSRED_RANDOM_DROP_THROUGHPUT                | * |
| Top CBQoS RED Statistics     | QOS_CBQOSRED_REDTAIL_DROP_PACKETS                  | * |
| Top CBQoS RED Statistics     | QOS_CBQOSRED_REDTAIL_DROP_THROUGHPUT               | * |
| Top CBQoS RED Statistics     | QOS_CBQOSRED_RED_TRANSMITTED_PACKETS               | * |
| Top CBQoS RED Statistics     | QOS_CBQOSRED_RED_TRANSMITTED_THROUGHPUT            | * |

An asterisk (\*) means that the value for the first entry for the QoS is used.

### Top CBQoS Class Map Pre-vs-Post

This chart displays information about the pre-policy and post-policy network traffic over the last 24 hours. Use this chart to compare information about the enterprise CBQoS policy by interface.

| Column                  | Description                                                                                                                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device                  | The name of the monitored device. Click this link to view additional information in OC.                                                                                                                           |
| Target                  | The name of the device interface. Click this link to view additional information in OC.                                                                                                                           |
| Pre-Policy Utilization  | The pre-policy percent network utilization. <ul style="list-style-type: none"> <li>Green - 0 through 75</li> <li>Yellow - 76 through 85</li> <li>Orange - 86 through 90</li> <li>Red - 91 through 100</li> </ul>  |
| Post-Policy Utilization | The post-policy percent network utilization. <ul style="list-style-type: none"> <li>Green - 0 through 75</li> <li>Yellow - 76 through 85</li> <li>Orange - 86 through 90</li> <li>Red - 91 through 100</li> </ul> |
| Pre-Policy Rate         | The pre-policy number of bits per second.                                                                                                                                                                         |
| Post-Policy Rate        | The post-policy number of bits per second.                                                                                                                                                                        |
| Pre-Policy Packets      | The pre-policy number of packets per second.                                                                                                                                                                      |

|                     |                                                         |
|---------------------|---------------------------------------------------------|
| Post-Policy Packets | The post-policy number of packets per second.           |
| Discarded Packets   | The post-policy number of discarded packets per second. |

### **Top CBQoS Police Action**

This chart displays information about the rate of network traffic marked by CBQoS Police Action policy over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column                    | Description                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------|
| Device                    | The name of the monitored device. Click this link to view additional information in OC. |
| Target                    | The name of the device interface. Click this link to view additional information in OC. |
| Conformed Bit Rate        | The number of bits per second treated as conforming by the policing policy.             |
| Violated Bit Rate         | The number of bits per second treated as violated by the policing policy.               |
| Conformed Packets Dropped | The number of packets per second treated as conforming by the policing policy.          |
| Exceeded Packets Dropped  | The number of packets per second treated as exceeding by the policing policy.           |
| Violated Packets Dropped  | The number of packets per second treated as violated by the policing policy.            |

### **Top CBQoS Queuing Statistics**

This chart displays information about the queue size for the CBQoS Queueing policy over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column              | Description                                                                             |
|---------------------|-----------------------------------------------------------------------------------------|
| Device              | The name of the monitored device. Click this link to view additional information in OC. |
| Target              | The name of the device interface. Click this link to view additional information in OC. |
| Current Queue Size  | The current queue size for the Queueing policy.                                         |
| Max Queue Size      | The maximum queue size.                                                                 |
| Pre-Policy Packets  | The pre-policy number of packets per second.                                            |
| Post-Policy Packets | The post-policy number of packets per second.                                           |

### **Top CBQoS Shaping Statistics**

This chart displays information about about the rate of network traffic for the CBQoS Traffic Shaping policy over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column | Description                                                                             |
|--------|-----------------------------------------------------------------------------------------|
| Device | The name of the monitored device. Click this link to view additional information in OC. |
| Target | The name of the device interface. Click this link to view additional information in OC. |

|                    |                                                                         |
|--------------------|-------------------------------------------------------------------------|
| Current Queue Size | The current queue size for the Traffic Shaping policy.                  |
| Delayed Packets    | The number of packets per second that have been delayed during shaping. |
| Dropped Packets    | The number of packets per second that have been dropped during shaping. |
| Delayed Throughput | The number of bytes per second that are delayed during shaping.         |
| Dropped Throughput | The number of bytes per second that are dropped during shaping.         |

### Top CBQoS RED Statistics

This chart displays information about the rate of network traffic for the CBQoS RED policy over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column                 | Description                                                                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device                 | The name of the monitored device. Click this link to view additional information in OC.                                                                      |
| Target                 | The name of the device interface. Click this link to view additional information in OC.                                                                      |
| RED Queue Size         | The current queue size for the RED policy.                                                                                                                   |
| Dropped Pkts           | The number of packets per second dropped when the number of packets in the queue was greater than the minimum threshold and less than the maximum threshold. |
| Dropped Throughput     | The number of bits per second dropped when the number of packets in the queue was greater than the minimum threshold and less than the maximum threshold.    |
| Tail Drop Pkts         | The number of packets per second dropped when the number of packets in the queue was greater than the maximum threshold.                                     |
| Tail Drop Throughput   | The number of bits per second dropped when the number of packets in the queue was greater than the maximum threshold.                                        |
| Transmitted Pkts       | The number of packets transmitted by the RED queue.                                                                                                          |
| Transmitted Throughput | The number of bits transmitted by the RED queue.                                                                                                             |

## Cisco UCM Unified Dashboard

Cisco CallManager is the software-based call-processing component of the Cisco IP Telephony solution that manages IP telephony devices and call services over the data network. The Cisco CallManager provides many functions, such as managing call setup, controlling devices, and collecting statistics on call quality. It can manage IP phones, media processing devices, voice gateways, and multimedia applications.

The Cisco UCM Unified Dashboard provides predefined list views for monitoring communication, their related resources and gateway utilization.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the Cisco UCM dashboard.

| QoS               | Subkey/Target                                                                                                                                                                                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| QOS_CCM_CALLS     | CallsAttempted<br>CallsCompleted<br>CallsInProgress<br>VideoCallsActive<br>VideoCallsCompleted                                                                                                                                                                                                               |
| QOS_CCM_RESOURCE  | VideoOutOfResources<br>MTPOutOfResources<br>MTPResourceActive<br>MTPResourceTotal<br>HWConferenceResourceActive<br>HWConferenceResourceAvailable<br>HWConferenceResourceTotal<br>T1ChannelsActive<br>PRChannelsActive<br>RegisteredAnalogAccess<br>RegisteredHardwarePhones<br>RegisteredOtherStationDevices |
| QOS_SERVICE_STATE | T1SpansInService<br>PRISpansInService                                                                                                                                                                                                                                                                        |

### Call Metrics

This chart displays information about the Call Metrics and is collected over time to identify the busiest calling hour.

| Column Name            | Description                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------|
| Calls Attempted        | Displays the total number of attempted calls                                                |
| Calls Completed        | Displays the number of calls actually connected                                             |
| Calls in Progress      | Displays the number of voice or video calls in progress                                     |
| Video Calls Active     | Displays the number of active video calls                                                   |
| Video Calls Completed  | Displays the number of video calls actually connected                                       |
| Video Out of Resources | Displays the number of failed attempts to allocate video resources when none were available |

### Gateway Utilization

This chart displays information about the Gateway Utilization of the Communication Manager to understand the call patterns and assess whether installation of additional resources is required.

| Column Name         | Description                                                    |
|---------------------|----------------------------------------------------------------|
| T1 Channels Active  | Displays the number of T1 CAS voice channels in an active call |
| T1 Spans in Service | Displays the number of T1 CAS spans available                  |
| PRI Channels Active | Displays the number of PRI voice channels in an active call    |

|                      |                                            |
|----------------------|--------------------------------------------|
| PRI Spans in Service | Displays the number of PRI spans available |
|----------------------|--------------------------------------------|

### **Phones**

This chart displays information about the registered Phones and other devices in the Call Manager. The registration status is monitored to ensure consistent optimized performance of the devices. This status must be monitored before and after any system upgrade to ensure that the system is completely restored.

| Column Name                      | Description                                                                     |
|----------------------------------|---------------------------------------------------------------------------------|
| Registered Analog Access         | Displays the number of registered Analog Access gateways                        |
| Registered Hardware Phones       | Displays the number of registered hardware IP phones                            |
| Registered Other Station Devices | Displays the number of registered station devices other than hardware IP phones |

### **Resources**

This chart displays information about the MTP and Hardware Resources in the Call Manager. This data is collected over time to help plan for resource growth and provisioning.

| Column Name                             | Description                                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------------------------|
| MTP Out of Resources                    | Displays the number of failed attempts to allocate an MTP resource from the registered devices |
| MTP Active Resource                     | Displays the total number of active MTP resources from the registered devices                  |
| MTP Total Resource                      | Displays the total number of registered MTP resources                                          |
| Hardware Conference Active Resources    | Displays the total number of active hardware conference resources on all registered devices    |
| Hardware Conference Resources Available | Displays the number of available hardware conference resources on all registered devices       |
| Hardware Conference Total Resources     | Displays the total number of registered hardware conference resources                          |

## **Cisco Unified Dashboard**

The Cisco Unified Dashboard provides four predefined list views with performance and status information about Cisco devices in your environment.

### **Contents**

#### **NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### **Cisco Required Data Sources**

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the Cisco dashboard.

| Probe         | QoS Metric              | SubKey/Target                                                                                                                             |
|---------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| cisco_monitor | QOS_CISCO_BUFFER_MISSES | Small Buffer Misses<br>Medium Buffer Misses<br>Big Buffer Misses<br>Large Buffer Misses<br>Very Large Buffer Misses<br>Huge Buffer Misses |
|               | QOS_CISCO_ENVIRONMENT   | Fan State (0)                                                                                                                             |
| cdm           | QOS_CPU_USAGE           | CPU Last 5 sec<br>CPU Last 1 min<br>CPU Last 5 min                                                                                        |
|               | QOS_MEMORY_USAGE        | Memory Used<br>Memory Free                                                                                                                |
|               | QOS_MEMORY_PERC_USAGE   | Memory Percent Free                                                                                                                       |

### **Cisco Device CPU Performance**

| Column     | Description                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------------------|
| Host       | IP address of the Cisco device.                                                                                         |
| Last 5 sec | Overall CPU busy percentage during the last 5-second period.<br>0 to 80 = Green<br>80 to 90 = Orange<br>90 to 100 = Red |
| Last 1 min | Overall CPU busy percentage during the last 1-minute period.<br>0 to 80 = Green<br>80 to 90 = Orange<br>90 to 100 = Red |
| Last 5 min | Overall CPU busy percentage during the last 5-minute period.<br>0 to 80 = Green<br>80 to 90 = Orange<br>90 to 100 = Red |

### **Cisco Device Memory Performance**

| Column | Description                                                        |
|--------|--------------------------------------------------------------------|
| Host   | IP address of the Cisco device.                                    |
| Used   | Number of megabytes of memory used during the last 5 minutes.      |
| Free   | Number of megabytes of memory available during the last 5 minutes. |

|              |                                                                                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------|
| Percent Free | Percent of memory available during the last 5 minutes.<br>20 to 100 = Green<br>10 to 20 = Orange<br>0 to 10 = Red |
|--------------|-------------------------------------------------------------------------------------------------------------------|

### **Cisco Device Buffer Misses**

The processor memory of the Cisco device is divided into pools. Each pool contains a number of memory blocks of equal size. These memory blocks are called buffers.

There are six buffer pools:

- Small - 104-byte buffers
- Medium - 600-byte buffers
- Big - 1524-byte buffers
- Large - 4520-byte buffers
- Very Large - 5024-byte buffers
- Huge - 18024-byte buffers

| Column     | Description                                                                       |
|------------|-----------------------------------------------------------------------------------|
| Host       | IP address of the Cisco device.                                                   |
| Small      | Number of buffer misses for the small buffer pool during the last 5 minutes.      |
| Medium     | Number of buffer misses for the medium buffer pool during the last 5 minutes.     |
| Big        | Number of buffer misses for the big buffer pool during the last 5 minutes.        |
| Large      | Number of buffer misses for the large buffer pool during the last 5 minutes.      |
| Very Large | Number of buffer misses for the very large buffer pool during the last 5 minutes. |
| Huge       | Number of buffer misses for the huge buffer pool during the last 5 minutes.       |

### **Cisco Device Environment Status**

| Column    | Description                                                                                                                                     |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Host      | IP address of the Cisco device.                                                                                                                 |
| Fan State | Status of the device fan during the last 5 minutes. Status is reported as normal, warning, critical, shutdown, not present, or not functioning. |

## **CloudStack Unified Dashboard**

The CloudStack Unified Dashboard provides predefined list views with information about the performance and health of the CloudStack environment. CloudStack refers to Apache CloudStack and Citrix CloudPlatform Powered by Apache CloudStack. The CloudStack Unified Dashboard provides information about performance of hosts, zones, pods, and VM instances, and about the health status of infrastructure components.

## Contents

### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### CloudStack Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated in order to populate data in the CloudStack dashboard.

| Probe                       | QoS                                            | Subkey/Target     |
|-----------------------------|------------------------------------------------|-------------------|
| cloudstack                  | QOS_CLOUDSTACK_HOST_CPU_USED                   | Current CPU Used  |
|                             | QOS_CLOUDSTACK_HOST_MEM_USED                   | Memory Used       |
|                             | QOS_CLOUDSTACK_HOST_MEM_TOTAL                  | *                 |
|                             | QOS_CLOUDSTACK_ZONE_CPU_PCT_USED               | *                 |
|                             | QOS_CLOUDSTACK_ZONE_MEMORY_PCT_USED            | *                 |
|                             | QOS_CLOUDSTACK_ZONE_ALLOCATED_STORAGE_PCT_USED | *                 |
|                             | QOS_CLOUDSTACK_ZONE_DIRECT_IP_PCT_USED         | *                 |
|                             | QOS_CLOUDSTACK_ZONE_PRIVATE_IP_PCT_USED        | *                 |
|                             | QOS_CLOUDSTACK_ZONE_PUBLIC_IP_PCT_USED         | *                 |
|                             | QOS_CLOUDSTACK_POD_CPU_USAGE                   | *                 |
|                             | QOS_CLOUDSTACK_POD_MEMORY_PCT_USED             | *                 |
|                             | QOS_CLOUDSTACK_POD_STORAGE_PCT_USED            | *                 |
|                             | QOS_CLOUDSTACK_POD_PRIVATE_IP_PCT_USED         | *                 |
|                             | QOS_CLOUDSTACK_VM_STATUS                       | VM Status         |
|                             | QOS_CLOUDSTACK_VM_CPU_NUMBER                   | *                 |
|                             | QOS_CLOUDSTACK_VM_CPU_SPEED                    | *                 |
|                             | QOS_CLOUDSTACK_VM_CPU_USED                     | *                 |
|                             | QOS_CLOUDSTACK_VM_MEM_ALLOC                    | Memory            |
|                             | QOS_CLOUDSTACK_VM_NET_READ                     | Network Kbs Read  |
|                             | QOS_CLOUDSTACK_VM_NET_WRITE                    | Network Kbs Write |
| QOS_CLOUDSTACK_SYS_VM_STATE | *                                              |                   |



An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

### **Host Performance**

This view displays information about the performance of CloudStack server hosts.

| <b>Column</b>     | <b>Description</b>                                                                                                                                                                                                                                                                                  |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host              | IP address or host name of system where the Citrix CloudStack server is running.<br>Enter text in the filter field in the column header to see only hosts that contain that text. Click the arrow next to the filter field to toggle between descending and ascending sorting of the column values. |
| CPU Usage         | Percent of CPU used on the host in the last week.<br>0 to 70 = Green<br>71 to 80 = Yellow<br>81 to 90 = Orange<br>91 and above = Red                                                                                                                                                                |
| Memory Used in GB | Number of gigabytes of memory used on the host in the last week.                                                                                                                                                                                                                                    |
| Total Memory      | Number of megabytes of memory on the host in the last week.                                                                                                                                                                                                                                         |

### **Zone Performance**

This view displays information about the performance of CloudStack zones.

| <b>Column</b>          | <b>Description</b>                                                                                                                                                                                                                                      |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zones Performance      | IP address or host name of the zone.<br>Enter text in the filter field in the column header to see only zones that contain that text. Click the arrow next to the filter field to toggle between descending and ascending sorting of the column values. |
| CPU Used               | Percent of allocated CPU in use in the last hour.                                                                                                                                                                                                       |
| Memory Used            | Percent of allocated memory in use in the last hour.                                                                                                                                                                                                    |
| Allocated Storage Used | Percent of the storage allocated to the zone that is in use in the last hour.                                                                                                                                                                           |
| Direct IP Used         | Percent of direct IP addresses used by VM instances in the last hour.                                                                                                                                                                                   |
| Private IP Used        | Percent of management IP addresses used by VM instances in the last hour.                                                                                                                                                                               |
| Public IP Used         | Percent of reserved system IP addresses, for this particular zone, used by VM instances in the last hour.                                                                                                                                               |

## Pod Performance

This view displays information about the performance of CloudStack pods.

| Column           | Description                                                                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host             | IP address or host name of the system where the pod is running. Enter text in the filter field in the column header to see only pods that contain that text. Click the arrow next to the filter field to toggle between descending and ascending sorting of the column values. |
| Pod CPU Usage    | Percent of host CPU in use by the pod in the last three weeks.<br>0 to 50 = Green<br>51 to 65 = Yellow<br>66 to 80 = Orange<br>81 and above = Red                                                                                                                              |
| Memory Usage     | Percent of host memory in use by the pod in the last three weeks.<br>0 to 60 = Green<br>61 to 75 = Yellow<br>76 to 90 = Orange<br>91 and above = Red                                                                                                                           |
| Storage Usage    | Percent of allocated storage in use by the pod in the last three weeks.<br>0 to 70 = Green<br>71 to 80 = Yellow<br>81 to 90 = Orange<br>91 and above = Red                                                                                                                     |
| Private IP Usage | Percent of management IP addresses used by pod in the last hour.                                                                                                                                                                                                               |

## Instance Performance

This view displays information about the performance of virtual machine (VM) instances in the CloudStack environment.

| Column       | Description                                                                                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VM Instances | IP address or host name of the system where the VM is running. Enter text in the filter field in the column header to see only VMs that contain that text.            |
| Status       | Status of the VM instance. Possible values are:<br>Running<br>Unknown<br>Starting<br>Migrating<br>Stopping<br>Stopped<br>Shut down<br>Destroyed<br>Expunging<br>Error |
| CPU Cores    | Number of CPU cores allocated to the VM.                                                                                                                              |
| CPU Speed    | Speed of the allocated CPU.                                                                                                                                           |

|                   |                                                                                 |
|-------------------|---------------------------------------------------------------------------------|
| CPU Used in Mhz   | Percent of allocated CPU capacity, in megahertz, in use in the last hour.       |
| Memory Allocation | Amount of memory, in megabytes, allocated to the VM.                            |
| Network Reads     | Number of kilobytes per second of data read from the network in the last hour.  |
| Network Writes    | Number of kilobytes per second of data written to the network in the last hour. |

## System Infrastructure Health

This view displays information about the health status of CloudStack infrastructure components.

| Column            | Description                                                                                                                                                                                                                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CloudStack System | IP address of the CloudStack system that runs the Admin REST API.<br>Enter text in the filter field in the column header to see only CloudStack systems that contain that text. Click the arrow next to the filter field to toggle between descending and ascending sorting of the column values. |
| System VM         | IP addresses of the system VMs that CloudStack manages to perform tasks in the cloud.<br>Enter text in the filter field in the column header to see only system VMs that contain that text.                                                                                                       |
| State             | Status of the CloudStack system.<br>Possible states are:<br>Up<br>Connecting<br>Disconnected<br>Creating<br>Rebalancing<br>Removed<br>Down<br>Alert<br>Error                                                                                                                                      |

## Datacenter Unified Dashboard

The Datacenter Unified Dashboard provides predefined list views with key performance indicators for your data center infrastructure such as server health, disk space, network response, and web sites.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### Datacenter Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the Datacenter dashboard.

| Probe        | QoS                   | Subkey/Target |
|--------------|-----------------------|---------------|
| cdm          | QOS_CPU_USAGE         | \$HOST        |
|              | QOS_MEMORY_PERC_USAGE | \$HOST        |
| net_connect  | QOS_NET_CONNECT       | *             |
| url_response | QOS_URL_RESPONSE      | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

For more information on configuring probes, see the documentation for each probe.

### Current Server Performance

| Column       | Description                                                                                                     |
|--------------|-----------------------------------------------------------------------------------------------------------------|
| Host         | Name of the host.                                                                                               |
| CPU Usage    | Percent of CPU in use.<br>0 to 94.99 = Green<br>95 to 96.99 = Yellow<br>97 to 98.99 = Orange<br>99 to 100 = Red |
| Memory Usage | Percent of memory in use.<br>0 to 69.99 = Green<br>70 to 89.99 = Orange<br>90 to 100 = Red                      |
| Alarm        | Lists the alarms for the host.                                                                                  |

### Server Disk Space Usage

| Column       | Description                                                                             |
|--------------|-----------------------------------------------------------------------------------------|
| Host         | Name of the host.                                                                       |
| Disk         | Name of the disk.                                                                       |
| Percent Used | Highest percentage of disk space usage for hosts in the group for the last ten minutes. |

### Network Response Time

| Column         | Description                                                       |
|----------------|-------------------------------------------------------------------|
| Monitored From | Name of host where UIM is installed and monitoring response time. |
| Host:Port      | Name and port type of the target host.                            |

|           |                                                                                                 |
|-----------|-------------------------------------------------------------------------------------------------|
| Resp Time | Time, in milliseconds, for a response to be received from the target host.                      |
| Resp Time | Gauge displaying the time, in milliseconds, for a response to be received from the target host. |

**URL Response Time (List)**

| Column         | Description                                                                                    |
|----------------|------------------------------------------------------------------------------------------------|
| Monitored From | Name of host where UIM is installed and monitoring response time.                              |
| Monitored Site | The web site being monitored.                                                                  |
| Resp Time      | Time, in milliseconds, for a response to be received from the target URL.                      |
| Resp Time      | Gauge displaying the time, in milliseconds, for a response to be received from the target URL. |
| Alarm          | Indicates whether there is an alarm generated by the probe.                                    |

**DB2 Unified Dashboard**

**Contents**

**DB\_Status**

| QoS Required              | Subkey/Target |
|---------------------------|---------------|
| QOS_DB2_CHECK_DBALIVE     | *             |
| QOS_DB2_DB_STATUS         | *             |
| QOS_DB2_CONNECTIONS_TOP   | *             |
| QOS_DB2_COORD_AGENTS_TOP  | *             |
| QOS_DB2_CAT_CACHE_LOOKUPS | *             |
| QOS_DB2_APPLS_CUR_CONS    | *             |

| Column | Description                                         |
|--------|-----------------------------------------------------|
| Host   | Name of the host where the DB2 server is installed. |

**Internals**

| QoS Required                   | Subkey/Target |
|--------------------------------|---------------|
| QOS_DB2_INT_ROLLBACKS          | *             |
| QOS_DB2_INT_COMMITS            | *             |
| QOS_DB2_INT_DEADLOCK_ROLLBACKS | *             |

|                          |   |
|--------------------------|---|
| QOS_DB2_INT_AUTO_REBINDS | * |
|--------------------------|---|

| Column | Description                                         |
|--------|-----------------------------------------------------|
| Host   | Name of the host where the DB2 server is installed. |

### Locks

| QoS Required             | Subkey/Target |
|--------------------------|---------------|
| QOS_DB2_LOCK_LIST_IN_USE | *             |
| QOS_DB2_LOCK_WAIT_TIME   | *             |
| QOS_DB2_LOCK_WAITS       | *             |
| QOS_DB2_LOCK_TIMEOUTS    | *             |

| Column | Description                                         |
|--------|-----------------------------------------------------|
| Host   | Name of the host where the DB2 server is installed. |

### Logs

| QoS Required            | Subkey/Target |
|-------------------------|---------------|
| QOS_DB2_DB_LOG_UTIL_RTO | *             |
| QOS_DB2_LOG_WRITES      | *             |
| QOS_DB2_LOG_READS       | *             |

| Column | Description                                         |
|--------|-----------------------------------------------------|
| Host   | Name of the host where the DB2 server is installed. |

### Misc

| QoS Required                    | Subkey/Target |
|---------------------------------|---------------|
| QOS_DB2_SORT_HEAP_ALLOCATED     | *             |
| OS_DB2_DB_HEAP_TOP              | *             |
| QOS_DB2_AGENTS_WAITING_ON_TOKEN | *             |
| QOS_DB2_PCT_SORT_OVERFLOW       | *             |

| Column | Description                                         |
|--------|-----------------------------------------------------|
| Host   | Name of the host where the DB2 server is installed. |

## Docker Unified Dashboard

The Docker Unified Dashboard provides predefined list views for monitoring the status of Docker virtualization environment resources (hosts and containers).

### Contents

#### Required Data Sources in the docker\_monitor Probe

The following table contains the monitors that you must activate in the docker\_monitor probe to see data in the Docker Unified Dashboard.

| Dashboard Chart  | QoS                                               | Target/Source |
|------------------|---------------------------------------------------|---------------|
| Docker Engines   | QOS_DOCKER_TOTALS_PERCENT_CPU_PCT                 | \$HOST        |
| Docker Engines   | QOS_DOCKER_TOTALS_IO_SERVICE_RECURSIVE_TOTAL_RATE | \$HOST        |
| Docker Engines   | QOS_DOCKER_TOTALS_RX_RATE_TOTAL_DOCKER            | \$HOST        |
| Docker Engines   | QOS_DOCKER_TOTALS_USAGE_TOTAL_KB                  | \$HOST        |
| Docker Engines   | QOS_DOCKER_TOTALS_PERCENT_USAGE_PCT               | \$HOST        |
| Containers       | QOS_DOCKER_CONTAINER_STATUS                       | *             |
| Containers       | QOS_DOCKER_CPU_PERCENT_CPU_PCT                    | *             |
| Containers       | QOS_DOCKER_DISK_IO_SERVICE_RECURSIVE_TOTAL_RATE   | *             |
| Containers       | QOS_DOCKER_NETWORK_RX_RATE                        | *             |
| Containers       | QOS_DOCKER_MEMORY_USAGE_KB                        | *             |
| Containers       | QOS_DOCKER_MEMORY_USAGE_PERCENT                   | *             |
| Container Estate | QOS_DOCKER_TOTALS_NUM_IMAGES_COUNT                | *             |
| Container Estate | QOS_DOCKER_TOTALS_NUM_CONTAINERS_COUNT            | *             |
| Container Estate | QOS_DOCKER_TOTALS_NUM_ACTIVE_CONTAINERS_COUNT     | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used.

## Docker Engines

This chart displays information about the CPU, network, and memory utilization of Docker hosts. Use this chart to view information about the lowest performing host resources.

| Column               | Description                                                                                                                                                                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                 | The name of a Docker container host resource. Click this link to view additional information in OC.                                                                                                                                                                            |
| CPU Usage [Day]      | This chart shows the percent CPU usage by the host over the past 24 hours. This value is a summary of all the containers on the host. <ul style="list-style-type: none"> <li>Green - 0 through 80</li> <li>Yellow - 80.1 through 90</li> <li>Red - 90.1 through 100</li> </ul> |
| CPU Usage            | The current percent CPU usage for the host. This value is a summary of all the containers on the host.                                                                                                                                                                         |
| Disk I/O Rate [Day]  | This chart shows the rate of kilobytes transferred to or from a block of IO devices by the host over the past 24 hours. This value is a summary of all the containers on the host.                                                                                             |
| Latest Disk I/O Rate | The current rate of kilobytes transferred to or from a block of IO devices by the host. This value is a summary of all the containers on the host.                                                                                                                             |
| Network Receive Rate | The current rate of packets being received by the host. This value is a summary of all the containers on the host.                                                                                                                                                             |
| Memory Usage         | The current memory use by the host. This value is a summary of all the containers on the host.                                                                                                                                                                                 |
| Memory Usage Percent | The percent memory usage by the containers on the host.                                                                                                                                                                                                                        |

## Containers

This chart displays information about the CPU, network, and memory utilization of Docker containers. Use this chart to view information about the lowest performing container resources.

| Column              | Description                                                                                                                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Container           | The name of a Docker container. The name of each container follows the naming convention <i>container name:image name</i> . Click this link to view additional information in OC.                                         |
| Status              | The status of the container. <ul style="list-style-type: none"> <li>Green - Running</li> <li>Orange - Restarting</li> <li>Yellow - Paused</li> <li>Blue - Created</li> <li>Red - Exited</li> <li>Red - Unknown</li> </ul> |
| CPU Usage [Day]     | This chart shows the percent CPU usage for the container over the past 24 hours.                                                                                                                                          |
| CPU Usage           | The current percent CPU usage for the container.                                                                                                                                                                          |
| Disk I/O Rate [Day] | This chart shows the rate of kilobytes transferred to or from a block of IO devices by the container over the past 24 hours.                                                                                              |



|                      |                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------|
| Latest Disk I/O Rate | The current rate of kilobytes transferred to or from a block of IO devices by the container.           |
| Network Receive Rate | The rate of packets being received by the container.                                                   |
| Memory Usage         | The memory usage by the container.                                                                     |
| Memory Usage Percent | The percent memory usage by the container.                                                             |
| Host                 | The name of the host resource for the container. Click this link to view additional information in OC. |

### Container Estate

This chart displays information about the general state of the Docker container environment. Use this chart to view information about the availability of docker containers and images.

| Column            | Description                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------|
| Host              | The name of a Docker container host resource. Click this link to view additional information in OC.                       |
| Images            | This gauge shows the number of images on the host. This value is a summary of all the containers on the host.             |
| Containers        | This gauge shows the number of containers on the host. This value is a summary of all the containers on the host.         |
| Active Containers | This gauge shows the number of running containers on the host. This value is a summary of all the containers on the host. |

## EMC Celerra Unified Dashboard

The EMC Celerra Unified Dashboard provides predefined list views with information about the status and capacity of the EMC Celerra storage system.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### EMC Celerra Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the EMC Celerra dashboard.

| Probe   | QoS                                   | Subkey/Target |
|---------|---------------------------------------|---------------|
| celerra | QOS_STORAGE_RAW_TOTAL_CAPACITY        | *             |
|         | QOS_STORAGE_RAW_FREE_CAPACITY_PERCENT | *             |
|         | QOS_STORAGE_NUM_OF_DISKS              | *             |
|         | QOS_STORAGE_NUM_OF_DEVICES            | *             |
|         | QOS_DMFS_TOTAL_CAPACITY               | *             |
|         | QOS_DMFS_USED_CAPACITY                | *             |

|                                |   |
|--------------------------------|---|
| QOS_DMFS_CAPACITY_FREE_PERCENT | * |
| QOS_SVG_SIZE_TOTAL             | * |
| QOS_SVM_SIZE_TOTAL             | * |
| QOS_DMSS_MEMORY_FREE           | * |
| QOS_DMSS_IDLE_CPU_PERCENT      | * |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

### **Datamovers Capacity Usage**

| Column                   | Description                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Data Movers File Systems | Name of the data mover. Enter text in the filter field in the column header to see only data mover names that contain that text. |
| Total Capacity in KBytes | Number of kilobytes in the data mover.                                                                                           |
| Used Capacity in KBytes  | Number of kilobytes used.                                                                                                        |
| Capacity Free in percent | Percent of capacity not used.<br>75 to 100 = Green<br>50 to 76 = Yellow<br>11 to 49 = Orange<br>1 to 10 = Red                    |

### **Storage Groups and Volumes**

| Column                 | Description                                                                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Celerra Systems        | Name of the system that hosts the Celerra server. Enter text in the filter field in the column header to see only Celerra system names that contain that text. |
| Celerra System Details | Name of the storage volume. Enter text in the filter field in the column header to see only storage volumes that contain that text.                            |
| Storage Group Size     | Size of the storage group.                                                                                                                                     |
| Meta Volume Size       | Size of the meta volume.                                                                                                                                       |

### **Memory and CPU Performance**

| Column                | Description                                                                                                                                                                                                                                        |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Celerra Systems       | Name of the system that hosts the Celerra server. Click the name of a host to view a Performance Report with memory and CPU data for that host. Enter text in the filter field in the column header to see only host names that contain that text. |
| Memory Free in KBytes | Number of kilobytes free on the host system.                                                                                                                                                                                                       |
| CPU Free in percent   | Percent of CPU not used.<br>50 to 100 = Green<br>25 to 50 = Yellow<br>10 to 25 = Orange<br>1 to 10 = Red                                                                                                                                           |

## Storage Summary

| Column          | Description                                                                                                                                                                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Celerra Systems | Name of the system that hosts the Celerra server. Click the name of a host to view a Performance Report with performance data for that host. Enter text in the filter field in the column header to see only Celerra system names that contain that text. |
| Total Capacity  | Number of gigabytes in the Celerra system.                                                                                                                                                                                                                |
| Free Capacity   | Percent of capacity not used.<br>50 to 100 = Green<br>25 to 50 = Yellow<br>10 to 25 = Orange<br>0 to 10 = Red                                                                                                                                             |
| Total Disks     | Number of disks.                                                                                                                                                                                                                                          |
| Total Devices   | Number of LUNs.                                                                                                                                                                                                                                           |

## EMC Clariion Unified Dashboard

The EMC Clariion Unified Dashboard provides predefined list views with information about the status and capacity of the EMC Clariion storage system.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### EMC Clariion Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the EMC Clariion dashboard.

| Probe    | QoS                                      | Subkey/Target |
|----------|------------------------------------------|---------------|
| clariion | QOS_STORAGE_RAW_TOTAL_CAPACITY           | *             |
|          | QOS_STORAGE_SYS_FAULTS                   | *             |
|          | QOS_STORAGE_TP_AVAILABLE_CAPACITY        | *             |
|          | QOS_STORAGE_TP_CONSUMED_CAPACITY         | *             |
|          | QOS_STORAGE_TP_PERCENT_FULL              | *             |
|          | QOS_STORAGE_TP_PERCENT_SUBSCRIBED        | *             |
|          | QOS_STORAGE_SP_BLOCKS_READ_PER_SECOND    | SP A<br>SP B  |
|          | QOS_STORAGE_SP_BLOCKS_WRITTEN_PER_SECOND | SP A<br>SP B  |

|                                      |              |
|--------------------------------------|--------------|
| QOS_STORAGE_SP_READ_IOPS             | SP A<br>SP B |
| QOS_STORAGE_SP_WRITE_IOPS            | SP A<br>SP B |
| QOS_STORAGE_SP_PCT_BUSY              | *            |
| QOS_STORAGE_SP_PCT_DIRTY             | SP A<br>SP B |
| QOS_STORAGE_FAST_CACHE_PCT_DIRTY_SPA | Fast Cache   |
| QOS_STORAGE_FAST_CACHE_PCT_DIRTY_SPB | Fast Cache   |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

### **Storage IO Performance**

| <b>Column</b>             | <b>Description</b>                                                                                                                                                                                                                                                      |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clariion Systems          | Name of the system that hosts the Clariion server. Click the name of a Clariion System to view a Performance Report with storage IO data for that system. Enter text in the filter field in the column header to see only Clariion System names that contain that text. |
| SP A - Blocks Read/Sec    | Number of blocks per second read by storage processor A.                                                                                                                                                                                                                |
| SP B - Blocks Read/Sec    | Number of blocks per second read by storage processor B.                                                                                                                                                                                                                |
| SP A - Blocks Written/Sec | Number of blocks per second written by storage processor A.                                                                                                                                                                                                             |
| SP B - Blocks Written/Sec | Number of blocks per second written by storage processor B.                                                                                                                                                                                                             |
| SP A - Read IOPS          | Number of read operations per second by storage processor A.                                                                                                                                                                                                            |
| SP B - Read IOPS          | Number of read operations per second by storage processor B.                                                                                                                                                                                                            |
| SP A - Write IOPS         | Number of write operations per second by storage processor A.                                                                                                                                                                                                           |
| SP B - Write IOPS         | Number of write operations per second by storage processor B.                                                                                                                                                                                                           |

### **Storage Processors Performance**

| <b>Column</b>               | <b>Description</b>                                                                                                                                                                                                                                                      |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clariion Systems            | Name of the system that hosts the Clariion server. Click the name of a Clariion System to view a Performance Report with storage IO data for that system. Enter text in the filter field in the column header to see only Clariion System names that contain that text. |
| SP A - Pct Busy             | Percent of time storage processor A is busy.                                                                                                                                                                                                                            |
| SP B - Pct Busy             | Percent of time storage processor B is busy.                                                                                                                                                                                                                            |
| SP A - Pct Dirty            | For storage processor A, percent of data that is in DRAM cache and has not been written to disk.                                                                                                                                                                        |
| SP B - Pct Dirty            | For storage processor B, percent of data that is in DRAM cache and has not been written to disk.                                                                                                                                                                        |
| SP A - Fast Cache Pct Dirty | For storage processor A, percent of data that is in FLASH cache and has not been written to disk.                                                                                                                                                                       |

|                             |                                                                                                   |
|-----------------------------|---------------------------------------------------------------------------------------------------|
| SP B - Fast Cache Pct Dirty | For storage processor B, percent of data that is in FLASH cache and has not been written to disk. |
|-----------------------------|---------------------------------------------------------------------------------------------------|

### **Storage System Health**

| Column           | Description                                                                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clariion Systems | Name of the system that hosts the Clariion server. Click the name of a Clariion System to view a Performance Report with storage IO data for that system. Enter text in the filter field in the column header to see only Clariion System names that contain that text. |
| Total Capacity   | Number of gigabytes in the Clariion storage system.                                                                                                                                                                                                                     |
| System Health    | Number of faults for the storage system.<br>0 = OK (Green)<br>1 or more = Failed (Red)                                                                                                                                                                                  |

### **Thin Pools Usage**

| Column             | Description                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Storage Thin Pools | Name of the thin pool. Enter text in the filter field in the column header to see only thin pool names that contain that text.      |
| Total Capacity     | Number of gigabytes available in the thin pool.                                                                                     |
| Consumed Capacity  | Number of gigabytes of the thin pool used.                                                                                          |
| Percent Full       | Percent of thin pool capacity consumed.<br>0 to 75 = Green<br>75 to 85 = Yellow<br>85 to 95 = Orange<br>95 to 100 = Red             |
| Percent Subscribed | Percent of thin pool capacity subscribed.<br>0 to 90 = Green<br>90 to 120 = Yellow<br>121 to 200 = Orange<br>Greater than 200 = Red |

## **EMC VMAX Unified Dashboard**

The EMC VMAX Unified Dashboard provides predefined list views with information about the status and capacity of the EMC VMAX storage system.

### **Contents**

#### **NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

## EMC VMAX Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the EMC VMAX dashboard.

| Probe                        | QoS                                             | Subkey/Target |
|------------------------------|-------------------------------------------------|---------------|
| vmax                         | QOS_STORAGE_SYMM_WRITE_PER_SEC                  | *             |
|                              | QOS_STORAGE_SYMM_READ_PER_SEC                   | *             |
|                              | QOS_STORAGE_SYMM_DIR_I_O_PER_SEC                | *             |
|                              | QOS_STORAGE_SYMM_WRITE_HIT_RATIO                | *             |
|                              | QOS_STORAGE_SYMM_READ_HIT_RATIO                 | *             |
|                              | QOS_STORAGE_SYMM_DISK_KB_READ_PER_SEC           | *             |
|                              | QOS_STORAGE_SYMM_DISK_KB_WRITE_PER_SEC          | *             |
|                              | QOS_STORAGE_SYMM_KB_READ_PER_SEC                | *             |
|                              | QOS_STORAGE_SYMM_KB_WRITE_PER_SEC               | *             |
|                              | QOS_STORAGE_SYMM_CACHE                          | *             |
|                              | QOS_STORAGE_SYMM_DIR_READ_WRITE_CACHE_HIT_RATIO | *             |
|                              | QOS_STORAGE_RAW_FREE_CAPACITY_PERCENT           | *             |
|                              | QOS_STORAGE_SYMM_PERCENT_SUBSCRIBED             | *             |
|                              | QOS_STORAGE_DIR_OP_STATUS                       | *             |
| QOS_STORAGE_DIR_READ_PER_SEC | *                                               |               |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

## System IO Performance

| Column          | Description                                                                                                                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host            | Name of the system that hosts the VMAX server. Click the name of a host to view a Performance Report with IO performance data for that host. Enter text in the filter field in the column header to see only host names that contain that text. |
| Write/Sec       | Number of write requests per second for the array.                                                                                                                                                                                              |
| Read/Sec        | Number of read requests per second for the array.                                                                                                                                                                                               |
| Dir I/O per Sec | Number of IO requests per second for all directors.                                                                                                                                                                                             |

|                 |                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Write Hit ratio | Aggregated ratio of write requests for the array found in cache, as opposed to disk. The higher this number, the better the performance. |
| Read Hit Ratio  | Aggregated ratio of read requests for the array found in cache, as opposed to disk. The higher this number, the better the performance.  |

### System Health

| Column                 | Description                                                                                                                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                   | Name of the system that hosts the VMAX server. Click the name of a host to view a Performance Report with data for that host. Enter text in the filter field in the column header to see only host names that contain that text.  |
| Cache Size             | Total cache size.                                                                                                                                                                                                                 |
| Cache Hit Ratio        | Aggregated ratio of read and write requests for the array found in cache, as opposed to disk. The higher this number, the better the performance.<br>70 to 100 = Green<br>20 to 70 = Yellow<br>10 to 20 = Orange<br>0 to 10 = Red |
| Raw Disk Free Capacity | Total capacity of all disks.<br>50 to 100 = Green<br>30 to 50 = Yellow<br>5 to 30 = Orange<br>0 to 5 = Red                                                                                                                        |
| Device Pool Subscribed | Percent of total disk capacity that is subscribed.<br>0 to 50 = Green<br>50.01 to 75 = Yellow<br>75.01 to 90 = Orange<br>Greater than 90 = Red                                                                                    |

### System Data Throughput

| Column              | Description                                                                                                                                                                                                                                 |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                | Name of the system that hosts the VMAX server. Click the name of a host to view a Performance Report with throughput data for that host. Enter text in the filter field in the column header to see only host names that contain that text. |
| Disk KB Read/Sec    | Read rate for all disks in kilobytes per second.                                                                                                                                                                                            |
| Disk KB Write/Sec   | Write rate for all disks in kilobytes per second.                                                                                                                                                                                           |
| Device KB Read/Sec  | Read rate for all logical devices in kilobytes per second.                                                                                                                                                                                  |
| Device KB Write/Sec | Write rate for all logical devices in kilobytes per second.                                                                                                                                                                                 |

### Front-End Directors Status

| Column              | Description           |
|---------------------|-----------------------|
| Front-End Directors | Name of the director. |

|                 |                                                          |
|-----------------|----------------------------------------------------------|
| Op Status       | Status of the director.<br>Online = Green<br>Other = Red |
| Read IO per sec | Read rate per second for the director.                   |

The EMC VMAX Unified Dashboard provides predefined list views with information about the status and capacity of the EMC VMAX storage system.

## EMC VPLEX Unified Dashboard

The vplex Unified Dashboard provides predefined list views for monitoring the health and performance of VPLEX system objects including Directors, Storage volumes, and Virtual Volumes.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### VPLEX Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the vplex dashboard. An asterisk (\*) means that this QoS brings data for all targets for which it is applicable.

| QoS                                      | Subkey/Target |
|------------------------------------------|---------------|
| QOS_DIRECTOR_OPERATIONAL_STATUS          | *             |
| QOS_DIRECTOR_CPU_UTILIZATION             | *             |
| QOS_DIRECTOR_MEMORY_HEAP_USAGE           | *             |
| QOS_DIRECTOR_FRONT_END_READ_THROUGHPUT   | *             |
| QOS_DIRECTOR_FRONT_END_WRITE_THROUGHPUT  | *             |
| QOS_DIRECTOR_FRONT_END_READ_LATENCY      | *             |
| QOS_DIRECTOR_FRONT_END_WRITE_LATENCY     | *             |
| QOS_DIRECTOR_FRONT_END_OPERATIONS        | *             |
| QOS_DIRECTOR_BACK_END_READ_THROUGHPUT    | *             |
| QOS_DIRECTOR_BACK_END_WRITE_THROUGHPUT   | *             |
| QOS_DIRECTOR_BACK_END_READ_LATENCY       | *             |
| QOS_DIRECTOR_BACK_END_WRITE_LATENCY      | *             |
| QOS_DIRECTOR_BACK_END_OPERATIONS         | *             |
| QOS_DIRECTOR_BACK_END_READ_IOPS          | *             |
| QOS_DIRECTOR_BACK_END_WRITE_IOPS         | *             |
| QOS_DIRECTOR_BACK_END_TIMEOUTS           | *             |
| QOS_DIRECTOR_STORAGE_VOLUME_READ_LATENCY | *             |



| QoS                                       | Subkey/Target |
|-------------------------------------------|---------------|
| QOS_DIRECTOR_STORAGE_VOLUME_WRITE_LATENCY | *             |
| QOS_DIRECTOR_VIRTUAL_VOLUME_READ_LATENCY  | *             |
| QOS_DIRECTOR_VIRTUAL_VOLUME_WRITE_LATENCY | *             |
| QOS_DIRECTOR_VIRTUAL_VOLUME_IOPS          | *             |
| QOS_DIRECTOR_FRONT_END_READ_IOPS          | *             |
| QOS_DIRECTOR_FRONT_END_WRITE_IOPS         | *             |

For more information on configuring probes, see the documentation for each probe at the [CA Unified Infrastructure Management Probes Library](#).

### **Director Status Summary**

This table displays information about all VPLEX system directors that are being monitored.

| Column Name        | Description                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------|
| Operational Status | The functional state of the director in the cluster. Possible values are (Ok, Stopping, Starting, Stopped, Unknown). |

### **Director CPU Utilization**

This table displays information about the total CPU utilization load on the director CPUs of the VPLEX system.

| Column Name     | Description                                                    |
|-----------------|----------------------------------------------------------------|
| CPU Utilization | The utilization load on the director CPUs of the VPLEX system. |

### **Director Memory Utilization**

This table displays information about Heap Memory and usage on a director.

| Column Name | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Heap Usage  | The percentage of heap memory used by the firmware on a director. |

### **Storage Volume Summary**

This table displays information about Storage Volumes performance and usage.

| Column Name   | Description                                                            |
|---------------|------------------------------------------------------------------------|
| Read Latency  | The latency or response time of read operations for a storage volume.  |
| Write Latency | The latency or response time of write operations for a storage volume. |

**Virtual Volume Summary**

This table displays information about Virtual Volumes performance and usage.

| Column Name         | Description                                                            |
|---------------------|------------------------------------------------------------------------|
| Read Latency        | The latency or response time of read operations for a virtual volume.  |
| Write Latency       | The latency or response time of write operations for a virtual volume. |
| Virtual Volume IOPS | The total throughput or IOPS for a virtual volume.                     |

**Director Front End Operations Summary**

This table displays information about front-end host IOPS for the VPLEX system.

| Column Name      | Description                                                                        |
|------------------|------------------------------------------------------------------------------------|
| Read IOPS        | The front-end read I/Os per second over time for the director on the VPLEX system. |
| Write IOPS       | The front-end read I/Os per second over time for the director on the VPLEX system. |
| Read Throughput  | The total front-end throughput in reads.                                           |
| Write Throughput | The total front-end throughput in writes.                                          |
| Read Latency     | The front-end I/O latency statistics pertaining to reads only.                     |
| Write Latency    | The front-end I/O latency statistics pertaining to writes only                     |

**Director Back End Operations Summary**

This table displays information about back-end storage IOPS for the VPLEX system.

| Column Name      | Description                                                                        |
|------------------|------------------------------------------------------------------------------------|
| Read IOPS        | The back-end read I/Os per second over time for the director on the VPLEX system.  |
| Write IOPS       | The back-end write I/Os per second over time for the director on the VPLEX system. |
| Read Latency     | The back-end I/O latency statistics pertaining to reads only.                      |
| Write Latency    | The back-end I/O latency statistics pertaining to writes only.                     |
| Read Throughput  | The total back-end throughput in reads.                                            |
| Write Throughput | The total back-end throughput in writes.                                           |
| Timeouts         | The total back-end timeouts by the director.                                       |

**Hadoop Unified Dashboard**

The Hadoop Unified Dashboard provides predefined list views for monitoring the performance of a Hadoop cluster.

**Contents**

## Required Data Sources

The following table contains the monitors that you must activate to see data in the Hadoop Unified Dashboard.

| Probe  | Dashboard Chart  | QoS                               | Subkey/Target |
|--------|------------------|-----------------------------------|---------------|
| hadoop | Cluster Summary  | QOS_HADOOP_CLUSTER_DECOM_NODES    | *             |
|        |                  | QOS_HADOOP_CLUSTER_LIVE_NODES     | *             |
|        |                  | QOS_HADOOP_CLUSTER_DEAD_NODES     | *             |
|        | HDFS Capacity    | QOS_HADOOP_HDFS_CAPACITY_TOTAL    | *             |
|        |                  | QOS_HADOOP_HDFS_CAPACITYUSED      | *             |
|        |                  | QOS_HADOOP_HDFS_CAPACITYREMAINING | *             |
|        |                  | QOS_HADOOP_HDFS_BLOCKCAPACITY     | *             |
|        |                  | QOS_HADOOP_HDFS_TOTALFILES        | *             |
|        |                  | QOS_HADOOP_HDFS_SNAPSHOTS         | *             |
|        |                  | QOS_HADOOP_HDFS_BLOCKSTOTAL       | *             |
|        | Host Summary     | QOS_HADOOP_SYS_CPU_SYSTEMS        | *             |
|        |                  | QOS_HADOOP_SYS_CPU_USER           | *             |
|        |                  | QOS_HADOOP_SYS_CPU_WAIT           | *             |
|        |                  | QOS_HADOOP_SYS_MEM_USED_PERCENT   | *             |
|        | Role CPU Summary | QOS_HADOOP_PROC_CPU_PERCENT       | *             |
|        |                  | QOS_HADOOP_PROC_CPU_TOTAL         | *             |
|        |                  | QOS_HADOOP_PROC_CPU_USER          | *             |
|        |                  | QOS_HADOOP_PROC_CPU_SYSTEMS       | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used.

## Cluster Summary

This chart displays information about the datanodes in a Hadoop cluster.

| Column | Description                                |
|--------|--------------------------------------------|
| Host   | The name or IP address of the host system. |

|             |                                         |
|-------------|-----------------------------------------|
| Target      | The name of the host system.            |
| Decom Nodes | The number of decommissioned datanodes. |
| Live Nodes  | The number of live datanodes.           |
| Dead Nodes  | The number of dead datanodes.           |

### **HDFS Capacity**

This chart displays information about a Hadoop Distributed File System (HDFS).

| Column             | Description                                            |
|--------------------|--------------------------------------------------------|
| Host               | The name or IP address of the host system.             |
| Capacity Total     | The total amount of HDFS capacity configured.          |
| Capacity Used      | The total amount HDFS capacity in use.                 |
| Capacity Remaining | The total amount of HDFS capacity remaining.           |
| Block Capacity     | The total amount of block capacity configured.         |
| Total Files        | The total number of files and directories in the HDFS. |
| Total Snapshots    | The total number of HDFS snapshots that are taken.     |
| Total Blocks       | The total number of blocks.                            |

### **Host Summary**

This chart displays information about the host systems in a Hadoop cluster.

| Column      | Description                                                                     |
|-------------|---------------------------------------------------------------------------------|
| Host        | The name or IP address of the host system.                                      |
| CPU Kernel  | The percent CPU use by the system level.                                        |
| CPU User    | The percent CPU use by the user level                                           |
| CPU Wait    | The percentage of CPU capacity that was idle due to waiting for an I/O request. |
| Memory Used | The percent total system memory that is in use.                                 |

### **Role CPU Summary**

This chart displays information about CPU use by Hadoop system processes.

| Column      | Description                                |
|-------------|--------------------------------------------|
| Host        | The name or IP address of the host system. |
| Roles       | The name of Hadoop system process.         |
| Usage       | The percent CPU use by the role.           |
| Total Time  | The total process CPU time.                |
| User Time   | The process CPU user time.                 |
| Kernel Time | The process CPU kernel time.               |

## Hitachi Unified Dashboard

The Hitachi Unified Dashboard provides six predefined list views for monitoring Hitachi servers. The views include metrics about performance, disk usage, and component status. When viewing the dashboard, click the name of an item in blue text (Host, Storage Array, Controller, Port, or LUN) to view a Performance Report for that item. Enter text in the filter field in a column header to see only items that contain that text. Click on a column header and then click the triangle icon to toggle between descending and ascending sorting of that column.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### Hitachi Required Data Sources

The table contains the probes and QoS metrics required for the preconfigured Hitachi dashboard.

The OC Dashboards template, found in the hitachi probe configuration UI, includes these QoS measurements and is provided to assist you in configuring the hitachi probe for the dashboard.

| QoS Required                              | Subkey/Target |
|-------------------------------------------|---------------|
| QOS_Storage_SP_Operational_Status         | Host          |
| QOS_Storage_Disk_Operational_Status       | *             |
| QOS_Storage_Disk_Capacity                 | *             |
| QOS_Storage_Disk_Consumable_Capacity      | *             |
| QOS_Storage_Vol_Capacity                  | *             |
| QOS_Storage_Vol_Total_IOS                 | *             |
| QOS_Storage_Vol_Read_IOS                  | *             |
| QOS_Storage_Vol_Write_IOS                 | *             |
| QOS_Storage_Vol_KBYTES_Transfered         | *             |
| QOS_Storage_Vol_Operational_Status        | *             |
| QOS_Storage_Port_Operational_Status       | *             |
| QOS_Storage_Port_Total_IOS                | *             |
| QOS_Storage_Port_KBYTES_Transfered        | *             |
| QOS_Storage_Array_Operational_Status      | Host          |
| QOS_Storage_Array_Total_Managed_Space     | Host          |
| QOS_Storage_Array_Remaining_Managed_Space | Host          |
| QOS_Storage_Array_Total_IOS               | Host          |
| QOS_Storage_Array_KBYTES_Transfered       | Host          |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

### **Hitachi Storage Array Summary**

This chart displays information about the status of the Hitachi storage array.

| <b>Column</b>      | <b>Description</b>                                                                                                                                                                          |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host               | Host name or IP address of the Hitachi storage array.                                                                                                                                       |
| Status             | Status of the storage array:<br>Unknown<br>OK<br>Degraded<br>Stressed<br>Error                                                                                                              |
| Total Capacity     | Total capacity, in gigabytes, of all disks in the array.                                                                                                                                    |
| Remaining Capacity | Number of gigabytes of total capacity not used.                                                                                                                                             |
| Total IOPS         | Number of I/O operations per second for the storage array during the last hour. This performance metric is critical to understanding bottlenecks or throughput in the storage array system. |
| Total KBytes       | Total kilobytes of data transferred during the last hour.                                                                                                                                   |

### **Hitachi Disk Summary**

This chart displays information about disk performance and usage.

| <b>Column</b>      | <b>Description</b>                                        |
|--------------------|-----------------------------------------------------------|
| Host               | Host name or IP address of the Hitachi storage array.     |
| Storage Array      | Name of the storage array.                                |
| Status             | Status of the disk:<br>OK<br>Unknown<br>Degraded<br>Error |
| Available Capacity | Total number of gigabytes available on the disk.          |
| Free Capacity      | Number of gigabytes not used on the disk.                 |

### **Hitachi Controller Summary**

This chart displays information about the status of the controller for the Hitachi storage array.

| <b>Column</b> | <b>Description</b>                                              |
|---------------|-----------------------------------------------------------------|
| Host          | Host name or IP address where the controller is running.        |
| Controller    | Name of the controller.                                         |
| Status        | Status of the controller:<br>OK<br>Unknown<br>Degraded<br>Error |

### **Hitachi Port Summary**

This chart displays information about port usage for the Hitachi storage array.

| <b>Column</b>           | <b>Description</b>                                                         |
|-------------------------|----------------------------------------------------------------------------|
| Port                    | Port used to access the Hitachi storage array.                             |
| Source                  | Name of the array in Hitachi storage system.                               |
| Status                  | Status of the port:<br>OK<br>Unknown<br>Degraded<br>Error                  |
| Total IOPS              | Number of I/O operations per second through the port during the last hour. |
| Total Bytes Transferred | Total number of bytes received through the port during the last hour.      |

### **Hitachi LUN Summary**

This chart displays information about LUN usage and performance.

| <b>Column</b>            | <b>Description</b>                                                              |
|--------------------------|---------------------------------------------------------------------------------|
| LUN                      | The logical unit number (LUN) identifies a logical disk created on a SAN.       |
| Total Capacity           | Total number of gigabytes on the LUN.                                           |
| Total IOPS               | Total number of I/O operations per second for the LUN during the last hour.     |
| Read IOPS                | Number of read operations per second for the LUN during the last hour.          |
| Write IOPS               | Number of write operations per second for the LUN during the last hour.         |
| Total KBytes Transferred | Total number of kilobytes written to or read from the LUN during the last hour. |
| Status                   | Status of the LUN:<br>OK<br>Unknown<br>Degraded<br>Error                        |

## **HP 3Par Unified Dashboard**

The HP 3Par Unified Dashboard provides predefined list views for monitoring the health and performance of HP 3Par storage system objects including Physical Disks, Logical Disks, CPG's, Virtual Volumes, and, Ports.

### **Contents**

#### **NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS

metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**HP 3PAR Required Data Sources**

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the HP 3Par dashboard.

| QoS                             | Subkey/Target |
|---------------------------------|---------------|
| QOS_CONTROLLER_CPU_UTILIZATION  | *             |
| QOS_LOGICAL_DISK_AVAILABILITY   | *             |
| QOS_LOGICAL_DISK_LATENCY        | *             |
| QOS_LOGICAL_DISK_THROUGHPUT     | *             |
| QOS_LOGICAL_DISK_UTILIZATION    | *             |
| QOS_PHYSICAL_DISK_AVAILABILITY  | *             |
| QOS_PHYSICAL_DISK_LATENCY       | *             |
| QOS_PHYSICAL_DISK_THROUGHPUT    | *             |
| QOS_PHYSICAL_DISK_UTILIZATION   | *             |
| QOS_VIRTUAL_VOLUME_AVAILABILITY | *             |
| QOS_VIRTUAL_VOLUME_LATENCY      | *             |
| QOS_VIRTUAL_VOLUME_THROUGHPUT   | *             |
| QOS_VIRTUAL_VOLUME_UTILIZATION  | *             |
| QOS_HP_3PAR_LATENCY             | *             |
| QOS_HP_3PAR_RAW_USED_CAPACITY   | *             |
| QOS_PORT_AVAILABILITY           | *             |

An asterisk (\*) means that this QOS brings data for all targets for which it is applicable.

For more information on configuring probes, see the documentation for each probe. This is available at the [CA Unified Infrastructure Management Probes Library](#).

**Resource Health Summary**

This chart displays information about all HP 3Par StoreServ systems which are being monitored.

| Column Name | Description                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------|
| Latency     | Total Time Required by the StoreServ System to Process a Single Storage Transaction or Data Request. |
| Utilization | Total Used Capacity of all storage objects in the StoreServ System.                                  |

**Controller Node CPU Utilization**

This chart displays information about the total CPU utilization of the Controller Nodes.

| Column Name     | Description                                  |
|-----------------|----------------------------------------------|
| CPU Utilization | Total CPU Utilization of the Controller Node |



**Logical Disk Health Summary**

This chart displays information about Logical Disks performance and usage.

| Column Name       | Description                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------|
| Availability      | Availability of the Logical Disks. [0(normal), 1(preserved), 2(stopping), 3(removing), 4(stopped), 5(orphan)] |
| Latency           | Latency of the Logical Disk in Milliseconds                                                                   |
| Throughput        | Logical Disk Kilobytes Read and Written per Second.                                                           |
| Utilized Capacity | Total Used Capacity of the Logical Disk.                                                                      |

**Physical Disk Health Summary**

This chart displays information about Physical Disks performance and usage.

| Column Name       | Description                                                                                                                                                                                                                                                                                                                   |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Availability      | Availability of the Physical Disks.[Unknown(0), Other(1), OK(2), Degraded(3), Stressed(4), Predictive Failure(5), Error(6), Non-Recoverable Error(7), Starting(8), Stopping(9), Stopped(10), In Service(11), No Contact(12), Lost Communication(13), Aborted(14), Dormant(15), Supporting Entity in Error(16), Completed(17)] |
| Latency           | Latency of the Physical Disk in Milliseconds.                                                                                                                                                                                                                                                                                 |
| Throughput        | Physical Disk Kilobytes Read and Written per Second.                                                                                                                                                                                                                                                                          |
| Utilized Capacity | Total Used Capacity of the Physical Disk.                                                                                                                                                                                                                                                                                     |

**Virtual Volume Health Summary**

This chart displays information about Virtual Volumes performance and usage.

| Column Name  | Description                                                                                                                                                                                                                                                                                                                    |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Availability | Availability of The Virtual Volumes.[Unknown(0), Other(1), OK(2), Degraded(3), Stressed(4), Predictive Failure(5), Error(6), Non-Recoverable Error(7), Starting(8), Stopping(9), Stopped(10), In Service(11), No Contact(12), Lost Communication(13), Aborted(14), Dormant(15), Supporting Entity in Error(16), Completed(17)] |
| Latency      | Latency of the Virtual Volumes in Milliseconds                                                                                                                                                                                                                                                                                 |
| Throughput   | Virtual Volume Kilobytes Read and Written per Second.                                                                                                                                                                                                                                                                          |
| Utilization  | Total Used Capacity of the Virtual Volume.                                                                                                                                                                                                                                                                                     |

### Port Status Summary

This chart displays information about HP 3PAR Ports availability.

| Column Name  | Description                                                                                                                                                                                                                                                                                                                       |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Availability | Availability of StoreServ System Port. [Unknown(0), Other(1), OK(2), Degraded(3), Stressed(4), Predictive Failure(5), Error(6), Non-Recoverable Error(7), Starting(8), Stopping(9), Stopped(10), In Service(11), No Contact(12), Lost Communication(13), Aborted(14), Dormant(15), Supporting Entity in Error(16), Completed(17)] |

## Hyper-V Unified Dashboard

### Contents

#### Hyper-V Required Data Sources

The table contains the the QoS metrics required for the preconfigured Hyper-V dashboard.

| QoS Required         | Subkey/Target                                                                                                |
|----------------------|--------------------------------------------------------------------------------------------------------------|
| QOS_NUMBER_VMS       | Running VMs                                                                                                  |
| QOS_UPTIME           | Host Uptime                                                                                                  |
| QOS_CPU_TIME_PCT     | Average CPU Utilization<br>Average CPU Idle Time<br>CPU Percent Processor Time<br>CPU Percent Interrupt Time |
| QOS_MEMORY_ALLOCATED | Free Physical Memory<br>Physical Memory Allocated<br>Total Visible Memory Size                               |
| QOS_DISK_SECTOR_IO   | Read Bytes Per Second<br>Write Bytes Per Second                                                              |
| QOS_MEMORY_FREE      | Free Physical Memory                                                                                         |
| QOS_NETWORK_KBPS     | Total Receive Throughput<br>Total Send Throughput<br>Bytes Total Per Second                                  |

### Hypervisor Summary

| Column                    | Description                                     |
|---------------------------|-------------------------------------------------|
| Host                      | Name of the host where the Hyperv exists.       |
| Profile                   | Target that is being monitored.                 |
| Running VMs               | Number of running virtual machines.             |
| Host Uptime               | Number of seconds a host remain up and running. |
| Average CPU Utilization   | % of processor time consumed by a hypervisor.   |
| Total Visible Memory Size | Memory size of hypervisor.                      |
| Read Bytes Per Second     | Read Bytes in disk sector per second.           |
| Write Bytes Per Second    | Write Bytes in disk sector per second.          |

**Host Resource CPU**

| Column                     | Description                               |
|----------------------------|-------------------------------------------|
| Host                       | Name of the host where the Hyperv exists. |
| Profile                    | Target that is being monitored.           |
| Average CPU Utilization    | % of processor time consumed of a host.   |
| Average CPU Idle Time      | Average time Host processor remains idle. |
| CPU Percent Processor Time | % of processor time consumed of a host.   |
| CPU Percent Interrupt Time | % of processor time was interrupted.      |

**Host Resource CPU**

| Column                    | Description                           |
|---------------------------|---------------------------------------|
| Host                      | Name of the host where Hyperv exists. |
| Profile                   | Target that is being monitored.       |
| Physical Memory Allocated | Total physical memory of host.        |
| Free Physical Memory      | Free physical memory of host.         |
| Total Visible Memory Size | Total visible memory of host.         |

**Host Network**

| Column                   | Description                                               |
|--------------------------|-----------------------------------------------------------|
| Host                     | Name of the host where the Hyperv exists.                 |
| Profile                  | Target that is being monitored.                           |
| Total Receive Throughput | Number of kilobytes received per second.                  |
| Total Send Throughput    | Number of kilobytes sent per second.                      |
| Bytes Total Per Second   | Number of bytes to transfer on a host network per second. |

**IBM\_SVC Unified Dashboard**

The IBM\_SVC Unified Dashboard provides predefined list views for monitoring the IBM System Storage SAN Volume Controller (SVC). The views include metrics about storage arrays, data transfer rate, and disk performance.

**Contents****NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**IBM\_SVC Required Data Sources**

The table contains the probes and QoS metrics required for the preconfigured IBM-SVC dashboard.

**NOTE**

The OC Dashboards template includes some of the required QoS measurements, but not all. Make sure all the measurements listed here are enabled in the probe.

| Probe   | Chart            | QoS Required                                                                                                                                                                                                                                                                                         |
|---------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IBM_SVC | Clusters         | QOS_STORAGE_CLUSTER_OPERATIONAL_STATUS<br>QOS_STORAGE_CLUSTER_PERCENT_FREE_CAPACITY<br>QOS_STORAGE_CLUSTER_TOTAL_USED_CAPACITY<br>QOS_STORAGE_CLUSTER_TOTAL_CAPACITY<br>QOS_STORAGE_CLUSTER_MDISK_MS<br>QOS_STORAGE_CLUSTER_VDISK_MS<br>QOS_STORAGE_CLUSTER_MDISK_IO<br>QOS_STORAGE_CLUSTER_VDISK_IO |
|         | Nodes Throughput | QOS_STORAGE_NODE_OPERATIONAL_STATUS<br>QOS_STORAGE_NODE_MDISK_R_MB<br>QOS_STORAGE_NODE_MDISK_W_MB<br>QOS_STORAGE_NODE_VDISK_R_MB<br>QOS_STORAGE_NODE_VDISK_W_MB                                                                                                                                      |
|         | Nodes Latency    | QOS_STORAGE_NODE_OPERATIONAL_STATUS<br>QOS_STORAGE_NODE_MDISK_MS<br>QOS_STORAGE_NODE_MDISK_R_MS<br>QOS_STORAGE_NODE_MDISK_W_MS<br>QOS_STORAGE_NODE_VDISK_MS<br>QOS_STORAGE_NODE_VDISK_R_MS<br>QOS_STORAGE_NODE_VDISK_W_MS                                                                            |
|         | MDisk            | QOS_STORAGE_MDISK_OPERATIONAL_STATUS<br>QOS_STORAGE_MDISK_BLOCK_SIZE<br>QOS_STORAGE_MDISK_CONSUMABLE_BLOCKS<br>QOS_STORAGE_MDISK_NUMBER_OF_BLOCKS<br>QOS_STORAGE_MDISK_CAPACITY                                                                                                                      |
|         | VDisk            | QOS_STORAGE_VDISK_OPERATIONAL_STATUS<br>QOS_STORAGE_VDISK_BLOCK_SIZE<br>QOS_STORAGE_VDISK_CONSUMABLE_BLOCKS<br>QOS_STORAGE_VDISK_NUMBER_OF_BLOCKS                                                                                                                                                    |

**IBM\_SVC Clusters**

This chart displays information about the state of IBM-SVC storage clusters.

| Column                | Description                                                                    |
|-----------------------|--------------------------------------------------------------------------------|
| Source                | The IP address of the configured resource.                                     |
| Target                | The name of the monitored target.                                              |
| Status                | Cluster operational status.<br>Green = Ok (2 - 2.99)<br>Red = Error (0 - 1.99) |
| Percent Free Capacity | The % free capacity of the storage cluster.                                    |
| Total Used Capacity   | Total capacity currently used by the storage cluster.                          |
| Total Capacity        | Total capacity of the storage cluster.                                         |
| Average MDisk Latency | Average MDisk latency in milliseconds.                                         |

|                       |                                                                    |
|-----------------------|--------------------------------------------------------------------|
| Average VDisk Latency | Average VDisk latency in milliseconds.                             |
| MDisk Throughput      | Number of MDisk (SAN and RAID) input/output operations per second. |
| VDisk Throughput      | Number of VDisk IOPS input/output operations per second.           |

### **IBM\_SVC Nodes Throughput**

This chart displays information about the data transfer rate of IBM\_SVC storage nodes.

| Column                 | Description                                                                 |
|------------------------|-----------------------------------------------------------------------------|
| Source                 | The IP address of the configured resource.                                  |
| Target                 | The name of the monitored target.                                           |
| Status                 | Node operational status.<br>Green = Ok (2 - 2.99)<br>Red = Error (0 - 1.99) |
| MDisk Read Throughput  | MDisk (SAN and RAID) read throughput in MBps.                               |
| MDisk Write Throughput | MDisk (SAN and RAID) write throughput in MBps.                              |
| VDisk Read Throughput  | VDisk (SAN and RAID) read throughput in MBps.                               |
| VDisk Write Throughput | VDisk (SAN and RAID) write throughput in MBps.                              |

### **IBM\_SVC Nodes Latency**

This chart displays information about the performance of IBM-SVC storage nodes.

| Column                      | Description                                                                 |
|-----------------------------|-----------------------------------------------------------------------------|
| Source                      | The IP address of the configured resource.                                  |
| Target                      | The name of the monitored target.                                           |
| Status                      | Node operational status.<br>Green = Ok (2 - 2.99)<br>Red = Error (0 - 1.99) |
| Average MDisk Latency       | Average MDisk latency in milliseconds.                                      |
| Average MDisk Read Latency  | Average MDisk read latency in milliseconds.                                 |
| Average MDisk Write Latency | Average MDisk write latency in milliseconds.                                |
| Average VDisk Latency       | Average VDisk latency in milliseconds.                                      |
| Average VDisk Read Latency  | Average VDisk read latency in milliseconds.                                 |
| Average VDisk Write Latency | Average VDisk write latency in milliseconds.                                |

### **IBM\_SVC MDisk**

This chart displays information about the state of IBM-SVC MDisk.

| Column | Description                                                                 |
|--------|-----------------------------------------------------------------------------|
| Source | The IP address of the configured resource.                                  |
| Target | The name of the monitored target.                                           |
| Status | MDisk operational status<br>Green = Ok (2 - 2.99)<br>Red = Error (0 - 1.99) |

|                   |                                         |
|-------------------|-----------------------------------------|
| Block Size        | MDisk block size in bytes.              |
| Consumable Blocks | MDisk blocks available for consumption. |
| Number of Blocks  | Total number of MDisk blocks.           |
| Capacity          | MDisk capacity in terabytes.            |

### IBM\_SVC VDisk

This chart displays information about the state of the IBM-SVC VDisk.

| Column            | Description                                                                 |
|-------------------|-----------------------------------------------------------------------------|
| Source            | The IP address of the configured resource.                                  |
| Target            | The name of the monitored target.                                           |
| Status            | VDisk operational status<br>Green = Ok (2 - 2.99)<br>Red = Error (0 - 1.99) |
| Block Size        | VDisk block size in bytes.                                                  |
| Consumable Blocks | VDisk blocks available for consumption.                                     |
| Number of Blocks  | Total number of VDisk blocks.                                               |

## IBM DS4K Unified Dashboard

The IBM DS4K Unified Dashboard provides predefined list views with information about the status and performance of the IBM DS4K disk storage system.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### IBM DS4K Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the IBM DS4K dashboard.

| Probe    | QoS                                      | Subkey/<br>Target |
|----------|------------------------------------------|-------------------|
| ibm ds4k | QOS_STORAGE_COMPONENT_OPERATIONAL_STATUS | *                 |
|          | QOS_STORAGE_SP_OPERATIONAL_STATUS        | *                 |
|          | QOS_STORAGE_ARRAY_TOTAL_MANGED_SPACE     | \$HOST<br>*       |
|          | QOS_STORAGE_DISK_OPERATIONAL_STATUS      | *                 |
|          | QOS_STORAGE_DISK_KBYTES_READ_RATE        | *                 |

|                                               |             |
|-----------------------------------------------|-------------|
| QOS_STORAGE_DISK_KBYTES_WRITT<br>EN_RATE      | *           |
| QOS_STORAGE_VOL_OPERATIONAL_S<br>TATUS        | *           |
| QOS_STORAGE_PORT_OPERATIONAL_<br>STATUS       | *           |
| QOS_STORAGE_ARRAY_OPERATIONAL_<br>_STATUS     | \$HOST      |
| QOS_STORAGE_ARRAY_REMAINING_M<br>ANAGED_SPACE | \$HOST      |
| QOS_STORAGE_POOL_CAPACITY_USE<br>D_PERCENT    | \$HOST<br>* |
| QOS_STORAGE_ARRAY_READ_HIT_RA<br>TIO          | \$HOST      |
| QOS_STORAGE_ARRAY_WRITE_HIT_R<br>ATIO         | \$HOST      |
| QOS_STORAGE_POOL_OPERATIONAL_<br>STATUS       | *           |
| QOS_STORAGE_POOL_TOTAL_MANAG<br>ED_SPACE      | *           |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

### **IBM DS4K Status Definitions**

The IBM DS4K Unified Dashboard displays the status of various components of the disk storage system. This table describes the possible statuses.

| Color  | Status                | Description                                                                                    |
|--------|-----------------------|------------------------------------------------------------------------------------------------|
| Cyan   | Unknown               | Device status could not be determined.                                                         |
| Cyan   | Other                 | Device status could not be determined.                                                         |
| Green  | OK                    | Device is functioning properly.                                                                |
| Yellow | Degraded              | Device is degraded or disabled. This usually means that device performance is not as expected. |
| Orange | Stressed              | Device is experiencing a heavy load.                                                           |
| Red    | Predictive failure    | Device is in a failure mode that can be predicted by its parent.                               |
| Red    | Error                 | Device is in an error state that can be identified by the device or its parent.                |
| Red    | Non-recoverable error | Device or its parent has detected an error that requires replacing the device.                 |
| Blue   | Starting              | Device is starting operation.                                                                  |
| Blue   | Stopping              | Device is shutting down.                                                                       |
| Blue   | Stopped               | Device has shut down.                                                                          |
| Green  | In service            | Device is in operation.                                                                        |

|        |                            |                                                                 |
|--------|----------------------------|-----------------------------------------------------------------|
| Cyan   | No contact                 | Client or parent device cannot contact the device.              |
| Cyan   | Lost communication         | Client or parent device has lost communication with the device. |
| Yellow | Aborted                    | Device has aborted its normal operation.                        |
| Cyan   | Dormant                    | Device is in sleep mode.                                        |
| Red    | Supporting entity in error | Child elements are in an error state.                           |
| Green  | Completed                  | Device has completed operation.                                 |

### **Storage Array Status**

| Column          | Description                                                                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage Array   | Name of the storage array. Enter text in the filter field in the column header to see only storage array names that contain that text. Click the name of an array to view a Performance Report with performance data for that storage array. |
| Status          | Status of the storage array.                                                                                                                                                                                                                 |
| Total Capacity  | Total capacity of all disks in the array.                                                                                                                                                                                                    |
| Free Capacity   | Number of gigabytes of total capacity not used.                                                                                                                                                                                              |
| Free Capacity   | Gauge displaying the percentage of total capacity not used.<br>5 to 100 = Green<br>2 to 4.99 = Orange<br>0 to 1.99 = Red                                                                                                                     |
| Read Hit Ratio  | Aggregated ratio of read requests for the array found in cache, as opposed to disk. The higher this number, the better the performance.<br>90 to 100 = Green<br>50 to 89.99 = Orange<br>0 to 49.99 = Red                                     |
| Write Hit Ratio | Aggregated ratio of write requests for the array found in cache, as opposed to disk. The higher this number, the better the performance.<br>90 to 100 = Green<br>50 to 89.99 = Orange<br>0 to 49.99 = Red                                    |

### **Disks Status**

| Column        | Description                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Storage Array | Name of the storage array. Enter text in the filter field in the column header to see only storage array names that contain that text. |
| Disk          | Name of the disk. Enter text in the filter field in the column header to see only disk names that contain that text.                   |
| Status        | Status of the disk.                                                                                                                    |
| Read Rate     | Rate, in kilobytes per second, at which data is read from disk.                                                                        |



|            |                                                                  |
|------------|------------------------------------------------------------------|
| Write Rate | Rate, in kilobytes per second, at which data is written to disk. |
|------------|------------------------------------------------------------------|

**Storage Pool Status**

| Column         | Description                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Storage Array  | Name of the storage array. Enter text in the filter field in the column header to see only storage array names that contain that text. |
| Storage Pool   | Name of storage pool. Enter text in the filter field in the column header to see only storage pool names that contain that text.       |
| Status         | Status of the storage pool.                                                                                                            |
| Total Capacity | Number of gigabytes in the storage pool.                                                                                               |
| Used Capacity  | Percent of total capacity of the storage pool used:<br>0 to 94.99 = Green<br>95 to 97.99 = Orange<br>98 to 100 = Red                   |

**Component Status**

| Column        | Description                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Storage Array | Name of the storage array. Enter text in the filter field in the column header to see only storage array names that contain that text. |
| Component     | Name of the component. Enter text in the filter field in the column header to see only component names that contain that text.         |
| Status        | Status of the component.                                                                                                               |

**Controller Status**

| Column        | Description                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Storage Array | Name of the storage array. Enter text in the filter field in the column header to see only storage array names that contain that text. |
| Controller    | Name of the controller. Enter text in the filter field in the column header to see only controller names that contain that text.       |
| Status        | Status of the controller.                                                                                                              |

**Port Status**

| Column        | Description                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Storage Array | Name of the storage array. Enter text in the filter field in the column header to see only storage array names that contain that text. |
| Port          | Port number in the controller. Enter a number in the filter field in the column header to see only ports that contain that number.     |
| Status        | Status of the port.                                                                                                                    |

**LUN Status**

| Column        | Description                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage Array | Name of the storage array. Enter text in the filter field in the column header to see only storage array names that contain that text.                                 |
| LUN           | The logical unit number (LUN) identifies a logical disk created on a SAN. Enter text in the filter field in the column header to see only LUNs that contain that text. |
| Status        | Status of the LUN.                                                                                                                                                     |

**IBM DS Next Unified Dashboard**

The `ibm_ds_next` Unified Dashboard provides predefined list views to monitor the health and performance of IBM DS8xxx storage systems.

**NOTE**

If your Unified Dashboard is not populating with data, ensure that all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**Contents****IBM DS Next Required Data Sources**

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the IBM DS Next dashboard. An asterisk (\*) means that this QoS brings data for all targets for which it is applicable.

**NOTE**

For more information on configuring probes, see the documentation for each probe.

| QoS                                    | Subkey/ Target |
|----------------------------------------|----------------|
| QOS_STORAGE_ARRAY_AVAILABLE_CAPACITY   | *              |
| QOS_STORAGE_ARRAY_OPERATIONAL_STATUS   | *              |
| QOS_STORAGE_ARRAY_TOTAL_CAPACITY       | *              |
| QOS_STORAGE_DISK_AVAILABLE_CAPACITY    | *              |
| QOS_STORAGE_DISK_EXTENT_STATUS         | *              |
| QOS_STORAGE_DISK_OPERATIONAL_STATUS    | *              |
| QOS_STORAGE_DISK_TOTAL_CAPACITY        | *              |
| QOS_STORAGE_POOL_AVAILABLE_CAPACITY    | *              |
| QOS_STORAGE_POOL_CAPACITY_USED_PERCENT | *              |
| QOS_STORAGE_POOL_OPERATIONAL_STATUS    | *              |
| QOS_STORAGE_POOL_TOTAL_IOS             | *              |
| QOS_STORAGE_PORT_TOTAL_IOS             | *              |
| QOS_STORAGE_PORT_TOTAL_IOPS_RATE       | *              |
| QOS_STORAGE_PORT_OPERATIONAL_STATUS    | *              |

|                                       |   |
|---------------------------------------|---|
| QOS_STORAGE_RANK_TOTAL_IOS            | * |
| QOS_STORAGE_RANK_READ_RESPONSE_TIME   | * |
| QOS_STORAGE_RANK_WRITE_RESPONSE_TIME  | * |
| QOS_STORAGE_VOL_AVAILABLE_CAPACITY    | * |
| QOS_STORAGE_VOL_DATA_TRANSFERRED_RATE | * |
| QOS_STORAGE_VOL_OPERATIONAL_STATUS    | * |
| QOS_STORAGE_VOL_TOTAL_IOPS_RATE       | * |

### **Arrays Summary**

This table displays information about the capacity and operational status of the monitored array in the storage system.

| Column Name        | Description                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Available Capacity | Available capacity of an array.                                                                                                                                                                                                                                                                                                                                  |
| Operational Status | Operational status of an array. Possible values are: Unknown (0), Other (1), Ok (2), Degraded (3), Stressed (4), Predictive Failure (5), Error (6), Non-Recoverable Error (7), Starting (8), Stopping (9), Stopped (10), In Service (11), No Contact (12), Lost Communication (13), Aborted (14), Dormant (15), Supporting Entity in Error (16), Completed (17). |
| Total Capacity     | Total capacity of an array.                                                                                                                                                                                                                                                                                                                                      |

### **Disks Summary**

This table displays information about the capacity, extent state and operational status of the monitored disk in the storage system.

| Column Name        | Description                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Available Capacity | Available capacity of a disk.                                                                                                                                                                                                                                                                                                                                  |
| Extent State       | Extent status of a disk. Possible values are (Unknown, OK, Warning, Minor failure, Major failure, Critical failure, Non-recoverable error, DMTF Reserved)                                                                                                                                                                                                      |
| Operational Status | Operational status of a disk. Possible values are: Unknown (0), Other (1), Ok (2), Degraded (3), Stressed (4), Predictive Failure (5), Error (6), Non-Recoverable Error (7), Starting (8), Stopping (9), Stopped (10), In Service (11), No Contact (12), Lost Communication (13), Aborted (14), Dormant (15), Supporting Entity in Error (16), Completed (17). |
| Total Capacity     | Total capacity of a disk.                                                                                                                                                                                                                                                                                                                                      |

### **Pools Summary**

This table displays information about the capacity, total IOs, and operational status of the monitored pool in the storage system.

| Column Name           | Description                                |
|-----------------------|--------------------------------------------|
| Available Capacity    | Available capacity of a pool.              |
| Percent Used Capacity | Utilized capacity of a pool in percentage. |

|                    |                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operational Status | Operational status of a pool. Possible values are: Unknown (0), Other (1), Ok (2), Degraded (3), Stressed (4), Predictive Failure (5), Error (6), Non-Recoverable Error (7), Starting (8), Stopping (9), Stopped (10), In Service (11), No Contact (12), Lost Communication (13), Aborted (14), Dormant (15), Supporting Entity in Error (16), Completed (17). |
| Total IOs          | Total number of IOs in a pool.                                                                                                                                                                                                                                                                                                                                 |

### **Ports Summary**

This table displays information about the total IOs, and operational status of the monitored port in the storage system.

| Column Name          | Description                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Total IOs            | Total number of IOs to a port.                                                                                                                                                                                                                                                                                                                                 |
| Total IOs Per Second | Average number of read and write operations per second in a sample period.                                                                                                                                                                                                                                                                                     |
| Operational Status   | Operational status of a port. Possible values are: Unknown (0), Other (1), Ok (2), Degraded (3), Stressed (4), Predictive Failure (5), Error (6), Non-Recoverable Error (7), Starting (8), Stopping (9), Stopped (10), In Service (11), No Contact (12), Lost Communication (13), Aborted (14), Dormant (15), Supporting Entity in Error (16), Completed (17). |

### **Ranks Summary**

This table displays information about the total IOs, read and write response time of the monitored rank in the storage system.

| Column Name         | Description                                           |
|---------------------|-------------------------------------------------------|
| Total IOs           | Total number of IOs in a rank.                        |
| Read Response Time  | Response time of the data read in a sample period.    |
| Write Response Time | Response time of the data written in a sample period. |

### **Volumes Summary**

This table displays information about the capacity, data transferred, total IOs and operational status of the monitored volume in the storage system.

| Column Name           | Description                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Available Capacity    | Available capacity in a volume.                                                                                                                                                                                                                                                                                                                                  |
| Data Transferred Rate | Rate of volume data transferred in a second.                                                                                                                                                                                                                                                                                                                     |
| Operational Status    | Operational status of a volume. Possible values are: Unknown (0), Other (1), Ok (2), Degraded (3), Stressed (4), Predictive Failure (5), Error (6), Non-Recoverable Error (7), Starting (8), Stopping (9), Stopped (10), In Service (11), No Contact (12), Lost Communication (13), Aborted (14), Dormant (15), Supporting Entity in Error (16), Completed (17). |
| Total IOs Per Second  | Average number of read and write operations per second in a sample period.                                                                                                                                                                                                                                                                                       |

## IBMVM Unified Dashboard

The IBMVM Unified Dashboard provides predefined list views for monitoring the IBM virtualization enabled systems (VM). The views include information about storage, CPU, and memory metrics.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### Required Data Sources

The table contains the probes and QoS metrics required for the preconfigured IBMVM dashboard.

#### NOTE

The OC Dashboards template includes some of the required QoS measurements, but not all. Make sure all the measurements listed here are enabled in the probe.

| Probe | Chart                                      | QoS Required                              |
|-------|--------------------------------------------|-------------------------------------------|
| IBMVM | Managed Systems CPU Metrics                | QOS_MS_PROC_UNITS                         |
|       | Managed Systems Disk Bandwidth             | QOS_DISK_BANDWIDTH                        |
|       | Managed Systems Disk Size                  | QOS_DISK_SIZE                             |
|       | Managed Systems Disk Transfer Rate         | QOS_DISK_KBPS                             |
|       | Managed Systems Global Shared Pool Metrics | QOS_CPU_POOL_SIZE<br>QOS_CPU_POOL_UTIL    |
|       | Managed Systems Memory Metrics             | QOS_MS_MEMORY<br>QOS_MS_MEMORY_ASSIGN_PCT |
|       | Managed Systems Metrics                    | QOS_EXEC_STATE<br>QOS_MS_SUPP_LPARS       |
|       | Managed Systems Storage Pool Metrics       | QOS_STORAGE_POOL                          |
|       | Managed Systems Storage Pool Utilization   | QOS_STORAGE_POOL_UTIL                     |
|       | VIO and VMs CPU Metrics                    | QOS_LPAR_PROCS                            |
|       | VIO and VMs Memory Metrics                 | QOS_LPAR_MEMORY                           |

### Managed Systems CPU Metrics

This chart displays information about the CPU metrics for the managed system. The metrics are relative to the host regarding what is available, configurable, deconfigured, or installed overall for VMs, including the VIO.

| Column                        | Description                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------|
| Host                          | The name or IP address of the managed system.                                              |
| Available Processing Units    | The number of available processing units.                                                  |
| Configurable Processing Units | The number of processing units configurable for partitions.                                |
| Deconfigured Processing Units | The number of processing units taken offline because of failure or manual deconfiguration. |
| Installed Processing Units    | The number of processing units installed on the managed system.                            |

### **Managed Systems Memory Metrics**

This chart displays information about the overall memory metrics at the managed system level that are available for VMs.

| Column                         | Description                                                              |
|--------------------------------|--------------------------------------------------------------------------|
| Host                           | The name or IP address of the managed system.                            |
| Assigned Memory                | The amount of memory assigned to VMs.                                    |
| Configurable Memory            | The total amount of configurable memory available on the managed system. |
| Deconfigured Memory            | The amount of memory on the managed system that has been deconfigured.   |
| Installed Memory               | The amount of memory installed on the managed system.                    |
| Unassigned Memory              | The amount of memory available to be assigned to VMs.                    |
| System Firmware Current Memory | The amount of memory used by the system firmware.                        |
| Percent Memory Assigned        | Percentage of configurable memory that has been assigned.                |

### **Managed Systems Global Shared Pool Metrics**

This chart displays information about the global shared processor pool for a particular managed system.

| Column                  | Description                                                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Host                    | The name or IP address of the managed system.                                                                                   |
| Global Pool Size        | Size of the global shared processor pool.                                                                                       |
| Global Pool Utilization | The average global shared processor pool utilization.<br>Green = 0.00 - 60.99<br>Orange = 61.00 - 80.100<br>Red = 81.00 - 101.0 |

### **Managed Systems Storage Pool Utilization**

This chart displays information about the storage pool utilization for the managed system.

| Column                   | Description                                                                                                 |
|--------------------------|-------------------------------------------------------------------------------------------------------------|
| Source                   | The name or IP address of the managed system.                                                               |
| Target                   | The name of the storage pool.                                                                               |
| Percent Pool Utilization | Percentage of storage space used.<br>Green = 0.00 - 60.99<br>Orange = 61.00 - 80.101<br>Red = 81.00 - 102.0 |

### **Managed Systems Storage Pool Metrics**

This chart displays information about the storage pool metrics, in Megabytes.

| Column        | Description                                   |
|---------------|-----------------------------------------------|
| Target        | The name of the storage pool.                 |
| Source        | The name or IP address of the managed system. |
| Metric Values | The storage pool used, size, and free space.  |

### Managed Systems Metrics

This chart displays information about the managed system logistical and state metrics.

| Column          | Description                                   |
|-----------------|-----------------------------------------------|
| Host            | The name or IP address of the managed system. |
| Execution State | The host managed system execution state.      |
| Max LPARs       | The maximum VMs supported by the host.        |

### Managed Systems Disk Bandwidth

This chart displays information about the disk bandwidth for managed system disks allocated to the VIO as shared storage.

| Column         | Description                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------------------|
| Target         | The name of the disk.                                                                                          |
| Source         | The name or IP address of the managed system.                                                                  |
| Disk Bandwidth | Percent bandwidth used for each disk.<br>Green = 0.00 - 60.99<br>Orange = 61.00 - 80.99<br>Red = 81.00 - 100.0 |

### Managed Systems Disk Transfer Rate

This chart displays information about the disk data transfer rate for managed system disks allocated to the VIO as shared storage.

| Column | Description                                           |
|--------|-------------------------------------------------------|
| Target | The name of the disk.                                 |
| Source | The name or IP address of the managed system.         |
| Disk   | The disk data transfer rate per second for each disk. |

### Managed Systems Disk Size

This chart displays information about the disk size for managed system disks allocated to the VIO as shared storage.

| Column    | Description                                   |
|-----------|-----------------------------------------------|
| Target    | The name of the disk.                         |
| Source    | The name or IP address of the managed system. |
| Disk Size | The size of the disk.                         |

### VIO and VMs CPU Metrics

This chart displays information about the shared processor CPU metrics for VIO and VMs from managed systems.

| Column            | Description                                                                       |
|-------------------|-----------------------------------------------------------------------------------|
| Host              | The name or IP address of the VM or the VIO server.                               |
| Active Processors | The number of processors or virtual processors that are active for the partition. |

|                              |                                                                                                           |
|------------------------------|-----------------------------------------------------------------------------------------------------------|
| Assigned Processors          | The current number of processors or virtual processors assigned to the partition.                         |
| Maximum Processors           | The maximum number of processors or virtual processors that can be dynamically assigned to the partition. |
| Minimum Processors           | The minimum number of processors or virtual processors that can be dynamically assigned to the partition. |
| Physical Processors Consumed | The number of physical processors used by the partition.                                                  |
| Current Processing Units     | The current number of processing units assigned to the logical partition.                                 |
| Runtime Processing Units     | The number of processing units that are varied on for the partition.                                      |

### **VIO and VMs Memory Metrics**

This chart displays information about the shared memory metrics for VIO and VMs from managed systems.

| Column          | Description                                                                     |
|-----------------|---------------------------------------------------------------------------------|
| Host            | The hostname or IP address of the VM or the VIO server.                         |
| Assigned Memory | The amount of memory assigned to the partition.                                 |
| Used Memory     | The memory used by the partition at the time of sample.                         |
| Maximum Memory  | The maximum amount of memory that can be dynamically assigned to the partition. |
| Minimum Memory  | The minimum amount of memory that can be dynamically assigned to the partition. |

## **IIS Unified Dashboard**

The IIS Unified Dashboard provides predefined list views for monitoring Disk Usage, HTTP Traffic, and Server Performance.

### **Contents**

#### **IIS Required Data Sources**

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the IIS dashboard.

| QoS                  | Subkey/Target |
|----------------------|---------------|
| QOS_BYTESRECEIVED_PS | *             |
| QOS_IIS_HTTPPRESTIME | *             |
| QOS_CPU_USAGE        | *             |
| QOS_IIS_DISK_USAGE   | *             |
| QOS_MEMORY_USAGE     | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.



### Disk Usage

This chart displays information about the Disk Usage.

| Column Name | Description                                                    |
|-------------|----------------------------------------------------------------|
| Disk Usage  | Monitors the disk usage for all the disks present on the probe |

### HTTP Traffic

This chart displays information about the HTTP Traffic.

| Column Name               | Description                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------|
| Bytes Received Per Second | Rate at which data bytes are received by the World Wide Web Publishing Service (WWW service) per second. |
| HTTP Response Time        | Measures the time in ms for the server to respond to a http request.                                     |

### Server Performance

This chart displays information about the Server Performance.

| Column Name  | Description                                         |
|--------------|-----------------------------------------------------|
| CPU Usage    | Measures the CPU Usage of the server in percentage. |
| Memory Usage | Monitors the Memory Usage in megabytes.             |

## Cisco IP SLA Unified Dashboard

The Cisco IP SLA Unified Dashboard provides predefined list views for monitoring information about the IP SLA (Internet protocol service level agreement) measurements on network interfaces.

### Contents

#### Required Data Sources in the snmpcollector Probe

To enable the required metrics, use the snmpcollector Template Editor to navigate to and open the Network Response Time template. Enable the required metrics in the Applications/Services, Jitter, Path, and Protocol templates that are included in the Network Response Time template.

|                       |                       |                                                                                                                                |
|-----------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Network Response Time | Applications/Services | Response Path Test DHCP<br>Response Path Test DNS<br>Response Path Test HTTP<br>Response Path Test Operation                   |
|                       | Jitter                | Response Path Test Ethernet Jitter<br>Response Path Test ICMP Jitter<br>Response Path Test Jitter<br>Response Path with Jitter |
|                       | Path                  | Response Path Test EthernetPing<br>Response Path Test ICMP<br>Response Path Test PathEcho                                      |

|  |          |                                                                             |
|--|----------|-----------------------------------------------------------------------------|
|  | Protocol | Response Path Test DLSW<br>Response Path Test TCP<br>Response Path Test UDP |
|--|----------|-----------------------------------------------------------------------------|

The following table contains the required monitors that you must activate in the snmpcollector templates to see data in the IPSLA Unified Dashboard.

| Dashboard Chart           | QoS                                                  | Subkey/Target |
|---------------------------|------------------------------------------------------|---------------|
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_MINIMUMRESPONSE           | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_MAXIMUMRESPONSE           | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_AVERAGERESPONSETIME       | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_JITTERIN                  | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_JITTEROUT                 | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_POSITIVEJITTER            | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_NEGATIVEJITTER            | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_MINIMUMMOSRATING          | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_PACKETSLOSSDESTSRC        | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_PACKETSLOSSSRCDEST        | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_PACKETSFAILEDATTEMPTS     | *             |
| Top IPSLA Jitter Tests    | QOS_RESPONSEPATHTESTJITTER_PACKETSSUCCESSFULATTEMPTS | *             |
| Top IPSLA ICMP Path Tests | QOS_RESPONSEPATHTESTICMP_MINIMUMRESPONSE             | *             |
| Top IPSLA ICMP Path Tests | QOS_RESPONSEPATHTESTICMP_MAXIMUMRESPONSE             | *             |
| Top IPSLA ICMP Path Tests | QOS_RESPONSEPATHTESTICMP_AVERAGERESPONSETIME         | *             |
| Top IPSLA ICMP Path Tests | QOS_RESPONSEPATHTESTICMP_PACKETSFAILEDATTEMPTS       | *             |
| Top IPSLA ICMP Path Tests | QOS_RESPONSEPATHTESTICMP_PACKETSSUCCESSFULATTEMPTS   | *             |
| Top IPSLA Path Echo Tests | QOS_RESPONSEPATHTESTPATHECHO_PATHAVAILABILITY        | *             |
| Top IPSLA Path Echo Tests | QOS_RESPONSEPATHTESTPATHECHO_MINIMUMRESPONSE         | *             |
| Top IPSLA Path Echo Tests | QOS_RESPONSEPATHTESTPATHECHO_MAXIMUMRESPONSE         | *             |

|                             |                                                    |   |
|-----------------------------|----------------------------------------------------|---|
| Top IPSLA Path Echo Tests   | QOS_RESPONSEPATHTESTPATHECHO_AVGRESPONSETIME       | * |
| Top IPSLA Path Echo Tests   | QOS_RESPONSEPATHTESTPATHECHO_PCTFAILEDATTEMPTS     | * |
| Top IPSLA Path Echo Tests   | QOS_RESPONSEPATHTESTPATHECHO_PCTSUCCESSFULATTEMPTS | * |
| Top IPSLA TCP Connect Tests | QOS_RESPONSEPATHTESTTCP_MINIMUMRESPONSE            | * |
| Top IPSLA TCP Connect Tests | QOS_RESPONSEPATHTESTTCP_MAXIMUMRESPONSE            | * |
| Top IPSLA TCP Connect Tests | QOS_RESPONSEPATHTESTTCP_AVGRESPONSETIME            | * |
| Top IPSLA TCP Connect Tests | QOS_RESPONSEPATHTESTTCP_PCTFAILEDATTEMPTS          | * |
| Top IPSLA TCP Connect Tests | QOS_RESPONSEPATHTESTTCP_PCTSUCCESSFULATTEMPTS      | * |
| Top IPSLA UDP Path Tests    | QOS_RESPONSEPATHTESTUDP_MINIMUMRESPONSE            | * |
| Top IPSLA UDP Path Tests    | QOS_RESPONSEPATHTESTUDP_MAXIMUMRESPONSE            | * |
| Top IPSLA UDP Path Tests    | QOS_RESPONSEPATHTESTUDP_AVGRESPONSETIME            | * |
| Top IPSLA UDP Path Tests    | QOS_RESPONSEPATHTESTUDP_PCTFAILEDATTEMPTS          | * |
| Top IPSLA UDP Path Tests    | QOS_RESPONSEPATHTESTUDP_PCTSUCCESSFULATTEMPTS      | * |
| Top IPSLA DHCP Tests        | QOS_RESPONSEPATHTESTDHCP_MINIMUMRESPONSE           | * |
| Top IPSLA UDP Path Tests    | QOS_RESPONSEPATHTESTDHCP_MAXIMUMRESPONSE           | * |
| Top IPSLA UDP Path Tests    | QOS_RESPONSEPATHTESTDHCP_AVGRESPONSETIME           | * |
| Top IPSLA UDP Path Tests    | QOS_RESPONSEPATHTESTDHCP_PCTFAILEDATTEMPTS         | * |
| Top IPSLA UDP Path Tests    | QOS_RESPONSEPATHTESTDHCP_PCTSUCCESSFULATTEMPTS     | * |
| Top IPSLA DNS Tests         | QOS_RESPONSEPATHTESTDNS_MINIMUMRESPONSE            | * |
| Top IPSLA DNS Tests         | QOS_RESPONSEPATHTESTDNS_MAXIMUMRESPONSE            | * |
| Top IPSLA DNS Tests         | QOS_RESPONSEPATHTESTDNS_AVGRESPONSETIME            | * |
| Top IPSLA HTTP Tests        | QOS_RESPONSEPATHTESTHTTP_MINIMUMRESPONSE           | * |
| Top IPSLA HTTP Tests        | QOS_RESPONSEPATHTESTHTTP_MAXIMUMRESPONSE           | * |
| Top IPSLA HTTP Tests        | QOS_RESPONSEPATHTESTHTTP_AVGRESPONSETIME           | * |

|                      |                                                |   |
|----------------------|------------------------------------------------|---|
| Top IPSLA HTTP Tests | QOS_RESPONSEPATHTESTHTTP_PCTFAILEDATTEMPTS     | * |
| Top IPSLA HTTP Tests | QOS_RESPONSEPATHTESTHTTP_PCTSUCCESSFULATTEMPTS | * |

An asterisk (\*) means that the value for the first entry for the QoS is used.

### Top IP SLA Jitter Tests

This chart displays information about IP SLA Jitter test performance over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column              | Description                                                                             |
|---------------------|-----------------------------------------------------------------------------------------|
| Device              | The name of the monitored device. Click this link to view additional information in OC. |
| Target              | The name of the device interface. Click this link to view additional information in OC. |
| Min.                | The minimum inter-packet delay in milliseconds.                                         |
| Max.                | The maximum inter-packet delay in milliseconds.                                         |
| Avg.                | The average inter-packet delay in milliseconds.                                         |
| Jitter In           | The inter-packet delay variance in milliseconds for inbound packets.                    |
| Jitter Out          | The inter-packet delay variance in milliseconds for outbound packets.                   |
| Positive Jitter     | The number of positive jitter values from packets sent.                                 |
| Negative Jitter     | The number of negative jitter values from packets sent.                                 |
| Min. MOS            | The minimum MOS value from IP SLA Jitter test packets sent.                             |
| Pct Pkt Loss DS-SRC | The number of packets per second lost from destination to source.                       |
| Pct Pkt Loss SRC-DS | The number of packets per second lost from source to destination.                       |
| Pct Errors          | The percentage of failed IP SLA operations.                                             |
| Pct Completions     | The percentage of completed IP SLA operations.                                          |

### Top IP SLA ICMP Path Tests

This chart displays information about IP SLA ICMP path test performance over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column          | Description                                                                             |
|-----------------|-----------------------------------------------------------------------------------------|
| Device          | The name of the monitored device. Click this link to view additional information in OC. |
| Target          | The name of the device interface. Click this link to view additional information in OC. |
| Min.            | The minimum ICMP response time in milliseconds.                                         |
| Max.            | The maximum ICMP response time in milliseconds.                                         |
| Avg.            | The average ICMP response time in milliseconds.                                         |
| Pct Errors      | The percentage of failed ICMP responses.                                                |
| Pct Completions | The percentage of successful ICMP responses.                                            |

**Top IP SLA Path Echo Tests**

This chart displays information about IP SLA path echo test performance over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column            | Description                                                                             |
|-------------------|-----------------------------------------------------------------------------------------|
| Device            | The name of the monitored device. Click this link to view additional information in OC. |
| Target            | The name of the device interface. Click this link to view additional information in OC. |
| Path Availability | The percent path availability.                                                          |
| Min.              | The minimum observed round trip time for the operation in milliseconds.                 |
| Max.              | The maximum observed round trip time for the operation in milliseconds.                 |
| Avg.              | The average observed round trip time for the operation in milliseconds.                 |
| Pct Errors        | The percentage of request errors.                                                       |
| Pct Completions   | The percentage of request completions.                                                  |

**Top IP SLA TCP Connect Tests**

This chart displays information about IP SLA TCP connect test performance over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column          | Description                                                                             |
|-----------------|-----------------------------------------------------------------------------------------|
| Device          | The name of the monitored device. Click this link to view additional information in OC. |
| Target          | The name of the device interface. Click this link to view additional information in OC. |
| Min.            | The minimum observed round trip time for the operation in milliseconds.                 |
| Max.            | The maximum observed round trip time for the operation in milliseconds.                 |
| Avg.            | The average observed round trip time for the operation in milliseconds.                 |
| Pct Errors      | The percentage of request errors, excluding timeouts, busies, and drops.                |
| Pct Completions | The percentage of request completions, excluding timeouts, busies, and drops.           |

**Top IP SLA UDP Path Tests**

This chart displays information about IP SLA UDP path test performance over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column | Description                                                                             |
|--------|-----------------------------------------------------------------------------------------|
| Device | The name of the monitored device. Click this link to view additional information in OC. |

|                 |                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------|
| Target          | The name of the device interface. Click this link to view additional information in OC. |
| Min.            | The minimum observed round trip time for the operation in milliseconds.                 |
| Max.            | The maximum observed round trip time for the operation in milliseconds.                 |
| Avg.            | The average observed round trip time for the operation in milliseconds.                 |
| Pct Errors      | The percentage of request errors, excluding timeouts, busies, and drops.                |
| Pct Completions | The percentage of request completions, excluding timeouts, busies, and drops.           |

### **Top IP SLA DHCP Tests**

This chart displays information about IP SLA DHCP test performance over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column          | Description                                                                             |
|-----------------|-----------------------------------------------------------------------------------------|
| Device          | The name of the monitored device. Click this link to view additional information in OC. |
| Target          | The name of the device interface. Click this link to view additional information in OC. |
| Min.            | The minimum observed round trip time for the operation in milliseconds.                 |
| Max.            | The maximum observed round trip time for the operation in milliseconds.                 |
| Avg.            | The average observed round trip time for the operation in milliseconds.                 |
| Pct Errors      | The percentage of request errors.                                                       |
| Pct Completions | The percentage of request completions.                                                  |

### **Top IP SLA DNS Tests**

This chart displays information about IP SLA DNS test performance over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column | Description                                                                             |
|--------|-----------------------------------------------------------------------------------------|
| Device | The name of the monitored device. Click this link to view additional information in OC. |
| Target | The name of the device interface. Click this link to view additional information in OC. |
| Min.   | The minimum observed round trip time for the operation in milliseconds.                 |
| Max.   | The maximum observed round trip time for the operation in milliseconds.                 |
| Avg.   | The average observed round trip time for the operation in milliseconds.                 |

## Top IP SLA HTTP Tests

This chart displays information about IP SLA HTTP test performance over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column          | Description                                                                             |
|-----------------|-----------------------------------------------------------------------------------------|
| Device          | The name of the monitored device. Click this link to view additional information in OC. |
| Target          | The name of the device interface. Click this link to view additional information in OC. |
| Min.            | The minimum observed round trip time for the operation in milliseconds.                 |
| Max.            | The maximum observed round trip time for the operation in milliseconds.                 |
| Avg.            | The average observed round trip time for the operation in milliseconds.                 |
| Pct Errors      | The percentage of request errors.                                                       |
| Pct Completions | The percentage of request completions.                                                  |

## JBoss Unified Dashboard

The JBoss Unified Dashboard provides predefined list views for monitoring the JBoss application server. You can configure the probe to measure more specific metrics based on these general metrics:

- count
- thread count
- memory usage

For example, the count metric can be configured to count any instance of JBoss function, such as total requests.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### JBoss Required Data Sources

The table contains the probes and QoS metrics required for the preconfigured JBoss dashboard.

| Probe | Chart           | QoS Required           |
|-------|-----------------|------------------------|
| JBoss | Counters        | QOS_JBOSS_COUNTER      |
| JBoss | Memory Usage    | QOS_JBOSS_MEMORY_USAGE |
| JBoss | Thread Counters | QOS_JBOSS_THREADCOUNT  |

#### NOTE

The OC Dashboards template includes some of the required QoS measurements, but not all. Make sure all the measurements listed here are enabled in the probe.

## JBoss Counters

You can use JBoss Counters to measure and tune various operations. JBoss Counters can be configured in the probe to count any function of a JBoss application server.

| Column        | Description                                                          |
|---------------|----------------------------------------------------------------------|
| Source        | The name or IP address of the managed system.                        |
| Target        | The name of the disk.                                                |
| Metric Values | The total for the count metric specified in the probe configuration. |

## JBoss Memory Usage

You can use JBoss Memory Usage to monitor and tune memory use. JBoss Memory Usage can be configured in the probe to measure various types of memory use.

| Column        | Description                                                                 |
|---------------|-----------------------------------------------------------------------------|
| Source        | The name or IP address of the managed system.                               |
| Target        | The name of the disk.                                                       |
| Metric Values | The total for the memory usage metric specified in the probe configuration. |

## JBoss Thread Counters

You can use the JBoss Thread Counters list view to optimize resource allocation based on server load. For example, if the number of active thread is 80% of the total maximum allowed, then you tune your system to enable better response times.

The Thread Counters can be configured in the probe to monitor individual or group threads.

| Column        | Description                                                                 |
|---------------|-----------------------------------------------------------------------------|
| Source        | The name or IP address of the managed system.                               |
| Target        | The name of the disk.                                                       |
| Metric Values | The total for the thread count metric specified in the probe configuration. |

## Lync\_Monitor Unified Dashboard

### Contents

### Lync\_Monitor Required Data Sources

| QoS Required            | Subkey/Target       |
|-------------------------|---------------------|
| QOS_%_IDLE_TIME         | Processor Idle Time |
| QOS_%_PROCESSOR_TIME    | CPU Processing Time |
| QOS_ACTIVE_TRANSACTIONS | Active Transactions |
| QOS_AVG_DISK_SEC/READ   | Disk Read           |
| QOS_AVG_DISK_SEC/WRITE  | Disk Write          |



The following QoS table is for the Lync 2010 counters:

| QoS Required                          | Subkey/Target          |
|---------------------------------------|------------------------|
| QOS_DATAMCU_-_005_-_MCU_HEALTH_STATE  | Data MCU Health State  |
| QOS_IMMCU_-_001_-_CONNECTED_USERS     | IMMCU Connected Users  |
| QOS_IMMCU_-_005_-_MCU_HEALTH_STATE    | IMMCU Health State     |
| QOS_USRV_-_002_-_QUEUE_LATENCY_(MSEC) | FrontEnd Queue Latency |
| QOS_USRV_-_004_-_SPROC_LATENCY_(MSEC) | FrontEnd Sproc Latency |

### **Processor Idle Time**

| Column              | Description                                    |
|---------------------|------------------------------------------------|
| Host                | Name of the host where the Lync server exists. |
| Profile             | Target that is being monitored.                |
| Processor Idle Time | Time span for which processor remain idle.     |

### **CPU Processing Time**

| Column              | Description                                    |
|---------------------|------------------------------------------------|
| Host                | Name of the host where the Lync server exists. |
| Profile             | Target that is being monitored.                |
| CPU Processing Time | % of processor time consumed by a lync server. |

### **Active Transactions**

| Column              | Description                                    |
|---------------------|------------------------------------------------|
| Host                | Name of the host where the Lync server exists. |
| Profile             | Target that is being monitored.                |
| Active Transactions | Number of Active transactions at a time.       |

### **Disk Read**

| Column    | Description                                        |
|-----------|----------------------------------------------------|
| Host      | Name of the host where the Lync server exists.     |
| Profile   | Target that is being monitored.                    |
| Disk Read | Average number of disk read operations per second. |

**Disk Write**

| Column     | Description                                         |
|------------|-----------------------------------------------------|
| Host       | Name of the host where the Lync server exists.      |
| Profile    | Target that is being monitored.                     |
| Disk Write | Average number of disk write operations per second. |

**Data MCU Health State**

| Column                | Description                                    |
|-----------------------|------------------------------------------------|
| Host                  | Name of the host where the Lync server exists. |
| Profile               | Target that is being monitored.                |
| Data MCU Health State | Data MCU Health State.                         |

**IMMCU Connected Users**

| Column                | Description                                    |
|-----------------------|------------------------------------------------|
| Host                  | Name of the host where the Lync server exists. |
| Profile               | Target that is being monitored.                |
| IMMCU Connected Users | IMMCU Connected Users.                         |

**IMMCU Health State**

| Column             | Description                                    |
|--------------------|------------------------------------------------|
| Host               | Name of the host where the Lync server exists. |
| Profile            | Target that is being monitored.                |
| IMMCU Health State | IMMCU Health State.                            |

**Front-End Queue Latency**

| Column                 | Description                                    |
|------------------------|------------------------------------------------|
| Host                   | Name of the host where the Lync server exists. |
| Profile                | Target that is being monitored.                |
| FrontEnd Queue Latency | Front End Queue Latency.                       |

## Front-End Stored Procedure Latency

| Column                 | Description                                    |
|------------------------|------------------------------------------------|
| Host                   | Name of the host where the Lync server exists. |
| Profile                | Target that is being monitored.                |
| FrontEnd Sproc Latency | Front End Stored Procedure Latency.            |

## Microsoft Azure Unified Dashboard

The Microsoft Azure Unified Dashboard provides predefined list views with key performance indicators for your Azure environment including virtual machines, websites, storage, and more.

### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### Azure Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the Azure dashboard.

| QoS                                      | Subkey/ Target |
|------------------------------------------|----------------|
| QOS_AZURE_STORAGE_STATE                  | *              |
| QOS_AZURE_STORAGE_AVAILABILITY           | *              |
| QOS_AZURE_STORAGE_SUCCESS_PERCENTAGE     | *              |
| QOS_AZURE_STORAGE_SUCCESS_COUNT          | *              |
| QOS_AZURE_STORAGE_TOTAL_REQUESTS         | *              |
| QOS_AZURE_VM_DISK_READ                   | *              |
| QOS_AZURE_VM_DISK_WRITE                  | *              |
| QOS_AZURE_VM_NETWORK_IN                  | *              |
| QOS_AZURE_VM_NETWORK_OUT                 | *              |
| QOS_AZURE_VM_CPU_USAGE                   | *              |
| QOS_AZURE_WEBSITE_AVG_MEMORY_WORKING_SET | *              |
| QOS_AZURE_WEBSITE_AVG_RESPONSE_TIME      | *              |
| QOS_AZURE_WEBSITE_CPU_TIME               | *              |
| QOS_AZURE_WEBSITE_DATA_IN                | *              |
| QOS_AZURE_WEBSITE_DATA_OUT               | *              |
| QOS_AZURE_WEBSITE_HTTP_ERRORS            | *              |
| QOS_AZURE_WEBSITE_HTTP_CLIENT_ERRORS     | *              |
| QOS_AZURE_WEBSITE_HTTP_REDIRECTS         | *              |
| QOS_AZURE_WEBSITE_HTTP_SERVER_ERRORS     | *              |
| QOS_AZURE_WEBSITE_HTTP_SUCCESSES         | *              |

|                         |   |
|-------------------------|---|
| QOS_AZURE_WEBSITE_STATE | * |
|-------------------------|---|

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

For more information on configuring probes, see the documentation for each probe.

### **VM Summary**

| Column                   | Description                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VM CPU Usage             | The percentage of CPU utilization.                                                                                                                                |
| VM Network Input         | The number of bytes received on all network interfaces by the VM. This metric identifies the volume of incoming network traffic to an application on a single VM. |
| VM Network Output        | The number of bytes sent out on all network interfaces by the VM. This metric identifies the volume of outgoing network traffic to an application on a single VM. |
| VM Disk Read Throughput  | Total disk read throughput.                                                                                                                                       |
| VM Disk Write Throughput | Total disk read throughput.                                                                                                                                       |
| VM State                 | The current availability and health status of the VMs. The values are as follows: 0-Started, 1-Starting, 2-Stopping, 3-Stopped, 4-Unknown                         |

### **Storage Summary**

| Column                     | Description                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Storage Available          | The availability of the specified storage account name.                                                                          |
| Storage Success Percentage | The percentage of successful storage requests.                                                                                   |
| Storage Success Count      | The number of successful storage requests.                                                                                       |
| Storage Total Requests     | The total number of requests made to the specified storage service. This number includes both, successful and failed requests.   |
| Storage State              | The status of the storage account. The values are as follows: 0-Created, 1-Creating, 2-ResolvingDns, 3-Changing, and 4-Deleting. |

### **Website Summary1**

| Column                             | Description                                                                                                                                                  |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Website Average Response Time      | The response time of the website.                                                                                                                            |
| Website Average Memory Working Set | The current size of the Working Set of the running process. The Working set includes the set of memory pages touched recently by the threads in the process. |
| Website CPU Time                   | The CPU usage of the website.                                                                                                                                |
| Website Data Input                 | Measures the data received by the website from clients.                                                                                                      |
| Website Data Output                | Measures the data sent by the website to clients                                                                                                             |
| Website State                      | The state of the website. The values are as follows: 0-Running, 1-Stopped                                                                                    |

## Website Summary2

| Column                     | Description                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------|
| Website Http Errors        | The number of Http "401 Unauthorized", "403 Forbidden", "404 Not Found" and "406 Not Acceptable" messages sent. |
| Website Http Client Errors | The number of Http "4xx Client Error" messages sent.                                                            |
| Website Http Redirects     | The number of Http "3xx Redirection" messages sent.                                                             |
| Website Http Server Errors | The number of Http "5xx Server Error" messages sent.                                                            |
| Website Http Successes     | The number of Http "2xx Success" messages sent.                                                                 |

## MongoDB Unified Dashboard

The MongoDB Unified Dashboard provides predefined list views for monitoring nodes in a MongoDB cluster.

### NOTE

: If your Unified Dashboard is not populating with data, verify that all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required monitors are active. For more information, see the help topic on required data sources for the Unified Dashboard.

### Required Data Sources

The following table contains the monitors that you must activate in the `mongodb_monitor` probe to see data in the MongoDB Unified Dashboard.

| Dashboard Chart    | QoS                              | Description                                                                                                                                                                                            |
|--------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cluster Summary    | QOS_MONGO_CLUSTER_VERSION        | The MongoDB version                                                                                                                                                                                    |
| Cluster Summary    | QOS_MONGODB_SYS_MEM_USED_PERCENT | The percentage of memory used                                                                                                                                                                          |
| Cluster Summary    | QOS_MONGODB_SYS_IO_USE_PERCENT   | The percentage of disk used                                                                                                                                                                            |
| Replica Set Status | QOS_MONGO_REPSET_STATUS_HEALTH   | The health of the replica set. Possible values are: (1) up or (0) down. This value is not returned for the member that returns the response status.                                                    |
| Replica Set Status | QOS_MONGO_REPSET_STATUS_UPTIME   | The number of seconds that this member has been online                                                                                                                                                 |
| Replica Set Status | QOS_MONGO_REPSET_STATUS_STATE    | The replica state of the member. Possible values are:<br>STARTUP = 0, PRIMARY = 1, SECONDARY = 2, RECOVERING = 3, STARTUP2 = 5, UNKNOWN = 6, ARBITER = 7, DOWN = 8, ROLLBACK = 9, REMOVED = 10.        |
| Replica Set Status | QOS_MONGO_REPSET_STATUS_PINGMS   | The number of milliseconds (ms) that a round-trip packet takes to travel between the remote member and the local instance. This value is not returned for the member that returns the response status. |
| Server Status      | QOS_MONGO_SRV_STATUS_UPTIME      | The number of seconds that the mongos or mongod process has been active.                                                                                                                               |

|               |                                                    |                                                                                                                                                                                                         |
|---------------|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Status | QOS_MONGO_SRV_STATUS_MEM_MAPPED                    | The amount of mapped memory by the database in megabytes (MB). Because MongoDB uses memory-mapped files, this value is likely to be roughly equivalent to the total size of your database or databases. |
| Server Status | QOS_MONGO_SRV_STATUS_GLOBALOCK_ACTIVECLIENTS_TOTAL | The total number of active client connections to the database. This count combines clients that are performing read operations (readers) and clients that are performing write operations (writers).    |
| Server Status | QOS_MONGO_SRV_STATUS_METRICS_DOCUMENT_INSERTED     | The total number of documents inserted                                                                                                                                                                  |
| Server Status | QOS_MONGO_SRV_STATUS_METRICS_DOCUMENT_DELETED      | The total number of documents deleted                                                                                                                                                                   |
| Server Status | QOS_MONGO_SRV_STATUS_METRICS_DOCUMENT_UPDATED      | The total number of documents updated                                                                                                                                                                   |

### **Cluster Summary**

The following table describes the Cluster Summary chart in the MongoDB Unified Dashboard.

| Column          | Description                        |
|-----------------|------------------------------------|
| Host            | The name or IP address of the host |
| Cluster Version | The version of the MongoDB cluster |
| Memory Usage    | The percentage of memory used      |
| Storage Usage   | The percentage of disk used        |

### **Replica Set Status**

The following table describes the Replica Set Status chart in the MongoDB Unified Dashboard.

| Column             | Description                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host               | The name or IP address of the host                                                                                                                                                                     |
| Target             | The logical or physical component under monitor                                                                                                                                                        |
| Replica Set Health | The health of the replica set. Possible values are: (1) up or (0) down. This value is not returned for the member that returns the response status.                                                    |
| Replica Set Uptime | The number of seconds that this member has been online                                                                                                                                                 |
| State              | The replica state of the member. Possible values are: STARTUP = 0, PRIMARY = 1, SECONDARY = 2, RECOVERING = 3, STARTUP2 = 5, UNKNOWN = 6, ARBITER = 7, DOWN = 8, ROLLBACK = 9, REMOVED = 10.           |
| Response Time      | The number of milliseconds (ms) that a round-trip packet takes to travel between the remote member and the local instance. This value is not returned for the member that returns the response status. |

## Server Status

The following table describes the Server Status chart in the MongoDB Unified Dashboard.

| Column             | Description                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host               | The name or IP address of the host                                                                                                                                                                            |
| Target             | The logical or physical component under monitor                                                                                                                                                               |
| Server Uptime      | The number of seconds that the mongos or mongod process has been active                                                                                                                                       |
| Memory Mapped      | The amount of mapped memory by the database in megabytes (MB). Because MongoDB uses memory-mapped files, this value is likely to be to be roughly equivalent to the total size of your database or databases. |
| Active Connection  | The total number of active client connections to the database. This count combines clients that are performing read operations (readers) and clients that are performing write operations (writers).          |
| Inserted Documents | The total number of documents inserted                                                                                                                                                                        |
| Deleted Documents  | The total number of documents deleted                                                                                                                                                                         |
| Update Documents   | The total number of documents updated                                                                                                                                                                         |

## Shard Statistics

The following table describes the Shard Statistics chart in the MongoDB Unified Dashboard.

| Column              | Description                                                                                           |
|---------------------|-------------------------------------------------------------------------------------------------------|
| Host                | The name or IP address of the host                                                                    |
| Target              | The logical or physical component under monitor                                                       |
| Document Count      | The percentage of the documents or objects of this collection found in this shard                     |
| Chunk Count         | The number of chunks of this collection found in this shard                                           |
| Average Object Size | The average size of an object in this shard of the collection. The scale argument affects this value. |

## MS Exchange 2007 Unified Dashboard

The MS Exchange 2007 Server Unified Dashboard provides pre-defined list views with information about your Microsoft Exchange 2003 server and Microsoft Exchange 2007 server, such as load, processor time, queues, and disk performance.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### MS Exchange Required Data Sources

The MS Exchange 2007 Unified Dashboard requires these probes:

- exchange\_monitor
- exchange\_monitor\_backend
- perfmon
- processes
- ntevl

This table lists the QoS metrics and subkeys or targets that must be activated on the probes to populate data in the MS Exchange 2007 dashboard.

| QoS Required                                                              | Subkey/Target                                |
|---------------------------------------------------------------------------|----------------------------------------------|
| QOS_MEMORY_PHYSICAL                                                       | *                                            |
| QOS_MEMORY_PHYSICAL_PERC                                                  | *                                            |
| QOS_EXCHANGE_MEMORY_AVAILABLE_MEGABYTES                                   | *                                            |
| QOS_EXCHANGE_MEMORY_PAGES_PER_SECOND                                      | *                                            |
| QOS_EXCHANGE_MEMORY_PAGING_FILE_USAGE                                     | *                                            |
| QOS_%_PROCESSOR_TIME                                                      | *                                            |
| QOS_%_USER_TIME                                                           | *                                            |
| QOS_EXCHANGE_IS_SEND_QUEUE_SIZE_-_PUBLIC_FOLDE<br>RSQOS_%_PRIVILEGED_TIME | *                                            |
| QOS_EXCHANGE_DISK_AVERAGE_DISK_QUEUE_LENGTH                               | *                                            |
| QOS_EXCHANGE_DISK_AVERAGE_DISK_BYTES_PER_TRAN<br>SFER                     | *                                            |
| QOS_EXCHANGE_DISK_AVERAGE_DISK_SECONDS_PER_R<br>EAD                       | *                                            |
| QOS_EXCHANGE_DISK_AVERAGE_DISK_SECONDS_PER_W<br>RITE                      | *                                            |
| QOS_EXCHANGE_IS_MESSAGE_OPENS_PER_SECOND_-_M<br>AILBOXES                  | *                                            |
| QOS_EXCHANGE_IS_MESSAGE_OPENS_PER_SECOND_-_P<br>UBLIC_FOLDERS             | *                                            |
| QOS_EXCHANGE_IS_RECEIVE_QUEUE_SIZE_-_MAILBOXES                            | *                                            |
| QOS_EXCHANGE_IS_SEND_QUEUE_SIZE_-_MAILBOXES                               | *                                            |
| QOS_EXCHANGE_IS_RECEIVE_QUEUE_SIZE_-_PUBLIC_FOL<br>DERS                   | *                                            |
| QOS_EXCHANGE_IS_SEND_QUEUE_SIZE_-_PUBLIC_FOLDE<br>RS                      | *                                            |
| QOS_EXCHANGE_SMTP_LOCAL_QUEUE_LENGTH                                      | Local Queue Length                           |
| QOS_EXCHANGE_SMTP_REMOTE_QUEUE_LENGTH                                     | Remote Queue Length                          |
| QOS_EXCHANGE_TRANS_ROLE_AGGREGATE_DELIVERY_Q<br>UEUE_LENGTH_(ALL_QUEUES)  | Aggregate Delivery Queue Length (All Queues) |
| QOS_EXCHANGE_TRANS_ROLE_POISON_QUEUE_LENGTH                               | Poison Queue Length                          |
| QOS_EXCHANGE_TRANS_ROLE_RETRY_MAILBOX_DELIVER<br>Y_QUEUE_LENGTH           | Retry Mailbox Delivery Queue Length          |
| QOS_EXCHANGE_TRANS_ROLE_UNREACHABLE_QUEUE_L<br>ENGTH                      | Unreachable Queue Length                     |
| QOS_EXCHANGE_MTA_CONNECTION_QUEUE_LENGTH                                  | Connection Queue Length (PendingRerouteQ)    |



|                                    |                   |
|------------------------------------|-------------------|
| QOS_EXCHANGE_MTA_WORK_QUEUE_LENGTH | Work Queue Length |
| QOS_CPU_USAGE                      |                   |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

**Memory Performance**

| Column                  | Description                                                                                                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                    | Name of the host where the Exchange server is installed.                                                                                                                        |
| Physical Memory         | Total amount of physical memory available to Windows.                                                                                                                           |
| Percent Physical Memory | Percentage of total amount of physical memory available to Windows.<br>0 to 50.99 = Green<br>51 to 75.99 = Yellow<br>76 to 89.99 = Orange<br>90 to 100 = Red                    |
| Available MB            | The amount of physical memory immediately available for allocation to a process or for system use.                                                                              |
| Pages/Sec               | The rate at which pages are read from or written to disk to resolve hard page faults. This counter is a primary indicator of the kinds of faults that cause system-wide delays. |
| Paging File Usage       | The percentage of a Page File instance in use.<br>0 to 50.99 = Green<br>51 to 59.99 = Yellow<br>60 to 74.99 = Orange<br>75 to 100 = Red                                         |

**Processor Utilization**

| Column               | Description                                                                                                                                    |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                 | Name of the host where the Exchange server is installed.                                                                                       |
| Perc Processor Time  | The percentage of elapsed time that the processor spends to execute a non-idle thread of the process.<br>0 to 74.99 = Green<br>75 to 100 = Red |
| Perc User Time       | The percentage of processor time spent in user mode.<br>0 to 74.99 = Green<br>75 to 100 = Red                                                  |
| Perc Privileged Time | The percentage of processor time spent in privileged mode.<br>0 to 74.99 = Green<br>75 to 100 = Red                                            |

**Disk Performance**

| Column | Description                                              |
|--------|----------------------------------------------------------|
| Host   | Name of the host where the Exchange server is installed. |

|                             |                                                                                                                       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Average Disk Queue Length   | The average number of both read and write requests that were queued for the selected disk during the sample interval. |
| Average Disk Bytes/Transfer | The average number of bytes transferred to or from the disk during write or read operations.                          |
| Average Disk Seconds/Read   | The average time to read data from the disk.                                                                          |
| Average Disk Seconds/Write  | The average time to write data to the disk.                                                                           |

### **IS Queues Msg Opens/Sec**

| Column                  | Description                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                    | Name of the host where the Exchange server is installed.                                                                                       |
| Mailboxes 1 hr avg      | This will show how often your users are opening messages within mailboxes. Peak load may show this coinciding with other system behavior.      |
| Public Folders 1 hr avg | This will show how often your users are opening messages within public folders. Peak load may show this coinciding with other system behavior. |

### **IS Send/Receive Queue Size**

| Column                            | Description                                              |
|-----------------------------------|----------------------------------------------------------|
| Host                              | Name of the host where the Exchange server is installed. |
| Mailbox Receive Queue Size        | Number of messages received in mail boxes.               |
| Mailbox Send Queue Size           | Number of messages sent from mail boxes.                 |
| Public Folders Receive Queue Size | Number of messages received in public folders.           |
| Public Folders Send Queue Size    | Number of messages sent from public folders.             |

### **Exchange SMTP Queues**

| Column | Description                                              |
|--------|----------------------------------------------------------|
| Host   | Name of the host where the Exchange server is installed. |
| Local  | Number of messages in the local SMTP queue.              |
| Remote | Number of messages in remote SMTP queue.                 |

#### **NOTE**

Data in this view will show up only for Exchange 2003 server setup.

### **Exchange Transport Role Queues**

| Column                 | Description                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------|
| Host                   | Name of the host where the Exchange server is installed.                                               |
| Messages               | Aggregate Delivery Queue Length (All Queues) is the number of items queued for delivery in all queues. |
| Poison                 | The number of items in the poison queue.                                                               |
| Retry Mailbox Delivery | The number of items in the retry mailbox queues.                                                       |
| Unreachable            | The number of items in the unreachable queues.                                                         |

**Exchange MTA Queues**

| Column             | Description                                               |
|--------------------|-----------------------------------------------------------|
| Host               | Name of the host where the Exchange server is installed.  |
| Connection 1hr avg | Average MTA connection queue length during the last hour. |
| Work 1hr avg       | Average MTA work queue length during the last hour.       |

**NOTE**

Data in this view will show up only for Exchange 2003 server setup.

**Exchange Server Load**

| Column                      | Description                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------|
| Host                        | Name of the host where the Exchange server is installed.                                                   |
| Processor Queue Length 1 hr | Number of processes queued for the Exchange server in the past hour.                                       |
| Current CPU Usage           | Percent of CPU consumed by the Exchange server.<br>0 to 80 = Green<br>80 to 90 = Orange<br>90 to 100 = Red |

**MS Exchange 2010 Unified Dashboard**

The MS Exchange Server 2010 Unified Dashboard provides pre-defined list views with information about your Microsoft Exchange server 2010, such as processor, memory performance, transport queues, domain controllers, .Net framework, and network counters.

**Contents****NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**MS Exchange 2010 Required Data Sources**

The MS Exchange 2007 Unified Dashboard requires these probes:

- exchange\_monitor
- exchange\_monitor\_backend
- perfmon
- processes
- ntevl

This table lists the QoS metrics and subkeys or targets that must be activated to populate data in the MS Exchange 2010 dashboard.

| QoS Required                           | Subkey/Target   |
|----------------------------------------|-----------------|
| QOS_EXCHANGE_PROCESSOR_USER_TIME       | User Time       |
| QOS_EXCHANGE_PROCESSOR_PRIVILEGED_TIME | Privileged Time |

|                                                                                |                                                          |
|--------------------------------------------------------------------------------|----------------------------------------------------------|
| QOS_EXCHANGE_PROCESSOR_PROCESSOR_QUEUE_LENGTH                                  | Processor Queue Length                                   |
| QOS_EXCHANGE_PROCESSOR_PROCESSOR_TIME                                          | Processor Time                                           |
| QOS_EXCHANGE_PROCESSOR_PROCESSOR_TIME_INSTANCE                                 | Processor Time Instance (processes)                      |
| QOS_EXCHANGE_MEMORY_AVAILABLE_MBYTES                                           | Available Mbytes                                         |
| QOS_EXCHANGE_MEMORY_POOL_PAGED_BYTES                                           | Pool Paged Bytes                                         |
| QOS_EXCHANGE_MEMORY_POOL_NONPAGED_MEGABYTES                                    | Pool Nonpaged Megabytes                                  |
| QOS_EXCHANGE_MEMORY_CACHE_BYTES                                                | Cache Bytes                                              |
| QOS_EXCHANGE_MEMORY_PRIVATE_BYTES                                              | Private Bytes                                            |
| QOS_EXCHANGE_MEMORY_VIRTUAL_BYTES                                              | Virtual Bytes                                            |
| QOS_EXCHANGE_TRANS_ROLE_AGGREGATE_DELIVERY_QUEUE_LENGTH_(ALL_QUEUES)-TRANSPORT | Aggregate Delivery Queue Length (All Queues) - Transport |
| QOS_EXCHANGE_TRANS_ROLE_ACTIVE_MAILBOX_DELIVERY_QUEUE_LENGTH-TRANSPORT         | Active Mailbox Delivery Queue Length - Transport         |
| QOS_EXCHANGE_TRANS_ROLE_RETRY_MAILBOX_DELIVERY_QUEUE_LENGTH-TRANSPORT          | Retry Mailbox Delivery Queue Length - Transport          |
| QOS_EXCHANGE_TRANS_ROLE_UNREACHABLE_QUEUE_LENGTH-TRANSPORT                     | Unreachable Queue Length - Transport                     |
| QOS_EXCHANGE_TRANS_ROLE_POISON_QUEUE_LENGTH-TRANSPORT                          | Poison Queue Length - Transport                          |
| QOS_EXCHANGE_TRANS_ROLE_MESSAGES_SUBMITTED_PER_SECOND                          | Messages Submitted Per Second                            |
| QOS_EXCHANGE_TRANS_ROLE_MESSAGES_COMPLETED_DELIVERY_PER_SECOND                 | Messages Completed Delivery Per Second                   |
| QOS_EXCHANGE_MSEXCHANGE_LDAP_SEARCHES_PER_SECOND                               | LDAP Searches Per Second(0)                              |
| QOS_EXCHANGE_MSEXCHANGE_LDAP_READ_TIME_PROCESSES                               | LDAP Read Time Processes                                 |
| QOS_EXCHANGE_MSEXCHANGE_LDAP_SEARCH_TIME_PROCESSES                             | LDAP Search Time Processes                               |
| QOS_EXCHANGE_MSEXCHANGE_LDAP_SEARCHES_TIMED_OUT_PER_MINUTE                     | LDAP Searches Timed Out Per Minute                       |
| QOS_EXCHANGE_MSEXCHANGE_LONG_RUNNING_LDAP_OPERATIONS_PER_MINUTE                | Long Running LDAP Operations Per Minute                  |
| QOS_EXCHANGE_MEMORY_DOTNET - TIME_IN_GC                                        | DOTNET Time in GC                                        |
| QOS_EXCHANGE_MEMORY_DOTNET - EXCEPTION_THROWN_PER_SEC                          | Dotnet - Exception Thrown Per Sec                        |
| QOS_EXCHANGE_MEMORY_DOTNET - BYTES_IN_ALL_HEAPS                                | DOTNET - Bytes In All Heaps                              |
| QOS_EXCHANGE_NETWORK_KILOBYTES_TOTAL_PER_SECOND                                | \$HOST                                                   |
| QOS_EXCHANGE_NETWORK_PACKETS_OUTBOUND_ERRORS                                   | Packet Outbound Errors                                   |
| QOS_EXCHANGE_NETWORK_TCPV4_CONNECTIONS_ESTABLISHED                             | TCPv4 Connections Established                            |

|                                                |                           |
|------------------------------------------------|---------------------------|
| QOS_EXCHANGE_NETWORK_TCPV6_CONNECTION_FAILURES | TCPv6 Connection Failures |
|------------------------------------------------|---------------------------|

### Processor Counters Exchange 2010

| Column                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                      | Name of the host where the Exchange server is installed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Processor User Time       | Percentage of processor time spent in user mode. User mode is a restricted processing mode designed for applications, environment subsystems, and integral subsystems.<br>0 to 74.99 = Green<br>75 = Red                                                                                                                                                                                                                                                                                                                                           |
| Processor Privileged Time | Percentage of processor time spent in privileged mode. Privileged mode is a processing mode designed for operating system components and hardware-manipulating drivers. It allows direct access to hardware and all memory.<br>0 to 74.99 = Green<br>75 = Red                                                                                                                                                                                                                                                                                      |
| Processor Queue Length    | Number of threads each processor is servicing. Processor queue length can be used to identify whether processor contention or high CPU utilization is caused by the processor capacity being insufficient to handle the workload assigned to it.<br>Processor Queue Length shows the number of threads that are delayed in the Processor Ready Queue and are waiting to be scheduled for execution. The listed value is the last observed value at the time the measurement was taken.<br>0 to 2.99 = Green<br>3.00 to 4.99 = Orange<br>5.00 = Red |
| Processor Time Instance   | Percentage of time that the processor is executing application or operating system processes. This is when the processor is not idle.                                                                                                                                                                                                                                                                                                                                                                                                              |

### Memory Performance Exchange 2010

| Column              | Description                                                                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                | Name of the host where the Exchange server is installed.                                                                                                                          |
| Available Megabytes | Amount of physical memory immediately available for allocation to a process or for system use.<br>0 to 49.99 = Red<br>50 to 75.99 = Orange<br>76 to 99.99 = Yellow<br>100 = Green |
| Pool Paged Bytes    | The portion of shared system memory that can be paged to the disk paging file.                                                                                                    |
| Pool Nonpaged Bytes | System virtual addresses guaranteed to be resident in physical memory at all times and can thus be accessed from any address space without incurring paging input/output (I/O).   |
| Cache Bytes         | Size, in bytes, of the file system cache.                                                                                                                                         |

**Transport Queues Exchange 2010**

| Column                               | Description                                                                                                                                                                |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                                 | Name of the host where the Exchange server is installed.                                                                                                                   |
| Aggregate Delivery Queue Length      | Total number of items queued for delivery in all queues.<br>0.00 to 1500.99 = Green<br>1501.00 to 3000.99 = Yellow<br>3001.00 to 4000.99 = Orange<br>4001.00 to 5000 = Red |
| Active Mailbox Delivery Queue Length | Number of items in the active mailbox queues.<br>0 to 100 = Green<br>101 to 200 = Yellow<br>201 to 249 = Orange<br>250 = Red                                               |
| Retry Mailbox Delivery               | Number of items in the retry mailbox queues.<br>0 to 50 = Green<br>51 to 74 = Yellow<br>75 to 99 = Orange<br>100 = Red                                                     |
| Unreachable Queue Length             | Number of items in the unreachable queues.<br>0 to 49 = Green<br>50 to 74 = Yellow<br>75 to 99 = Orange<br>100 = Red                                                       |
| Poison Queue Length                  | Number of items in the poison queue.<br>0.00 to 0.00 = Green<br>0.01 = Red                                                                                                 |
| Messages Submitted per Second        | Rate that messages are submitted by clients.                                                                                                                               |
| Messages Completed Delivery/Sec      | Rate that messages are delivered to all recipients.                                                                                                                        |

**Exchange 2010 Domain Controllers Connectivity Counters**

| Column                              | Description                                                                                                                                                                                     |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                                | Name of the host where the Exchange server is installed.                                                                                                                                        |
| Searches/Second                     | Number of LDAP search requests issued per second.                                                                                                                                               |
| Searches Timed Out/Minute           | Number of LDAP searches that returned LDAP_Timeout during the last minute.<br>0 to 2.99 = Green<br>3 to 6.99 = Yellow<br>7 to 9.99 = Orange<br>10 = Red                                         |
| Long Running LDAP Operations/Minute | Number of LDAP operations on this domain controller that took longer than the specified threshold per minute.<br>0 to 14.99 = Green<br>15 to 24.99 = Yellow<br>25 to 49.99 = Orange<br>50 = Red |

**Network Counters Exchange 2010**

| Column                        | Description                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                          | Name of the host where the Exchange server is installed.                                                                                                                                                                                     |
| TCPv4 Connections Established | Number of TCP connections for which the state is either ESTABLISHED or CLOSE-WAIT. The number of TCP connections is constrained by the size of the nonpaged pool. When the nonpaged pool is depleted, no new connections can be established. |
| TCPv6 Connection Failures     | Number of TCP connections for which the state is either ESTABLISHED or CLOSE-WAIT. The number of TCP connections is constrained by the size of the nonpaged pool. When the nonpaged pool is depleted, no new connections can be established. |

**Read Time Processes**

| Column    | Description                                                                                  |
|-----------|----------------------------------------------------------------------------------------------|
| Host      | Name of the host where the Exchange server is installed.                                     |
| Process   | Target that is being monitored.                                                              |
| Read Time | Time to send an LDAP read request to the specified domain controller and receive a response. |

**Search Time Processes**

| Column      | Description                                                 |
|-------------|-------------------------------------------------------------|
| Host        | Name of the host where the Exchange server is installed.    |
| Process     | Target that is being monitored.                             |
| Search Time | Time to send an LDAP search request and receive a response. |

**.NET time in GC**

| Column  | Description                                                                                                                                                                                                |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host    | Name of the host where the Exchange server is installed.                                                                                                                                                   |
| Process | Target that is being monitored.                                                                                                                                                                            |
| Time    | When garbage collection has occurred. When the counter exceeds the threshold, the CPU is cleaning up and is not being used efficiently for load. Adding memory to the server would improve this situation. |

**.NET Exceptions Per Second**

| Column         | Description                                                                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host           | Name of the host where the Exchange server is installed.                                                                                                         |
| Process        | Target that is being monitored.                                                                                                                                  |
| Exceptions/sec | Number of exceptions thrown per second. These include both .NET framework exceptions and unmanaged exceptions that are converted into .NET framework exceptions. |

**.NET Bytes in All Heaps**

| Column  | Description                                              |
|---------|----------------------------------------------------------|
| Host    | Name of the host where the Exchange server is installed. |
| Process | Target that is being monitored.                          |
| Bytes   | Memory allocated in bytes on the GC heaps.               |

**MS Exchange 2013 Unified Dashboard**

The MS Exchange Server 2013 Unified Dashboard provides pre-defined list views with information about your Microsoft Exchange server 2013, such as processor, memory performance, transport queues, domain controllers, .Net framework, and network counters.

**Contents****NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**MS Exchange 2013 Required Data Sources**

The MS Exchange 2013 Unified Dashboard requires these probes:

- exchange\_monitor
- exchange\_monitor\_backend
- perfmon
- processes
- ntevl

This table lists the QoS metrics and subkeys or targets that must be activated to populate data in the MS Exchange 2013 dashboard.

| QoS Required                                       | Subkey/Target                       |
|----------------------------------------------------|-------------------------------------|
| QOS_EXCHANGE_MEMORY_POOL_PAGED_BYTES               | Pool Paged Bytes                    |
| QOS_EXCHANGE_MEMORY_CACHE_BYTES                    | Cache Bytes                         |
| QOS_EXCHANGE_PROCESSOR_USER_TIME                   | User Time                           |
| QOS_EXCHANGE_PROCESSOR_PRIVILEGED_TIME             | Privileged Time                     |
| QOS_EXCHANGE_PROCESSOR_PROCESSOR_QUEUE_LENGTH      | Processor Queue Length              |
| QOS_EXCHANGE_PROCESSOR_PROCESSOR_TIME_INSTANCE     | Processor Time Instance (processes) |
| QOS_EXCHANGE_NETWORK_TCPV4_CONNECTIONS_ESTABLISHED | TCPv4 Connections Established       |
| QOS_EXCHANGE_NETWORK_TCPV6_CONNECTION_FAILURES     | TCPv6 Connection Failures           |
| QOS_EXCHANGE_MSEXCHANGE_LDAP_SEARCHES_PER_SECOND   | LDAP Searches Per Second(0)         |



|                                                                           |                                                 |
|---------------------------------------------------------------------------|-------------------------------------------------|
| QOS_EXCHANGE_MSEXCHANGE_LDAP_SEARCHES_TIMED_OUT_PER_MINUTE                | LDAP Searches Timed Out Per Minute              |
| QOS_EXCHANGE_MSEXCHANGE_LDAP_SEARCH_TIME_PROCESSES                        | LDAP Search Time Processes                      |
| QOS_EXCHANGE_MSEXCHANGE_LDAP_READ_TIME_PROCESSES                          | LDAP Read Time Processes                        |
| QOS_EXCHANGE_MEMORY_DOTNET - TIME_IN_GC                                   | DOTNET Time in GC                               |
| QOS_EXCHANGE_MEMORY_DOTNET - EXCEPTION_THROWN_PER_SEC                     | DOTNET - Exception Thrown Per Sec               |
| QOS_EXCHANGE_MEMORY_PRIVATE_BYTES                                         | Private Bytes                                   |
| QOS_EXCHANGE_MEMORY_VIRTUAL_BYTES                                         | Virtual Bytes                                   |
| QOS_EXCHANGE_MEMORY_DOTNET - BYTES_IN_ALL_HEAPS                           | DOTNET - Bytes In All Heaps                     |
| QOS_EXCHANGE_ANTI_MALWARE_ANTI-MALWARE_AGENT_MESSAGES_CONTAINING_MALWARE  | Anti-Malware Agent Messages Containing Malware  |
| QOS_EXCHANGE_ANTI_MALWARE_ANTI-MALWARE_AGENT_MESSAGES_SCANNED             | Anti-Malware Agent Messages Scanned             |
| QOS_EXCHANGE_TRANS_ROLE_OUTBOUND:_SUBMITTED_MAIL_ITEMS_PER_SECOND-2013    | Submitted Mail Items Per Second                 |
| QOS_EXCHANGE_TRANS_ROLE_INBOUND:_LOCALDELIVERYCALLSPERSECOND-2013         | Local Delivery Calls Per Second                 |
| QOS_EXCHANGE_TRANS_ROLE_MESSAGES_SUBMITTED_PER_SECOND_-_INFORMATION_STORE | Messages Submitted Per Second-Information Store |

**Anti-Malware Agent Messages Scanned**

| Column                              | Description                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------|
| Host                                | Name of the host where the exchange server is installed.                        |
| Process                             | Target that is being monitored.                                                 |
| Anti-Malware Agent Messages Scanned | Scan the messages sent to or received from a mailbox server in the past minute. |

**Anti-Malware Agent Messages Containing Malware**

| Column                              | Description                                                                                        |
|-------------------------------------|----------------------------------------------------------------------------------------------------|
| Host                                | Name of the host where the exchange server is installed.                                           |
| Process                             | Target that is being monitored.                                                                    |
| Anti-Malware Agent Messages Scanned | Number of messages received containing malware. For example, a virus that is filtered in a minute. |

**Messages Submitted Per Second - Information Store**

| Column  | Description                                              |
|---------|----------------------------------------------------------|
| Host    | Name of the host where the exchange server is installed. |
| Process | Target that is being monitored.                          |

|                                                 |                                                                                                      |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Messages Submitted Per Second Information Store | Messages Submitted Per Second is the number of messages enqueued in the submission queue per second. |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------|

### **Local Delivery Calls Per Second**

| Column                              | Description                                                |
|-------------------------------------|------------------------------------------------------------|
| Host                                | Name of the host where the exchange server is installed.   |
| Process                             | Target that is being monitored.                            |
| Anti-Malware Agent Messages Scanned | Displays the number of local delivery attempts per second. |

### **Submitted Mail Items Per Second**

| Column                          | Description                                                            |
|---------------------------------|------------------------------------------------------------------------|
| Host                            | Name of the host where the exchange server is installed.               |
| Process                         | Target that is being monitored.                                        |
| Submitted Mail Items Per Second | Displays the number of mail items that have been submitted per second. |

### **LDAP**

| Column                    | Description                                                                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                      | Name of the host where the Exchange server is installed.                                                                                                |
| Searches/Second           | Number of LDAP search requests issued per second.                                                                                                       |
| Searches Timed Out/Minute | Number of LDAP searches that returned LDAP_Timeout during the last minute.<br>0 to 2.99 = Green<br>3 to 6.99 = Yellow<br>7 to 9.99 = Orange<br>10 = Red |

### **Memory Counters**

| Column           | Description                                                                    |
|------------------|--------------------------------------------------------------------------------|
| Host             | Name of the host where the Exchange server is installed.                       |
| Host             | Name of the host where the Exchange server is installed.                       |
| Pool Paged Bytes | The portion of shared system memory that can be paged to the disk paging file. |
| Cache Bytes      | Size, in bytes, of the file system cache.                                      |

### **Memory Private Bytes**

| Column               | Description                                                                                             |
|----------------------|---------------------------------------------------------------------------------------------------------|
| Host                 | Name of the host where the Exchange server is installed.                                                |
| Process              | Target that is being monitored.                                                                         |
| Memory Private Bytes | Shows the current number of bytes this process has allocated that can't be shared with other processes. |

**Memory Virtual Bytes**

| Column               | Description                                                                              |
|----------------------|------------------------------------------------------------------------------------------|
| Host                 | Name of the host where the Exchange server is installed.                                 |
| Process              | Target that is being monitored.                                                          |
| Memory Virtual Bytes | Represents (in bytes) how much virtual address space the process is currently consuming. |

**Network Counters Exchange 2013**

| Column                        | Description                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                          | Name of the host where the Exchange server is installed.                                                                                                                                                                                     |
| TCPv4 Connections Established | Number of TCP connections for which the state is either ESTABLISHED or CLOSE-WAIT. The number of TCP connections is constrained by the size of the nonpaged pool. When the nonpaged pool is depleted, no new connections can be established. |
| TCPv6 Connection Failures     | Number of TCP connections for which the state is either ESTABLISHED or CLOSE-WAIT. The number of TCP connections is constrained by the size of the nonpaged pool. When the nonpaged pool is depleted, no new connections can be established. |

**Exchange 2013 Processor Counters**

| Column                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                      | Name of the host where the Exchange server is installed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Processor User Time       | Percentage of processor time spent in user mode. User mode is a restricted processing mode designed for applications, environment subsystems, and integral subsystems.<br>0 to 74.99 = Green<br>75 = Red                                                                                                                                                                                                                                                                                                                                        |
| Processor Privileged Time | Percentage of processor time spent in privileged mode. Privileged mode is a processing mode designed for operating system components and hardware-manipulating drivers. It allows direct access to hardware and all memory.<br>0 to 74.99 = Green<br>75 = Red                                                                                                                                                                                                                                                                                   |
| Processor Queue Length    | Number of threads each processor is servicing. Processor queue length can be used to identify whether processor contention or high CPU utilization is caused by the processor capacity being insufficient to handle the workload assigned to it. Processor Queue Length shows the number of threads that are delayed in the Processor Ready Queue and are waiting to be scheduled for execution. The listed value is the last observed value at the time the measurement was taken.<br>0 to 2.99 = Green<br>3.00 to 4.99 = Orange<br>5.00 = Red |
| Processor Time Instance   | Percentage of time that the processor is executing application or operating system processes. This is when the processor is not idle.                                                                                                                                                                                                                                                                                                                                                                                                           |

**Search Time Processes**

| Column      | Description                                                 |
|-------------|-------------------------------------------------------------|
| Host        | Name of the host where the Exchange server is installed.    |
| Process     | Target that is being monitored.                             |
| Search Time | Time to send an LDAP search request and receive a response. |

**Read Time Processes**

| Column    | Description                                                                                  |
|-----------|----------------------------------------------------------------------------------------------|
| Host      | Name of the host where the Exchange server is installed.                                     |
| Process   | Target that is being monitored.                                                              |
| Read Time | Time to send an LDAP read request to the specified domain controller and receive a response. |

**.NET Exceptions Thrown**

| Column         | Description                                                                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host           | Name of the host where the Exchange server is installed.                                                                                                         |
| Process        | Target that is being monitored.                                                                                                                                  |
| Exceptions/sec | Number of exceptions thrown per second. These include both .NET framework exceptions and unmanaged exceptions that are converted into .NET framework exceptions. |

**.NET time in GC**

| Column  | Description                                                                                                                                                                                                |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host    | Name of the host where the Exchange server is installed.                                                                                                                                                   |
| Process | Target that is being monitored.                                                                                                                                                                            |
| Time    | When garbage collection has occurred. When the counter exceeds the threshold, the CPU is cleaning up and is not being used efficiently for load. Adding memory to the server would improve this situation. |

**.NET Bytes in All Heaps**

| Column  | Description                                              |
|---------|----------------------------------------------------------|
| Host    | Name of the host where the Exchange server is installed. |
| Process | Target that is being monitored.                          |
| Bytes   | Memory allocated in bytes on the GC heaps.               |

**MS SharePoint Server Unified Dashboard**

The SharePoint Unified Dashboard provides predefined list views with information about your SharePoint server, such as CPU Performance and Memory usage, network utilization, disk usage and performance, and SQL server statistics.

**Contents**

**NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**SharePoint Required Data Sources**

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the SharePoint dashboard.

| Probe                | QoS Required                                                     | Subkey/Target                                                                               |
|----------------------|------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| sharepoint           | QOS_%_PROCESSOR_TIME                                             | MOSS2007 - CPU Total Processor Time_<br>%Processor Time                                     |
|                      | QOS_PROCESSOR_QUEUE_LENGTH                                       | MOSS2007 - Processor Queue<br>Length_Processor Queue Length                                 |
|                      | QOS_BYTES_TOTAL/SEC                                              | MOSS2007 - Network Interface - Total<br>Bytes_Bytes Total/sec                               |
|                      | QOS_BYTES_SENT/SEC                                               | MOSS2007 - Network Interface - Bytes<br>Sent_Bytes sent/sec                                 |
|                      | QOS_BYTES_RECEIVED/SEC                                           | MOSS2007 - Network Interface - Bytes<br>Received_Bytes Received/sec                         |
|                      | QOS_PACKETS_OUTBOUND_ERRORS                                      | MOSS2007 - Network Interface - Packets<br>Outbound errors_Packets Outbound Errors           |
|                      | QOS_%_USAGE                                                      | MOSS2007 - Paging File: %Usage_<br>%Usage                                                   |
|                      | QOS_%_USAGE_PEAK                                                 | MOSS2007 - Paging File: %Usage Peak_<br>%Usage Peak                                         |
|                      | QOS_AVAILABLE_MBYTES                                             | MOSS2007 - Availability of Memory in<br>Bytes_Available                                     |
|                      | QOS_PAGES/SEC                                                    | MOSS2007 - Memory_Pages Per<br>Second_Pages/sec                                             |
|                      | QOS_CACHE_FAULTS/SEC                                             | MOSS2007 - Cache Faults Per Sec_Cache<br>Faults/sec                                         |
|                      | QOS_PAGE_FAULTS/SEC                                              | MOSS2007 - Page Faults Per<br>Second_Page Faults/sec                                        |
|                      | QOS_BUFFER_CACHE_HIT_RATIO                                       | MOSS2007 - SQL Server: Buffer Manager<br>- Buffer Cache Hit Ratio_Buffer cache hit<br>ratio |
|                      | QOS_CACHE_HIT_RATIO                                              | MOSS2007 - SQL Server: Cache Hit<br>Ratio_Cache Hit Ratio                                   |
|                      | QOS_LATCH_WAITS/SEC                                              | MOSS2007 - SQL Server: Latch Waits/<br>sec_Latch Waits/sec                                  |
|                      | QOS_NUMBER_OF_DEADLOCKS/SEC                                      | MOSS2007 - SQL Server: Number of<br>Deadlocks/sec_Number of Deadlocks/sec                   |
| QOS_USER_CONNECTIONS | MOSS2007 - SQL Server: User<br>Connections_User Connections      |                                                                                             |
| QOS_BYTES_SENT/SEC   | MOSS2007 - Web Service - Bytes Sent Per<br>Second_Bytes Sent/sec |                                                                                             |

|                             |                                                                         |
|-----------------------------|-------------------------------------------------------------------------|
| QOS_CURRENT_CONNECTIONS     | MOSS2007 - Web Service_Current Connections                              |
| QOS_CONNECTION_ATTEMPTS/SEC | MOSS 2007 - Web Service Connection Attempts_Connection Attempts/sec     |
| QOS_%_PROCESSOR_TIME        | MOSS2007 - Process - W3WP Processor Time_%Processor Time                |
| QOS_WORKING_SET             | MOSS2007 - Process - W3WP Working Set_Working Set                       |
| QOS_REQUESTS_EXECUTING      | MOSS2007 - ASP.NET Applications - Requests Executing_Requests Executing |
| QOS_REQUEST_WAIT_TIME       | MOSS2007 - ASP.NET Applications - Requests Wait Time_Request Wait Time  |
| QOS_REQUESTS/SEC            | MOSS2007 - ASP.NET Applications_Requests/sec                            |
| QOS_REQUESTS_REJECTED       | MOSS2007 - ASP.NET Applications - Requests Rejected_requests Rejected   |

### **CPU Performance**

| Column                 | Description                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Host                   | Name of the host where the SharePoint server is installed.                                                                               |
| Processor Time Perc    | Percentage of elapsed time the processor spends to execute a non-idle thread.<br>0 to 70 = Green<br>71 to 79 = Yellow<br>80 to 100 = Red |
| Processor Queue Length | If the threshold of this rule is exceeded, the processor is not fast enough.                                                             |

### **Memory Usage and Performance**

| Column                                    | Description                                                                                                                                                                                                                                                                                    |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                                      | Name of the host where the SharePoint server is installed.                                                                                                                                                                                                                                     |
| Paging File Perc Usage and Perc used Peak | The server paging file, sometimes called the swap file, holds virtual memory addresses on disk. Page faults occur when a process has to stop and wait while required virtual resources are retrieved from disk into memory.<br>Page faults are more frequent if physical memory is inadequate. |
| Avail MB                                  | Amount of physical memory, in megabytes, immediately available for allocation to a process or for system use.<br>Insufficient memory leads to excessive use of the page file and an increase in the number of page faults per second.                                                          |
| Pages/sec                                 | Rate at which the pages are read from or written to disk to resolve hard page faults. A large number indicates system-wide performance problems.<br>0 to 7 = Green<br>8 to 9 = Yellow<br>10 = Red                                                                                              |

|                  |                                                                                                                                                                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cache Faults/sec | Rate at which faults occur when a page is sought in the file system cache and is not found. This may be a soft fault when the page is found in memory or a hard fault when the page is on the disk.<br>0.0 to 0.99 = Green<br>1.0 = Red |
| Page Faults/sec  | Number of times data was not found in memory. It measures the average number of pages faulted per second.                                                                                                                               |

## ASP.NET

| Column             | Description                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host               | Name of the host where the SharePoint server is installed.                                                                                                                                                                                                                                |
| Requests Executing | Number of requests currently executing.                                                                                                                                                                                                                                                   |
| Request Wait Time  | Number of milliseconds that the most recent request waited in the queue for processing. As the number of wait events increases, users experience degraded page-rendering performance.                                                                                                     |
| Requests/sec       | Number of requests executed per second. This represents the current throughput of the application. Under constant load, this number should remain within a certain range, barring other server work (such as garbage collection, cache cleanup thread, external server tools, and so on). |
| Req Queued         | Number of requests waiting to be processed.<br>0 to 300 = Green<br>301 to 500 = Yellow<br>501 = Red                                                                                                                                                                                       |
| Requests Rejected  | Total number of requests not executed because of insufficient server resources to process them. This counter represents the number of requests that return a 503 HTTP status code, indicating the server is too busy.                                                                     |

## Network Utilization

| Column                 | Description                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Host                   | Name of the host where the SharePoint server is installed.                                                                              |
| Bytes Total/sec        | Rate at which the data is sent and received via the Network Interface Card.<br>0 to 39.9 = Green<br>40.0 to 49.9 = Yellow<br>50.0 = Red |
| Bytes Recd/sec         | Rate at which data bytes are received by the web service.                                                                               |
| Bytes Sent/sec         | Rate at which data bytes are sent by the web service.                                                                                   |
| Packet Outbound Errors | Number of outbound packets that could not be transmitted because of errors.                                                             |

## Disk Usage and Performance

| Column     | Description                                                |
|------------|------------------------------------------------------------|
| Host       | Name of the host where the SharePoint server is installed. |
| Writes/sec | Number of writes to disk per second.                       |

|                       |                                                                                           |
|-----------------------|-------------------------------------------------------------------------------------------|
| Reads/sec             | Number of reads to disk per second.                                                       |
| Perc Idle Time        | Percentage of time the disk system was not processing requests and no work was queued.    |
| Avg Write Q Length    | Average number of write requests that are queued.                                         |
| Avg Read Q Length     | Average number of read requests that are queued.                                          |
| Avg Disk sec/Transfer | Number of read and writes completed per second, regardless of how much data they involve. |

### **SQL Server Statistics**

| Column                 | Description                                                                                                                                                                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                   | Name of the host where the SharePoint server is installed.                                                                                                                                                                                                                             |
| Buffer Cache Hit Ratio | Percentage of pages found in the buffer cache without having to read from disk.<br>The ratio is the total number of cache hits divided by the total number of cache lookups since an instance of SQL Server was started.<br>0.0 to 60.9 = Red<br>61.0 to 89.0 = Yellow<br>90.0 = Green |
| Cache Hit Ratio        | Ratio between cache hits and lookups for plans.                                                                                                                                                                                                                                        |
| Latch Waits/sec        | Number of latch requests per second that could not be granted immediately.                                                                                                                                                                                                             |
| Deadlocks/sec          | Number of deadlocks on the SQL Server per second.                                                                                                                                                                                                                                      |
| User Connections       | Number of user connections on your instance of SQL Server.                                                                                                                                                                                                                             |

### **W3WP Process**

| Column         | Description                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Host           | Name of the host where the SharePoint server is installed.                                                                        |
| Proc Time Perc | Percent of elapsed time that all process threads use the processor.<br>0.0 to 49.0 = Green<br>49.1 to 74.9 = Yellow<br>75.0 = Red |
| Working Set    | The set of memory pages recently touched by the threads in the process.<br>0 to 79.0 = Green<br>80.0 = Red                        |

### **Web Front End Server**

| Column              | Description                                                 |
|---------------------|-------------------------------------------------------------|
| Host                | Name of the host where the SharePoint server is installed.  |
| Bytes Sent/sec      | Rate at which data bytes are sent by the web service.       |
| Current Connections | Monitors current IIS connections.                           |
| Connection Attempts | Rate at which connections to the web service are attempted. |



## MS SQL Server Unified Dashboard

The MS SQL Server Unified Dashboard provides predefined list views with information about your MS SQL server, such as load, locks, performance reports and list designer, server processes, database performance and user statistics.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### MS SQL Server Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the MS SQL Server dashboard.

| Probe     | QoS                                        | Subkey/Target              |
|-----------|--------------------------------------------|----------------------------|
| sqlserver | QOS_SQLSERVER_FG_FREESPACE_WITH_AVAIL_DISK | Free Space with Avail Disk |
|           | QOS_SQLSERVER_ACTIVE_USERS                 | *                          |
|           | QOS_SQLSERVER_BLOCKED_USERS                | *                          |
|           | QOS_SQLSERVER_BUF_CACHEHIT_RATIO           | *                          |
|           | QOS_SQLSERVER_CHECK_DBALIVE                | *                          |
|           | QOS_SQLSERVER_FREE_SPACE                   | Free Space                 |
|           | QOS_SQLSERVER_LOCK_REQUESTS                | *                          |
|           | QOS_SQLSERVER_LOCK_TIMEOUTS                | *                          |
|           | QOS_SQLSERVER_LOCK_WAITS                   | *                          |
|           | QOS_SQLSERVER_LOGIN_COUNT                  | *                          |
|           | QOS_SQLSERVER_SERVER_CPU                   | Server CPU                 |
|           | QOS_SQLSERVER_SERVER_STARTUP               | *                          |
|           | QOS_SQLSERVER_TRANSACTIONS                 | *                          |
|           | QOS_SQLSERVER_USER_CPU                     | User CPU                   |
| cdm       | QOS_CPU_USAGE                              | *                          |
|           | QOS_PROC_QUEUE_LEN                         | *                          |
| processes | QOS_PROCESS_CPU                            | *                          |
|           | QOS_PROCESS_MEMORY                         | *                          |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

### Database Performance

| Column | Description                                         |
|--------|-----------------------------------------------------|
| Host   | Name of the host where the SQL server is installed. |

|                        |                                                                                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status                 | Monitors connectivity to the database instance. The different status are: <ul style="list-style-type: none"> <li>• Connection Up = Green</li> <li>• Connection Down = Red</li> </ul>                                         |
| Buffer Cache Hit Ratio | Monitors the buffer cache-hit ratio. The different thresholds are: <ul style="list-style-type: none"> <li>0 to 50.99 = Red</li> <li>51 to 74.99 = Orange</li> <li>75 to 84.99 = Yellow</li> <li>85 to 100 = Green</li> </ul> |
| Uptime                 | Monitors the uptime (in days) of the database server.                                                                                                                                                                        |
| Server CPU             | Monitors CPU usage by the database in a monitoring interval.                                                                                                                                                                 |

### **FG Free Space with Available Disk**

| Column                            | Description                                                                  |
|-----------------------------------|------------------------------------------------------------------------------|
| Host                              | Name of the host where the SQL server is installed.                          |
| FG Free Space with Available Disk | Monitors free space in filegroups after considering the available disk size. |

### **Free Space**

| Column     | Description                                         |
|------------|-----------------------------------------------------|
| Host       | Name of the host where the SQL server is installed. |
| Free Space | Monitors free space in filegroups.                  |

### **Locks**

| Column        | Description                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host          | Name of the host where the SQL server is installed.                                                                                                                                                    |
| Lock Waits    | Monitors number of lock waits per second.                                                                                                                                                              |
| Lock Requests | Monitors number of lock requests per second.                                                                                                                                                           |
| Lock Timeouts | Monitors number of lock-timeouts per second. The different thresholds are: <ul style="list-style-type: none"> <li>0 to .79 = Green</li> <li>.8 to .99 = Yellow</li> <li>1 and greater = Red</li> </ul> |

### **Processes**

| Column       | Description                                                                        |
|--------------|------------------------------------------------------------------------------------|
| Server       | Name of the host where the SQL server is installed.                                |
| Process Name | Name of the SQL server process.                                                    |
| CPU          | Percent of CPU consumed by the SQL server process in the last hour.                |
| Memory       | Number of kilobytes of memory consumed by the SQL server process in the last hour. |

**NOTE**

To monitor data in the Processes view, create a profile in the **processes** probe and configure it to monitor CPU and Memory QoS values.

**Server Load**

| Column                          | Description                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                            | Host name of the robot where the <b>cdm</b> probe is deployed.                                                                                                                                  |
| Processor Queue Length 1 hr avg | Average load of the system in the last hour.                                                                                                                                                    |
| Current CPU Usage               | Percentage of CPU used by the system. The different thresholds are: <ul style="list-style-type: none"> <li>• 0 to 80 = Green</li> <li>• 80 to 90 = Orange</li> <li>• 90 to 100 = Red</li> </ul> |

**Transactions**

| Column       | Description                                           |
|--------------|-------------------------------------------------------|
| Host         | Name of the host where the SQL server is installed.   |
| Transactions | Monitors the number of transactions in the past hour. |

**User CPU**

| Column   | Description                                         |
|----------|-----------------------------------------------------|
| Host     | Name of the host where the SQL server is installed. |
| User CPU | Monitors percentage of CPU Usage by user.           |

**User Statistics**

| Column        | Description                                                    |
|---------------|----------------------------------------------------------------|
| Host          | Name of the host where the SQL server is installed.            |
| Active Users  | Monitors the number of active user per database.               |
| Blocked Users | Monitors the number of users blocked.                          |
| Login Count   | Monitors the number of users currently logged into the server. |

**NETAPP ONTAP Unified Dashboard**

The netapp\_ontap Unified Dashboard provides predefined list views to monitor the health and performance of storage objects such as disks, volumes, and aggregates and storage systems running Data ONTAP 8.3x version in Cluster mode.

**Contents****NOTE**

: If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS

metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**NETAPP ONTAP Required Data Sources**

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the NETAPP ONTAP dashboard. An asterisk (\*) means that this QoS brings data for all targets for which it is applicable.

| QoS                                      | Subkey/Target |
|------------------------------------------|---------------|
| QOS_STORAGE_CPU_UTILIZATION              | *             |
| QOS_STORAGE_TOTAL_IOPS                   | *             |
| QOS_STORAGE_TOTAL_AVERAGE_LATENCY        | *             |
| QOS_STORAGE_TOTAL_CAPACITY_AGGR          | *             |
| QOS_STORAGE_USED_CAPACITY_AGGR           | *             |
| QOS_STORAGE_FREE_CAPACITY_AGGR           | *             |
| QOS_STORAGE_PERCENT_CAPACITY_USED_AGGR   | *             |
| QOS_STORAGE_PERCENT_CAPACITY_FREE_AGGR   | *             |
| QOS_STORAGE_TOTAL_SNAPSHOT_CAPACITY_AGGR | *             |
| QOS_STORAGE_SNAPSHOT_USED_CAPACITY_AGGR  | *             |
| QOS_STORAGE_SNAPSHOT_FREE_CAPACITY_AGGR  | *             |
| QOS_STORAGE_PERCENT_SNAPSHOT_USED_AGGR   | *             |
| QOS_STORAGE_PERCENT_SNAPSHOT_FREE_AGGR   | *             |
| QOS_STORAGE_ENV_OVER_TEMPERATURE_STATUS  | *             |
| QOS_STORAGE_FAILED_FAN                   | *             |
| QOS_STORAGE_FAILED_POWER_SUPPLY_COUNT    | *             |
| QOS_STORAGE_NVRAM_BATTERY_STATUS         | *             |
| QOS_STORAGE_TOTAL_DISK_COUNT             | *             |
| QOS_STORAGE_NUMBER_OF_FAILED_DISKS       | *             |
| QOS_STORAGE_NUM_OF_HOT_SPARES            | *             |
| QOS_STORAGE_TOTAL_RAW_CAPACITY           | *             |
| QOS_STORAGE_OPERATIONAL_STATUS_INTERFACE | *             |
| QOS_STORAGE_LUN_IOPS                     | *             |
| QOS_STORAGE_LUN_OTHER_IOPS               | *             |
| QOS_STORAGE_LUN_READ_IOPS                | *             |
| QOS_STORAGE_LUN_WRITE_IOPS               | *             |
| QOS_STORAGE_LUN_AVG_LATENCY              | *             |
| QOS_STORAGE_LUN_AVG_OTHER_LATENCY        | *             |
| QOS_STORAGE_LUN_AVG_READ_LATENCY         | *             |
| QOS_STORAGE_LUN_AVG_WRITE_LATENCY        | *             |
| QOS_STORAGE_LUN_ERROR_COUNT              | *             |
| QOS_STORAGE_LUN_ONLINE                   | *             |
| QOS_STORAGE_LUN_PERCENT_USED             | *             |
| QOS_STORAGE_LUN_READ_BYTES               | *             |

| QoS                                     | Subkey/Target |
|-----------------------------------------|---------------|
| QOS_STORAGE_LUN_TOTAL_SIZE              | *             |
| QOS_STORAGE_LUN_SIZE_USED               | *             |
| QOS_STORAGE_LUN_WRITE_BYTES             | *             |
| QOS_STORAGE_STATUS_QTREE                | *             |
| QOS_STORAGE_DISK_UTILIZATION            | *             |
| QOS_STORAGE_VSERVER_STATE               | *             |
| QOS_STORAGE_VOLUME_STATUS               | *             |
| QOS_STORAGE_TOTAL_CAPACITY_VOL          | *             |
| QOS_STORAGE_USED_CAPACITY_VOL           | *             |
| QOS_STORAGE_FREE_CAPACITY_VOL           | *             |
| QOS_STORAGE_PERCENT_CAPACITY_USED_VOL   | *             |
| QOS_STORAGE_TOTAL_SNAPSHOT_CAPACITY_VOL | *             |
| QOS_STORAGE_SNAPSHOT_USED_CAPACITY_VOL  | *             |
| QOS_STORAGE_SNAPSHOT_FREE_CAPACITY_VOL  | *             |
| QOS_STORAGE_PERCENT_SNAPSHOT_USED_VOL   | *             |

For more information about configuring probes, see the documentation for each probe.

### **System Statistics Summary**

This table displays information about all system statistics that are being monitored.

| Column Name           | Description                                                                                                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| CPU Utilization       | The percent of time that the CPU has been doing useful work since the last time a client requested the CPU Busy Time Percent. |
| Total IOPS            | The total operations per second.                                                                                              |
| Total Average Latency | The average latency for all operations in the system in milliseconds.                                                         |

### **Aggregate Summary**

This table displays information about the aggregates on the NetApp Storage system.

| Column Name                    | Description                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------|
| Total Capacity                 | The total capacity for the referenced file system.                                      |
| Used Capacity                  | The used capacity for the referenced file system.                                       |
| Free Capacity                  | The free capacity for the referenced file system.                                       |
| Used Capacity Percent          | The used capacity inpercentage for the referenced file system.                          |
| Free Capacity Percent          | The free capacity inpercentage for the referenced file system.                          |
| Snapshot Total Capacity        | The total capacity for the snapshot on the referenced file system.                      |
| Snapshot Used Capacity         | The used capacity for the snapshot on the referenced file system.                       |
| Snapshot Free Capacity         | The free capacity for the snapshot on the referenced file system.                       |
| Snapshot Percent Used Capacity | The total used disk space for the snapshot in percentage on the referenced file system. |

| Column Name                    | Description                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------|
| Snapshot Percent Free Capacity | The total free disk space for the snapshot in percentage on the referenced file system. |

### **Controller Summary**

This table displays information about the controllers on the NetApp Storage system.

| Column Name               | Description                                                                                                                                                                                                                                                                                                                          |     |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Over Temperature Status   | The current state of the hardware whether it is currently operating outside of its recommended temperature range. The possible values are [0 (within recommended temperature range) and 1 (outside recommended temperature range)].                                                                                                  |     |
| Fans Outside RPM Count    | The number of chassis fans that are not operating within the recommended RPM range.                                                                                                                                                                                                                                                  |     |
| Failed Power Supply count | The number of power supplies that are in degraded mode.                                                                                                                                                                                                                                                                              |     |
| NVRAM Battery Status      | The current status of the NVRAM battery or batteries. The possible values are [0 (battery_ok), 1 (battery_partially_discharged), 2 (battery_fully_discharged) and 3 (battery_not_present), 4 (battery_near_end_of_life), 5 (battery_at_end_of_life), 6 (battery_unknown), 7 (battery_over_charged), and, 8 (battery_fully_charged)]. | 1.0 |

### **Disk Summary**

This table displays information about the disks on the NetApp Storage system.

| Column Name        | Description                                    |
|--------------------|------------------------------------------------|
| Total Disk Count   | The total number of disks on the system.       |
| Failed Disk Count  | The number of disks that are currently broken. |
| Spare Disk Count   | The number of available spare disks.           |
| Total Raw Capacity | The total raw capacity of the system.          |

### **Ethernet Interface Summary**

This table displays information about the status of the Ethernet Interfaces on the NetApp Storage system.

| Column Name        | Description                                                                 |
|--------------------|-----------------------------------------------------------------------------|
| Operational Status | The status of the interface. The possible values are [0 (Up) and 1 (Down)]. |

**LUN IOPS and Latency Summary**

This table displays information about LUN IOPS and Latency on the NetApp Storage system.

| Column Name               | Description                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| LUN IOPS                  | The total number of Target side SCSI operations for this LUN since the statistics were last reset.                            |
| LUN Other IOPS            | The total number of Target side SCSI operations that are not read or write for this LUN since the statistics were last reset. |
| LUN Read IOPS             | The total number of Target side SCSI read operations for this LUN since the statistics were last reset.                       |
| LUN Write IOPS            | The total number of Target side SCSI write operations for this LUN since the statistics were last reset.                      |
| LUN Average Latency       | The average latency for all operations in the system in milliseconds.                                                         |
| LUN Average Other Latency | The average latency for all other operations in the system in milliseconds.                                                   |
| LUN Average Read Latency  | The average latency for all read operations in the system in milliseconds.                                                    |
| LUN Average Write Latency | The average latency for all write operations in the system in milliseconds.                                                   |

**LUN Summary**

This table displays information about LUN performance on the NetApp Storage system.

| Column Name      | Description                                                                         |
|------------------|-------------------------------------------------------------------------------------|
| LUN Error Count  | The total number of errors seen on this LUN since the statistics were last reset.   |
| LUN Online       | Whether the LUN is online. The possible values are [0 (Online), 1 (Offline)].       |
| LUN Percent Used | The percent utilization for the LUN.                                                |
| LUN Read Bytes   | The total number of bytes read from this LUN since the statistics were last reset.  |
| LUN Size         | The total size of the LUN.                                                          |
| LUN Size Used    | The size used in GB that is in use on the LUN.                                      |
| LUN Write Bytes  | The total number of bytes written to this LUN since the statistics were last reset. |

**Qtree Summary**

This table displays information about Qtree performance on the NetApp Storage system.

| Column Name  | Description                                                                    |
|--------------|--------------------------------------------------------------------------------|
| Qtree Status | The status of the qtree. The possible values are [0 (Normal) and 1 (Readonly)] |

### **Used Disk Performance Summary**

This table displays information about used disk performance on the NetApp Storage system.

| Column Name      | Description                                                   |
|------------------|---------------------------------------------------------------|
| Disk Utilization | The disk utilization percentage on the referenced disk drive. |

### **vServer Summary**

This table displays information about vServer performance on the NetApp Storage system.

| Column Name    | Description                                                                                                                                   |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| vServer Status | The status of the vServer. The possible values are [0 (Running), 1 (Stopped), 2 (Starting), 3 (Stopping), 4 (Initializing), and 5(Deleting)]. |

### **Volume Summary**

This table displays information about Virtual Volumes performance on the NetApp Storage system.

| Column Name             | Description                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------|
| Volume Status           | The status of the volume. The possible values are [0 (Online), 1 (Offline), 2 (Restricted) and 3 (mixed)]. |
| Total Capacity          | The total capacity of the volume.                                                                          |
| Used Capacity           | The used capacity of the volume.                                                                           |
| Free Capacity           | The total capacity that is free for use on the volume.                                                     |
| Percent Capacity Used   | The total used capacity in percentage on the volume.                                                       |
| Total Snapshot Capacity | The total capacity for the snapshot in the volume.                                                         |
| Snapshot Used Capacity  | The used capacity for the snapshot in the volume.                                                          |
| Snapshot Free Capacity  | The free capacity available in the volume and the snapshot reserve.                                        |
| Percent Snapshot Used   | The used capacity in percentage for the snapshot in the volume.                                            |

## **Network Unified Dashboard**

The Network Unified Dashboard provides predefined list views with information about your network performance.

### **Contents**

#### **NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.



**Network Required Data Sources**

The table contains the probes and QoS metrics required for the preconfigured Network dashboard.

| Probe             | QoS Required                      |
|-------------------|-----------------------------------|
| interface_traffic | QOS_INTERFACE_TRAFFIC_PERC        |
| net_connect       | QOS_NET_CONNECT                   |
| url_response      | QOS_URL_RESPONSE                  |
| cisco_monitor     | QOS_MEMORY_USAGE<br>QOS_CPU_USAGE |

**Web Site Response Time**

| Column         | Description                                                                                                |
|----------------|------------------------------------------------------------------------------------------------------------|
| Monitored From | Name of the host with the url_response probe that is monitoring web site response time.                    |
| Profile Name   | Name of the profile configured in the url_response probes. Typically this is the name of the web site.     |
| Resp Time      | Average time, in milliseconds, to receive a response to an HTTP GET request during the last hour.          |
| Resp Time      | Graph of average time, in milliseconds, to receive a response to an HTTP GET request during the last hour. |
| Alarm          | Alarms generated by the url_response probe, if any.                                                        |

**Cisco Device Health**

| Column      | Description                                                               |
|-------------|---------------------------------------------------------------------------|
| Host        | IP address of the Cisco device.                                           |
| Memory Used | Last reported number of megabytes of memory consumed by the Cisco device. |
| Memory Free | Last reported number of megabytes of memory available.                    |
| CPU Usage   | Last reported percent of CPU consumed by the Cisco device.                |

**Ping Response Time**

| Column              | Description                                                                        |
|---------------------|------------------------------------------------------------------------------------|
| Monitored From Host | Name of the host with the net_connect probe that is monitoring ping response time. |
| Host:Port           | Name of the host and port number that the ping request was sent to.                |
| Response Time       | Last reported time, in milliseconds, to receive a response to the ping request.    |

**Interface Bandwidth**

| Column | Description                                        |
|--------|----------------------------------------------------|
| Device | Name of the device where the interface is located. |

|           |                                                                                                                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Origin    | QoS data from probes is tagged with a name to identify the origin of the data. The origin name is set in the controller probe GUI. If the origin name is not set, the hub name is used. |
| Interface | Type of interface.                                                                                                                                                                      |
| Bandwidth | Last reported percent of bandwidth consumed by traffic on the interface.                                                                                                                |

## Nutanix Clusters Unified Dashboard

The Nutanix Clusters Unified Dashboard provides predefined list views for monitoring clusters in a Nutanix virtualization environment.

### Contents

#### **Required Data Sources in the nutanix\_monitor Probe**

The following table contains the monitors that you must activate in the nutanix\_monitor probe to see data in the Nutanix Clusters Unified Dashboard. You can quickly enable these monitors in the nutanix\_monitor probe by applying a copy of the Nutanix Factory Template in the probe configuration.

| Dashboard Chart                 | QoS                                   | Target/Source |
|---------------------------------|---------------------------------------|---------------|
| Nutanix Cluster Summary         | QOS_NUTANIX_CLUSTER_HOST_COUNT        | Host          |
| Nutanix Cluster Summary         | QOS_NUTANIX_CLUSTER_NUMBER_VMS        | Host          |
| Nutanix Cluster Summary         | QOS_NUTANIX_CLUSTER_VMs_ON            | Host          |
| Nutanix Cluster Summary         | QOS_NUTANIX_CLUSTER_VMs_Off           | Host          |
| Nutanix Cluster Summary         | QOS_NUTANIX_CLUSTER_CPU_USAGE         | Host          |
| Nutanix Cluster Summary         | QOS_NUTANIX_CLUSTER_MEMORY_USAGE      | Host          |
| Nutanix Cluster Storage Summary | QOS_NUTANIX_CLUSTER_STORAGE_CAPACITY  | Host          |
| Nutanix Cluster Storage Summary | QOS_NUTANIX_CLUSTER_STORAGE_USAGE     | Host          |
| Nutanix Cluster Storage Summary | QOS_NUTANIX_CLUSTER_STORAGE_USAGE_PCT | Host          |
| Nutanix Cluster Storage Summary | QOS_NUTANIX_STORAGE_FREE_AMOUNT       | Host          |
| Nutanix Cluster Storage Summary | QOS_NUTANIX_CLUSTER_LATENCY           | Host          |
| Nutanix Cluster Storage Summary | QOS_NUTANIX_CLUSTER_IOPS              | Host          |
| Nutanix Cluster Storage Summary | QOS_NUTANIX_CLUSTER_IO_BW             | Host          |

## Nutanix Cluster Summary

This chart displays information about the resources that are associated with a Nutanix cluster. Use this chart to view information about cluster capacity.

| Column               | Description                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------|
| Host                 | The name of a Nutanix cluster host resource. Click this link to view additional information in OC. |
| Host Count           | The number of hosts in this cluster.                                                               |
| VM Count             | The number of VMs in this cluster.                                                                 |
| VM On Count          | The number of VMs in a cluster with a power state of on.                                           |
| VM Off Count         | The number of VMs in a cluster with a power state of off.                                          |
| Cluster CPU Usage    | The percent CPU usage by the cluster.                                                              |
| Cluster Memory Usage | The percent memory usage by the cluster.                                                           |

## Nutanix Cluster Storage Summary

This chart displays information about storage utilization by a cluster. Use this chart to view information about the clusters with the least amount of storage capacity.

| Column           | Description                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------|
| Host             | The name of a Nutanix cluster host resource. Click this link to view additional information in OC. |
| Storage Capacity | Storage capacity for this cluster in GB.                                                           |
| Storage Usage    | Storage usage for this cluster in GB.                                                              |
| Storage Used Pct | The percentage of storage used by this cluster.                                                    |
| Storage Free     | The amount of free storage for this cluster in GB.                                                 |
| Latency          | The average IO latency in microseconds.                                                            |
| IOPS             | The number of cluster IOs per second.                                                              |
| IO Bandwidth     | The IO Bandwidth in Kbps.                                                                          |

## Nutanix Containers Unified Dashboard

The Nutanix Containers Unified Dashboard provides predefined list views for monitoring containers in a Nutanix virtualization environment.

### Contents

#### Required Data Sources in the nutanix\_monitor Probe

The following table contains the monitors that you must activate in the nutanix\_monitor probe to see data in the Nutanix Containers Unified Dashboard. You can quickly enable these monitors in the nutanix\_monitor probe by applying a copy of the Nutanix Factory Template in the probe configuration.

| Dashboard Chart           | QoS                                  | Target/Source |
|---------------------------|--------------------------------------|---------------|
| Nutanix Container Summary | QOS_NUTANIX_TOTAL_CONTAINER_CAPACITY | *             |
| Nutanix Container Summary | QOS_NUTANIX_TOTAL_CONTAINER_USAGE    | *             |

|                           |                                           |   |
|---------------------------|-------------------------------------------|---|
| Nutanix Container Summary | QOS_NUTANIX_AVERAGE_CONTAINER_LATENCY     | * |
| Nutanix Container Summary | QOS_NUTANIX_AVERAGE_CONTAINER_IOPS        | * |
| Nutanix Container Details | QOS_NUTANIX_CONTAINER_STORAGE_CAPACITY    |   |
| Nutanix Container Details | QOS_NUTANIX_CONTAINER_STORAGE_USED        |   |
| Nutanix Container Details | QOS_NUTANIX_CONTAINER_STORAGE_USAGE       | * |
| Nutanix Container Details | QOS_NUTANIX_CONTAINER_STORAGE_FREE_AMOUNT | * |
| Nutanix Container Details | QOS_NUTANIX_CONTAINER_LATENCY             | * |
| Nutanix Container Details | QOS_NUTANIX_CONTAINER_IOPS                | * |

An asterisk (\*) means that the value for the first entry for the QoS is used.

### **Nutanix Container Details**

This chart displays information about the containers that exist in a Nutanix environment. Use this chart to view information about the availability of a container.

| Column           | Description                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------------------|
| Container        | The name of a Nutanix storage pool and an associated container. Click this link to view additional information in OC. |
| Storage Capacity | The container storage capacity in GBs.                                                                                |
| Storage Used     | The amount of storage in use by the container in GBs.                                                                 |
| Storage Used Pct | The percentage of storage used by this container.                                                                     |
| Storage Free     | The amount of free storage on the container in GBs.                                                                   |
| Latency          | The average IO latency for the container in milliseconds.                                                             |
| IOPS             | The IO latency per second.                                                                                            |

## **Nutanix Disks Unified Dashboard**

The Nutanix Disks Unified Dashboard provides predefined list views for monitoring disks in a Nutanix virtualization environment.

### **Contents**

#### **Required Data Sources in the nutanix\_monitor Probe**

The following table contains the monitors that you must activate in the nutanix\_monitor probe to see data in the Nutanix Disks Unified Dashboard.

| Dashboard Chart                                   | QoS                             | Target/Source |
|---------------------------------------------------|---------------------------------|---------------|
| Nutanix Total Disk Summary (Roll up of all disks) | QOS_NUTANIX_TOTAL_DISK_CAPACITY | *             |
| Nutanix Total Disk Summary (Roll up of all disks) | QOS_NUTANIX_TOTAL_DISK_USED     | *             |
| Nutanix Total Disk Summary (Roll up of all disks) | QOS_NUTANIX_AVERAGE_DISK_USAGE  | *             |

|                      |                           |   |
|----------------------|---------------------------|---|
| Nutanix Disk Details | QOS_NUTANIX_DISK_CAPACITY | * |
| Nutanix Disk Details | QOS_NUTANIX_DISK_USED     | * |
| Nutanix Disk Details | QOS_NUTANIX_DISK_USAGE    | * |
| Nutanix Disk Details | QOS_NUTANIX_DISK_ONLINE   | * |

An asterisk (\*) means that the value for the first entry for the QoS is used.

### **Nutanix Disk Details**

This chart displays information about the disk resources that are associated with a storage pool. Use this chart to view information about current disk usage. You can quickly enable these monitors in the nutanix\_monitor probe by applying a copy of the Nutanix Factory Template in the probe configuration.

| Column           | Description                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Disk             | The ID of the storage pool and an associated disk resource. Click this link to view additional information in OC.             |
| Storage Capacity | The total disk storage capacity in GB.                                                                                        |
| Storage Used     | The amount of disk storage that is used in GB.                                                                                |
| Storage Usage    | The percent disk space that is used by the disk.                                                                              |
| On Line          | Indicates the disk state: <ul style="list-style-type: none"> <li>• Green = 1 - Normal</li> <li>• Red = 0 - Failure</li> </ul> |

## **Nutanix Hosts Unified Dashboard**

The Nutanix Hosts Unified Dashboard provides predefined list views for monitoring the status of hosts in a Nutanix virtualization environment.

### **Contents**

#### **Required Data Sources in the nutanix\_monitor Probe**

The following table contains the monitors that you must activate in the nutanix\_monitor probe to see data in the Nutanix Hosts Unified Dashboard. You can quickly enable these monitors in the nutanix\_monitor probe by applying a copy of the Nutanix Factory Template in the probe configuration.

| Dashboard Chart              | QoS                                  | Target/Source |
|------------------------------|--------------------------------------|---------------|
| Nutanix Host Summary         | QOS_NUTANIX_HOST_NUMBER_VMS          | \$HOST        |
| Nutanix Host Summary         | QOS_NUTANIX_HOST_VMS_CPU_USAGE       | \$HOST        |
| Nutanix Host Summary         | QOS_NUTANIX_HOST_MEMORY_USAGE        | \$HOST        |
| Nutanix Host Storage Summary | QOS_NUTANIX_HOST_STORAGE_CAPACITY    | \$HOST        |
| Nutanix Host Storage Summary | QOS_NUTANIX_HOST_STORAGE_USAGE       | \$HOST        |
| Nutanix Host Storage Summary | QOS_NUTANIX_HOST_STORAGE_FREE_AMOUNT | \$HOST        |

|                              |                                        |        |
|------------------------------|----------------------------------------|--------|
| Nutanix Host Storage Summary | QOS_NUTANIX_HOST_STORAGE_USAG<br>E_PCT | \$HOST |
| Nutanix Host Storage Summary | QOS_NUTANIX_HOST_SSD_USAGE             | \$HOST |
| Nutanix Host Storage Summary | QOS_NUTANIX_HOST_SSD_CAPACITY          | \$HOST |
| Nutanix Host Storage Summary | QOS_NUTANIX_HOST_LATENCY               | \$HOST |
| Nutanix Host Storage Summary | QOS_NUTANIX_HOST_IOPS                  | \$HOST |

### **Nutanix Host Summary**

This chart displays summary information for the resources that are associated with a Nutanix host system. Use this chart to view information about the lowest performing host systems.

| Column            | Description                                                                          |
|-------------------|--------------------------------------------------------------------------------------|
| Host              | The name of the host resource. Click this link to view additional information in OC. |
| VM Count          | The number of VMs on this host.                                                      |
| VM CPU Usage      | The percent CPU usage on the host by VMs.                                            |
| Host Memory Usage | The percent host memory usage.                                                       |

### **Nutanix Host Storage Summary**

This chart displays information about the available storage on a Nutanix host. Use this chart to view information about hosts with low storage.

| Column           | Description                                                                          |
|------------------|--------------------------------------------------------------------------------------|
| Host             | The name of the host resource. Click this link to view additional information in OC. |
| Storage Capacity | The host storage capacity in GBs.                                                    |
| Storage Usage    | The host storage usage in GBs.                                                       |
| Storage Free     | The amount of free storage on the host in GBs.                                       |
| Storage Used Pct | The percentage of storage used by this host.                                         |
| SSD Capacity     | The host storage tier SSD capacity in GBs.                                           |
| SSD Usage        | The host storage tier SSD usage in GBs.                                              |
| Latency          | The average IO latency for the host in milliseconds.                                 |
| IOPS             | The number of input/output operations per second on the host.                        |

## **Nutanix Storage Pools Unified Dashboard**

The Nutanix Storage Pools Unified Dashboard provides predefined list views for monitoring storage pools in a Nutanix virtualization environment.

### **Contents**

### Required Data Sources in the nutanix\_monitor Probe

The following table contains the monitors that you must activate in the nutanix\_monitor probe to see data in the Nutanix Storage Pools Unified Dashboard. You can quickly enable these monitors in the nutanix\_monitor probe by applying a copy of the Nutanix Factory Template in the probe configuration.

| Dashboard Chart                        | QoS                                   | Target/Source |
|----------------------------------------|---------------------------------------|---------------|
| Nutanix Storage Pool Summary           | QOS_NUTANIX_STORAGEPOOLS_CAPACITY     | *             |
| Nutanix Storage Pool Summary           | QOS_NUTANIX_STORAGEPOOLS_USAGE        | *             |
| Nutanix Storage Pool Summary           | QOS_NUTANIX_STORAGEPOOLS_LATENCY      | *             |
| Nutanix Storage Pool Summary           | QOS_NUTANIX_STORAGEPOOLS_IOPS         | *             |
| Nutanix Storage Pool Summary           | QOS_NUTANIX_STORAGEPOOLS_IO_BANDWIDTH | *             |
| Nutanix Storage Pool Disk Summary      | QOS_NUTANIX_TOTAL_DISK_CAPACITY       | *             |
| Nutanix Storage Pool Disk Summary      | QOS_NUTANIX_TOTAL_DISK_USED           | *             |
| Nutanix Storage Pool Disk Summary      | QOS_NUTANIX_AVERAGE_DISK_USAGE        | *             |
| Nutanix Storage Pool Container Summary | QOS_NUTANIX_TOTAL_CONTAINER_CAPACITY  | *             |
| Nutanix Storage Pool Container Summary | QOS_NUTANIX_TOTAL_CONTAINER_USAGE     | *             |
| Nutanix Storage Pool Container Summary | QOS_NUTANIX_AVERAGE_CONTAINER_LATENCY | *             |
| Nutanix Storage Pool Container Summary | QOS_NUTANIX_AVERAGE_CONTAINER_IOPS    | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used.

### Nutanix Storage Pool Summary

This chart displays summary information for a storage pool. Use this chart to view information about storage pool performance.

| Column           | Description                                                                                |
|------------------|--------------------------------------------------------------------------------------------|
| Storage Pool     | The ID of the storage pool resource. Click this link to view additional information in OC. |
| Storage Capacity | The capacity of this storage pool in GBs.                                                  |
| Storage Usage    | The percentage of storage storage that is used for this storage pool.                      |
| Latency          | The average IO latency in milliseconds.                                                    |
| IOPS             | The number of IOs per second to this storage pool.                                         |
| Bandwidth        | The IO bandwidth in Kbps.                                                                  |

### **Nutanix Storage Pool Disk Summary**

This chart displays summary information for all the disks in a storage pool. Use this chart to view information about disk capacity.

| Column              | Description                                                                                |
|---------------------|--------------------------------------------------------------------------------------------|
| Storage Pool        | The ID of the storage pool resource. Click this link to view additional information in OC. |
| Total Disk Capacity | The total capacity for all monitored disks in GBs.                                         |
| Total Disk Used     | The total storage that is used for all monitored disks in GBs.                             |
| Average Disk Usage  | The total percent usage for all monitored disks.                                           |

### **Nutanix Storage Pool Container Summary**

This chart displays summary information for all the containers in a storage pool. Use this chart to view information about container performance.

| Column         | Description                                                                                |
|----------------|--------------------------------------------------------------------------------------------|
| Storage Pool   | The ID of the storage pool resource. Click this link to view additional information in OC. |
| Total Capacity | The total storage capacity for all monitored containers in GBs.                            |
| Total Usage    | The total percent usage for all monitored containers.                                      |
| Latency        | Average container latency for all monitored containers in milliseconds.                    |
| IOPS           | Average number of IOs for all monitored containers in operations per second.               |

## **Nutanix VMs Unified Dashboard**

The Nutanix VMs Unified Dashboard provides predefined list views for monitoring VMs in a Nutanix virtualization environment.

### **Contents**

#### **Required Data Sources in the nutanix\_monitor Probe**

The following table contains the monitors that you must activate in the nutanix\_monitor probe to see data in the Nutanix VMs Unified Dashboard. You can quickly enable these monitors in the nutanix\_monitor probe by applying a copy of the Nutanix Factory Template in the probe configuration.

| Dashboard Chart    | QoS                         | Target/Source |
|--------------------|-----------------------------|---------------|
| Nutanix VM Summary | QOS_NUTANIX_VM_POWER_STATE  | \$HOST        |
| Nutanix VM Summary | QOS_NUTANIX_VM_CPU_USAGE    | \$HOST        |
| Nutanix VM Summary | QOS_NUTANIX_VM_MEMORY_USAGE | \$HOST        |



## Nutanix VM Summary

This chart displays general information about the VMs in a Nutanix environment. Use this chart to view information about VM performance.

| Column       | Description                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| VM           | The name of the VM resource. Click this link to view additional information in OC.                                                      |
| Power State  | Indicates the VM power state: <ul style="list-style-type: none"> <li>Green = On</li> <li>Red = Off</li> <li>Yellow = Unknown</li> </ul> |
| CPU Usage    | The VM CPU usage in bytes.                                                                                                              |
| Memory Usage | The VM percent memory usage.                                                                                                            |

## OpenStack Unified Dashboard

The OpenStack Unified Dashboard provides predefined list views to monitor the health and performance of OpenStack servers.

### NOTE

If your Unified Dashboard is not populating with data, ensure that all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### Contents

### OpenStack Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the OpenStack dashboard. An asterisk (\*) means that this QoS brings data for all targets for which it is applicable.

### NOTE

For more information on configuring probes, see the documentation for each probe.

| QoS                                                 | Subkey/ Target |
|-----------------------------------------------------|----------------|
| QOS_OPENSTACK_AVAILABILITY_ZONE_STATUS              | *              |
| QOS_OPENSTACK_CONTROLLER_NODE_STATUS                | *              |
| QOS_OPENSTACK_CONTROLLER_NODE_SERVICE_STATUS        | *              |
| QOS_OPENSTACK_COMPUTE_NODE_GUEST_COUNT              | *              |
| QOS_OPENSTACK_COMPUTE_NODE_VIRTUAL_CPU_CNT          | *              |
| QOS_OPENSTACK_COMPUTE_NODE_VIRTUAL_CPU_USED_CNT     | *              |
| QOS_OPENSTACK_COMPUTE_NODE_VIRTUAL_CPU_USED_PERCENT | *              |
| QOS_OPENSTACK_COMPUTE_NODE_TOTAL_LOCAL_MEMORY       | *              |

|                                                      |   |
|------------------------------------------------------|---|
| QOS_OPENSTACK_COMPUTE_NODE_FREE_LOCAL_MEMORY         | * |
| QOS_OPENSTACK_COMPUTE_NODE_USED_LOCAL_MEMORY         | * |
| QOS_OPENSTACK_COMPUTE_NODE_LOCAL_MEMORY_USED_PERCENT | * |
| QOS_OPENSTACK_COMPUTE_NODE_TOTAL_LOCAL_DISK          | * |
| QOS_OPENSTACK_COMPUTE_NODE_FREE_LOCAL_DISK           | * |
| QOS_OPENSTACK_COMPUTE_NODE_USED_LOCAL_DISK           | * |
| QOS_OPENSTACK_COMPUTE_NODE_LOCAL_DISK_USED_PERCENT   | * |
| QOS_OPENSTACK_INSTANCE_POWER_STATUS                  | * |
| QOS_OPENSTACK_INSTANCE_STATUS                        | * |
| QOS_OPENSTACK_INSTANCE_TOTAL_AVAILABLE_CPU           | * |
| QOS_OPENSTACK_INSTANCE_CPU_USAGE                     | * |
| QOS_OPENSTACK_INSTANCE_TOTAL_CPU_TIME_USED           | * |
| QOS_OPENSTACK_INSTANCE_DISK_SIZE                     | * |
| QOS_OPENSTACK_INSTANCE_READ_REQUEST_RATE             | * |
| QOS_OPENSTACK_INSTANCE_READ_THROUGHPUT               | * |
| QOS_OPENSTACK_INSTANCE_TOTAL_READ_REQUESTS           | * |
| QOS_OPENSTACK_INSTANCE_TOTAL_WRITE_REQUESTS          | * |
| QOS_OPENSTACK_INSTANCE_DATA_READ                     | * |
| QOS_OPENSTACK_INSTANCE_DATA_WRITE                    | * |
| QOS_OPENSTACK_INSTANCE_WRITE_THROUGHPUT              | * |
| QOS_OPENSTACK_INSTANCE_WRITE_REQUEST_RATE            | * |
| QOS_OPENSTACK_INSTANCE_TOTAL_MEMORY                  | * |
| QOS_OPENSTACK_INSTANCE_MEMORY_ALLOCATION             | * |
| QOS_OPENSTACK_INSTANCE_MEMORY_UTILIZATION            | * |
| QOS_OPENSTACK_INSTANCE_NETWORK_INCOMING_BYTES        | * |
| QOS_OPENSTACK_INSTANCE_NETWORK_INCOMING_BYTES_RATE   | * |
| QOS_OPENSTACK_INSTANCE_NETWORK_OUTGOING_BYTES        | * |
| QOS_OPENSTACK_INSTANCE_NETWORK_OUTGOING_BYTES_RATE   | * |
| QOS_OPENSTACK_SERVICE_ENDPOINT_STATUS                | * |
| QOS_OPENSTACK_PROJECT_MEMORY_SIZE                    | * |
| QOS_OPENSTACK_PROJECT_VOLUME_STORAGE_SIZE            | * |
| QOS_OPENSTACK_PROJECT_CPU                            | * |
| QOS_OPENSTACK_PROJECT_VM_INSTANCES                   | * |
| QOS_OPENSTACK_VOLUME_SIZE                            | * |
| QOS_OPENSTACK_VOLUME_STATUS                          | * |

**Availability Zone Health Summary**

This table displays information about the operational status of the availability zones in the OpenStack server.

| Column Name | Description                                                                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status      | This metric is the operational status of the availability zone. Possible values are as follows: <ul style="list-style-type: none"> <li>• 1 - Available</li> <li>• 2-4 - Not Available</li> </ul> |

**Controller Node Health Summary**

This table displays information about the operational status of the controller nodes in the OpenStack server.

| Column Name | Description                                                                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status      | This metric is the operational status of the controller node service. Possible values are as follows: <ul style="list-style-type: none"> <li>• 0 - Down</li> <li>• 1 - Up</li> </ul> |

**Controller Node Services Health Summary**

This table displays information about the operational status of the controller node services in the OpenStack server.

| Column Name | Description                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status      | This metric is the operational status of the controller node. Possible values are as follows: <ul style="list-style-type: none"> <li>• 0 - Down</li> <li>• 1 - Up</li> </ul> |

**Compute Node CPU Performance Summary**

This table displays information about the CPU metrics of the compute nodes in the OpenStack server.

| Column Name              | Description                                                                 |
|--------------------------|-----------------------------------------------------------------------------|
| Guest Count              | This metric is the number of instance instances on the compute node.        |
| Virtual CPU Count        | The number of virtual CPUs available for the compute node.                  |
| Virtual CPU Used Count   | The number of virtual CPUs that are currently used by the compute node.     |
| Virtual CPU Used Percent | The percentage of virtual CPUs that are currently used by the compute node. |

**Compute Node Disk Performance Summary**

This table displays information about the disk metrics of the compute nodes in the OpenStack server.

| Column Name | Description                                                                                    |
|-------------|------------------------------------------------------------------------------------------------|
| Total Disk  | This metric is the total size of the local disk (in Gigabytes) available for the compute node. |

|                   |                                                                                          |
|-------------------|------------------------------------------------------------------------------------------|
| Free Disk         | This metric is the size of the local disk (in Gigabytes) not used by the compute node.   |
| Used Disk         | This metric is the size of the local disk (in Gigabytes) used by the compute node.       |
| Disk Used Percent | This metric is the percentage of the local disk (in Gigabytes) used by the compute node. |

### **Compute Node Memory Performance Summary**

This table displays information about the memory metrics of the compute nodes in the OpenStack server.

| Column Name         | Description                                                                            |
|---------------------|----------------------------------------------------------------------------------------|
| Total Memory        | This metric is the total local memory (in Gigabytes) available for the compute node.   |
| Free Memory         | This metric is the local memory (in Gigabytes) not used by the compute node.           |
| Used Memory         | This metric is the local memory (in Gigabytes) used by the compute node.               |
| Memory Used Percent | This metric is the percentage of local memory (in Gigabytes) used by the compute node. |

### **Instance Health Summary**

This table displays information about the power and operational status of the instances in the OpenStack server.

| Column Name  | Description                                                                                                                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status       | This metric is the operational status of the instance. Possible values are as follows: <ul style="list-style-type: none"> <li>• 0 - Unknown</li> <li>• 1 - Active</li> <li>• 2 - Shutoff</li> <li>• 3 - Suspended</li> </ul> |
| Power Status | This metric is the availability status of the instance. Possible values are as follows: <ul style="list-style-type: none"> <li>• 1 - Running</li> <li>• 4 - Shutdown</li> </ul>                                              |

### **Instance CPU Performance Summary**

This table displays information about the CPU details of the instances in the OpenStack server.

| Column Name                  | Description                                                                        |
|------------------------------|------------------------------------------------------------------------------------|
| Total CPU Time Used          | This metric is the total CPU time (in hours) used by the instance.                 |
| Average CPU Usage            | This metric is the average percentage of virtual CPU that is used by the instance. |
| Available Virtual Processors | This metric is the number of virtual CPUs available to the instance.               |

**Instance Disk Performance Summary**

This table displays information about the disk details of the instances in the OpenStack server.

| Column Name          | Description                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------|
| Disk Size            | This metric is the total size of the local disk (in Gigabytes) available for the instance.                             |
| Total Read Requests  | This metric is the number of disk read requests performed by the instance.                                             |
| Read Request Rate    | This metric is the average number of disk read operations performed by the instance in a second.                       |
| Read Throughput      | This metric is the average data read (in Kilobytes) in disk read operations performed by the instance in a second.     |
| Data Read Volume     | This metric is the total size (in Kilobytes) of the data read by the instance from the disk.                           |
| Total Write Requests | This metric is the number of disk write requests performed by the instance.                                            |
| Write Request Rate   | This metric is the average number of disk write operations performed by the instance in a second.                      |
| Write Throughput     | This metric is the average data (in Kilobytes) written in disk write operations performed by the instance in a second. |
| Data Write Volume    | This metric is the total size (in Kilobytes) of the data written by the instance to the disk.                          |

**Instance Memory Performance Summary**

This table displays information about the memory details of the instances in the OpenStack server.

| Column Name | Description                                                                |
|-------------|----------------------------------------------------------------------------|
| Available   | This metric is the total memory (in Megabytes) available for the instance. |
| Allocated   | This metric is the total memory (in Megabytes) allocated to the instance.  |
| Utilized    | This metric is the total memory (in Megabytes) utilized by the instance.   |

**Instance Network Performance Summary**

This table displays information about the network details of the instances in the OpenStack server.

| Column Name         | Description                                                                      |
|---------------------|----------------------------------------------------------------------------------|
| Incoming Bytes      | This metric is the number of incoming bytes of data on the network interface.    |
| Incoming Bytes Rate | This metric is the incoming bytes of data per second on the network interface.   |
| Outgoing Bytes      | This metric is the number of outgoing bytes of data from the network interface.  |
| Outgoing Bytes Rate | This metric is the outgoing bytes of data per second from the network interface. |

### **Project Performance Summary**

This table displays information about the projects in the OpenStack server.

| Column Name     | Description                                                                           |
|-----------------|---------------------------------------------------------------------------------------|
| Total Instances | This metric is the number of instances assigned to the project.                       |
| Total VCPUs     | This metric is the number of virtual CPUs available to the project.                   |
| Memory Size     | This metric is the total memory (in Gigabytes) available for the project.             |
| Volume Storage  | This metric is the total size of the volume (in Gigabytes) available for the project. |

### **Service Endpoint Health Summary**

This table displays information about the service endpoints in the OpenStack server.

| Column Name | Description                                                                                                                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status      | This metric is the operational status of the service endpoint. Possible values are as follows: <ul style="list-style-type: none"> <li>• 0 - Down</li> <li>• 1 - Up</li> <li>• 2,3 - Not Supported</li> </ul> |

### **Volume Health Summary**

This table displays information about the volumes in the OpenStack server.

| Column Name | Description                                                                                                                                                                                                                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status      | This metric is the operational status of the volume. Possible values are as follows: <ul style="list-style-type: none"> <li>• 0 - Error</li> <li>• 1 - In Use</li> <li>• 2 - Attaching</li> <li>• 3 - Detaching</li> <li>• 4 - Creating</li> <li>• 5 - Deleting</li> <li>• 6 - Available</li> <li>• 7 - Error Deleting</li> </ul> |
| Size        | This metric is the size of the disk volume, in Gigabytes.                                                                                                                                                                                                                                                                         |

## **Oracle RAC Unified Dashboard**

The ORACLE RAC Unified Dashboard provides predefined list views for monitoring RAC Database Health, RAC Instance Node Performance, Access Latency, and Instance Node Health.

### **Contents**

## Oracle RAC Required Data Sources

This table lists the QoS metrics, and subkeys or targets that must be activated to populate data in the ORACLE RAC dashboard.

| QoS Metric                            | SubKey/Target |
|---------------------------------------|---------------|
| QOS_ORACLE_CHECK_DBALIVE              | *             |
| QOS_ORACLE_TABLESPACE_FREE            | *             |
| QOS_ORACLE_TABLESPACE_ALLOC_FREE      | *             |
| QOS_ORACLE_TABLESPACE_TEMP_FREE       | *             |
| QOS_ORACLE_FLASH_RECOVERY_AREA_MEMORY | *             |
| QOS_ORACLE_TABLESPACE_SIZE            | *             |
| QOS_ORACLE_DATABASE_SIZE              | *             |
| QOS_ORACLE_INSTANCE_STATUS            | *             |
| QOS_ORACLE_RSRC_MGR_CPU_WAIT_TIME     | *             |
| QOS_ORACLE_MEMORY_USAGE               | *             |
| QOS_ORACLE_SGA_MEMORY_FREE            | *             |
| QOS_ORACLE_AVG_BUSY_TIME              | *             |
| QOS_ORACLE_ACTIVE_USER                | *             |
| QOS_ORACLE_ACTIVE_CONNECTION_RATIO    | *             |
| QOS_ORACLE_ACCESS_LATENCY             | *             |
| QOS_ORACLE_GC_CR_BLOCKS_SERVED        | *             |
| QOS_ORACLE_GC_CR_BLOCKS_RECEIVED      | *             |
| QOS_ORACLE_BUF_CACHEHIT_RATIO         | *             |
| QOS_ORACLE_DICT_CACHEHIT_RATIO        | *             |
| QOS_ORACLE_SESSION_WAITS              | *             |
| QOS_ORACLE_SYSTEM_STATICS             | *             |
| QOS_ORACLE_SYSTEM_WAITS               | *             |
| QOS_ORACLE_DBFILE_IO                  | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

## Data Access Latency

This chart displays information about the Data Access Latency, which helps you understand how efficiently the cache is used for serving database queries. The optimum usage of cache is necessary for minimizing the query response time.

| QoS Name                        | Description                                                         |
|---------------------------------|---------------------------------------------------------------------|
| Access Latency                  | Monitors the overall data access latency of the Oracle database.    |
| Consistent Read Blocks Served   | Monitors the total number of blocks constructed by the BSP process. |
| Consistent Read Blocks Received | Monitors the total number of blocks received.                       |

|                            |                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Buffer Cache Hit Ratio     | Monitors the buffer cache-hit ratio. Higher the ratio, better is the performance.<br>0 to 50.99 = Red<br>51 to 74.99 = Orange<br>75 to 84.99 = Yellow<br>85 to 100 = Green |
| Dictionary Cache Hit Ratio | Monitors the dictionary cache-hit ratio.                                                                                                                                   |

### **RAC Database Health**

This chart displays information about the RAC Database Health, lets you monitor database status and disk space. The optimum disk space helps you effectively use your hardware resources while ensuring performance and availability.

| Column Name                | Description                                                                    |
|----------------------------|--------------------------------------------------------------------------------|
| Database Alive Status      | Monitors connectivity to the database instance.                                |
| Total Free Tablespace      | Monitors tablespaces for the available space.                                  |
| Allocated Free Tablespace  | Monitors tablespaces for available space left in allocated files.              |
| Temporary Free Tablespace  | Monitors temporary tablespaces for the available space.                        |
| Free Flash Recovery Memory | Monitors the available memory in the flash recovery area.                      |
| Tablespace Size            | Monitors tablespaces size in MB.                                               |
| Database Size              | Monitors space size (in bytes) for each database, log and data files together. |

### **RAC Instance Node Health**

This chart displays information about the Instance Node Health, which helps you ensuring proper load balancing between all RAC instances. This chart alerts the Database Administrator (DBA) when any instance goes up or down.

| QoS Name                   | Description                                                                   |
|----------------------------|-------------------------------------------------------------------------------|
| Sessions Wait Counter      | Monitors the sessions wait counter.                                           |
| System Statistical Counter | Monitors the various system statistical counters since start of the instance. |
| System Wait Counter        | Monitors the system wait counter.                                             |
| Database File IO           | Monitors the database file I/O operations.                                    |

### **RAC Node Instance Performance**

This chart displays information about the RAC Node Instance Performance, which symbolizes how efficiently all RAC instances are utilized for optimum database performance.

| QoS Name                       | Description                                                                                                 |
|--------------------------------|-------------------------------------------------------------------------------------------------------------|
| Node Status                    | Monitors the state of the current instance.                                                                 |
| Resource Manager CPU Wait Time | Monitors the total number of hundredths of a second that Oracle processes have been in a ready state.       |
| Node Memory Usage              | Monitors the memory consumption in bytes of Oracle users (PGA).                                             |
| Free SGA Memory                | Monitors the free SGA memory.                                                                               |
| Average Busy Time              | Monitors the number of hundredths of a second that a processor has been busy executing user or kernel code. |



|                         |                                           |
|-------------------------|-------------------------------------------|
| Currently Active Users  | Checks the currently active Oracle users. |
| Active Connection Ratio | Monitors the active connection ratio.     |

## Oracle Unified Dashboard

The Oracle Unified Dashboard provides predefined list views for monitoring Available Tablespace, Database Utilization, Free SGA Memory, Resource Utilization Count, and Server Information.

### NOTE

If you enable any of these resources to collect metrics, you must disable alarm collection before you enable them (unless you want to collect the alarm data).

### Contents

#### Oracle Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the Oracle dashboard.

| QoS                                   | Subkey/Target |
|---------------------------------------|---------------|
| QOS_ORACLE_SGA_Memory_Free            | *             |
| QOS_ORACLE_check_dbalive              | *             |
| QOS_ORACLE_memory_usage               | *             |
| QOS_ORACLE_resource_utilization_count | *             |
| QOS_ORACLE_buf_cachehit_ratio         | *             |
| QOS_ORACLE_database_size              | *             |
| QOS_ORACLE_tablespace_free            | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

#### Available Tablespace

This chart displays information about the Available Tablespace.

| Column Name          | Description                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------|
| Available Tablespace | Measures the percentage of free space in a tablespace, considering the maximal possible tablespace size. |

#### Database Utilization

This chart displays information about the database utilization.

| Column Name            | Description                                                                                                                                                                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Buffer Cache Hit Ratio | Percentage of pages found in the buffer cache without having to read from disk.<br>It can be low at the start of a new application, before the cache is filled with data. If it stays low for many intervals you should consider increasing the size of the cache (DB_BLOCK_BUFFERS). |

|               |                                                                                 |
|---------------|---------------------------------------------------------------------------------|
| Database Size | Monitors space size (in bytes) for each database, log, and data files together. |
|---------------|---------------------------------------------------------------------------------|

### **Free SGA Memory**

This chart displays information about the free SGA memory.

| Column Name     | Description                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Free SGA Memory | The SGA (System Global Area) is an area of memory (RAM) allocated when an Oracle Instance starts up. It measures the SGA free memory usage in bytes. |

### **Resource Utilization Count**

This chart displays information about the resource utilization count.

| Column Name                | Description                                                                         |
|----------------------------|-------------------------------------------------------------------------------------|
| Resource Utilization Count | Monitors database utilization for resources (Processes, Sessions and Transactions). |

### **Server Information**

This chart displays information about the server information.

| Column Name           | Description                                                                                                                                                                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database Alive Status | Monitors connectivity to the database instance. This checkpoint tries to connect to an instance and the value returned as 1 or 0.                                                                                                                                                                      |
| Memory Usage          | Monitors memory consumption in bytes of Oracle users (PGA). If the system has enough physical memory, increase parameter PGA_AGGREGATE_TARGET or change to automatic PGA management (9i). Otherwise look into V\$PROCESS, V\$PGASTAT, V\$SQL_WORKAREA views to find most memory consuming Oracle user. |

## **Power Unified Dashboard**

The Data Center Power Unified Dashboard provides predefined list views with information about power usage in your data center.

### **Contents**

#### **NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### **Power Required Data Sources**

The table contains the probes and QoS metrics required for the preconfigured Power dashboard.

| Probe | QoS Required                                                   |
|-------|----------------------------------------------------------------|
| power | QOS_BATTERY_TIME_REMAINING<br>QOS_DCIE<br>QOS_PUE<br>QOS_VOLTS |

### **UPS Battery Runtime Remaining**

| Column                    | Description                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------|
| Target                    | DataCenter plus the IP address, name, object identifier, or description of the data center. |
| Battery Runtime Remaining | Expected runtime of the UPS in minutes.                                                     |

### **Data Center Power Effectiveness**

| Column     | Description                                                                                                                                                         |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target     | The data center name. For the current version of the power probe this is always Data Center.                                                                        |
| PUE Value  | Measurement of the energy efficiency of a data center. Calculated by dividing the total facility power by the total IT equipment power. PUE is the inverse of DCIE. |
| PUE Result | Efficiency level of measured PUE.                                                                                                                                   |

### **Data Center Infrastructure Efficiency**

| Column       | Description                                                                                                                                                                 |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target       | DataCenter plus the IP address, name, object identifier, or description of the data center.                                                                                 |
| DCIE         | Measurement of the energy efficiency of a data center. DCIE is calculated by dividing the total IT equipment power by the total facility power. DCIE is the inverse of PUE. |
| DCIE Results | Efficiency level of measured DCIE.                                                                                                                                          |

### **UPS Input Line Voltage**

| Column | Description                                                                                 |
|--------|---------------------------------------------------------------------------------------------|
| Name   | DataCenter plus the IP address, name, object identifier, or description of the data center. |
| Volts  | Voltage of the UPS input line.                                                              |
| Volts  | Voltage of the UPS input line, displayed as a line graph.                                   |

## Processes Unified Dashboard

The Processes Unified Dashboard provides predefined list views for checking process availability, monitoring process CPU, and Memory.

### Contents

#### Processes Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the *processes* dashboard.

| QoS                | Subkey/Target |
|--------------------|---------------|
| QOS_PROCESS_CPU    | *             |
| QOS_PROCESS_MEMORY | *             |
| QOS_PROCESS_STATE  | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

#### Process Performance

This chart displays information about the Process Performance. If you click the name of a process under Target, the corresponding Performance report opens.

| Column Name          | Description                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Host                 | Name of the host where the process is running.                                                                                      |
| Target               | Lists the processes present in your environment.                                                                                    |
| Process CPU usage    | Measures the CPU Usage of the process in percentage<br>0 to 70 = Green<br>71 to 80 = Yellow<br>81 to 90 = Orange<br>91 to 100 = Red |
| Process Memory Usage | Monitors the Memory Usage of process in kilobytes.                                                                                  |
| Process Availability | Monitors the availability (up/down) of a process<br>Green = UP (1 - 1)<br>Red = DOWN (0 - 0)                                        |

## PureStorage All-Flash Array Unified Dashboard

The PureStorage All-Flash Array Unified Dashboard provides predefined list views for monitoring the health and performance of the logical and physical components of PureStorage Flash Array. These components include drives, hardware, network, volumes, hosts, and hostgroups.

### Contents

## PureStorage Required Data Sources

The following table contains the monitors that you must activate in the purestorage probe to see data in the PureStorage Unified Dashboard. You can quickly enable these monitors in the purestorage probe by applying a copy of the PureStorage Factory Template in the probe configuration.

| QoS                              | Subkey/Target |
|----------------------------------|---------------|
| QOS_PS_ARRAY_DATA_REDUCTION      | *             |
| QOS_PS_ARRAY_CAPACITY            | Array         |
| QOS_PS_ARRAY_AVG_IO_SIZE         | *             |
| QOS_PS_DRIVE_STATUS              | Drive         |
| QOS_PS_DRIVE_CAPACITY            | Drive         |
| QOS_PS_DRIVE_FAIL_DETECTED       | Drive         |
| QOS_PS_HARDWARE_STATUS           | Hardware      |
| QOS_PS_HARDWARE_SPEED            | Hardware      |
| QOS_PS_NETWORK_NIC_STATUS        | Network       |
| QOS_PS_NETWORK_MTU               | Network       |
| QOS_PS_NETWORK_PORT_SPEED        | Network       |
| QOS_PS_HOSTGROUP_DATA_REDUCTION  | *             |
| QOS_PS_HOSTGROUP_SNAPSHOTS       | *             |
| QOS_PS_HOSTGROUP_TOTAL_REDUCTION | *             |
| QOS_PS_HOSTGROUP_TOTAL           | *             |
| QOS_PS_HOSTGROUP_THIN_PROVISION  | *             |
| QOS_PS_HOSTGROUP_SIZE            | *             |
| QOS_PS_HOST_VOLUMES              | *             |
| QOS_PS_HOST_DATA_REDUCTION       | *             |
| QOS_PS_HOST_TOTAL_REDUCTION      | *             |
| QOS_PS_HOST_SNAPSHOTS            | *             |
| QOS_PS_HOST_TOTAL                | *             |
| QOS_PS_HOST_THIN_PROVISION       | *             |
| QOS_PS_VOLUME_DATA_REDUCTION     | *             |
| QOS_PS_VOLUME_TOTAL_REDUCTION    | *             |
| QOS_PS_VOLUME_SNAPSHOTS          | *             |
| QOS_PS_VOLUME_INPUT_PER_SEC      | *             |

An asterisk (\*) means that this QOS brings data for all targets for which it is applicable.

## ArrayMonitorList

This view displays information about the PureStorage FlashArray device which is being monitored.

| Column Name | Description                                                                       |
|-------------|-----------------------------------------------------------------------------------|
| Avg IO Size | The average size (in kilobytes) of the input/output operations on the FlashArray. |

|                        |                                                                             |
|------------------------|-----------------------------------------------------------------------------|
| Data Reduction [Ratio] | The data reduction ratio (written over provisioned data) of the FlashArray. |
| Capacity               | The total capacity (in gigabytes) of the FlashArray.                        |
| Used Capacity          | The total used capacity (in gigabytes) of the FlashArray.                   |
| Reads / Sec            | The total number of read requests processed per second on the FlashArray.   |
| Writes / Sec           | The total number of write requests processed per second on the FlashArray.  |
| Total IOPS             | The total number of input/output operations per second of the FlashArray.   |
| Total Bandwidth        | The total bandwidth consumed by the FlashArray.                             |
| Input / Sec            | The number of bits read per second on the FlashArray.                       |
| Output / Sec           | The number of bits written per second on the FlashArray.                    |
| Read Latency           | The average arrival to completion time for a FlashArray read operation.     |
| Write Latency          | The average arrival to completion time for a FlashArray write operation.    |

### **DrivesMonitorList**

This view displays the status of the drives in the PureStorage FlashArray.

| Column Name      | Description                                                                                                                                                                                                                                                                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Capacity         | The total capacity of the drives (in gigabytes) in the FlashArray.                                                                                                                                                                                                                                                                               |
| Status           | The status of the drives present in the FlashArray. You can set up the threshold for operational status using a numeric value between 0 and 2. Each number is assigned an operational status value of supported components, as follows: <ul style="list-style-type: none"> <li>• Healthy: 0</li> <li>• Empty: 1</li> <li>• Unknown: 2</li> </ul> |
| Failure Detected | The failure state detected in the FlashArray drives. You can set up the threshold for operational status using a numeric values 0 and 1. Each number is assigned an operational status value of supported components, as follows: <ul style="list-style-type: none"> <li>• False: 0</li> <li>• True: 1</li> </ul>                                |

### **HardwareMetrics**

This view displays the hardware status and temperature of the PureStorage FlashArray.

| Column Name | Description                                                                                                                                                                                                                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status      | The status of the FlashArray hardware. You can set up the threshold for operational status using a numeric value between 0 and 2. Each number is assigned an operational status value of supported components, as follows: <ul style="list-style-type: none"> <li>• OK: 0</li> <li>• NotInstalled: 1</li> <li>• Unknown: 2</li> </ul> |

|             |                                                          |
|-------------|----------------------------------------------------------|
| Temperature | The temperature (in celsius) of the FlashArray hardware. |
|-------------|----------------------------------------------------------|

### **HostgroupsMetrics**

This view displays information about the capacity of the PureStorage FlashArray hostgroups.

| Column Name             | Description                                                                           |
|-------------------------|---------------------------------------------------------------------------------------|
| Snapshots               | The total capacity (in gigabytes) of the snapshots on the FlashArray hostgroup.       |
| Total Reduction [Ratio] | The ratio of the total data reduced on the FlashArray hostgroup.                      |
| Volumes                 | The total capacity (in gigabytes) of the volumes in a FlashArray hostgroup.           |
| Total                   | The total amount of used space (in gigabytes) on the FlashArray hostgroup.            |
| Data Reduction [Ratio]  | The data reduction ratio (written over provisioned data) of the FlashArray hostgroup. |
| Size                    | The total capacity (in gigabytes) of the FlashArray hostgroup.                        |
| Thin Provision [Ratio]  | The ratio of the dynamically reserved storage space on the FlashArray hostgroup.      |

### **HostMetrics**

This view displays the information about the capacity of the PureStorage FlashArray hosts.

| Column Name             | Description                                                                      |
|-------------------------|----------------------------------------------------------------------------------|
| Snapshots               | The total capacity (in gigabytes) of the snapshots on the FlashArray host.       |
| Total Reduction [Ratio] | The ratio of the total data reduced on the FlashArray host.                      |
| Volumes                 | The total capacity (in gigabytes) of the volumes in a FlashArray host.           |
| Total                   | The total capacity of used space (in gigabytes) on the FlashArray host.          |
| Data Reduction [Ratio]  | The data reduction ratio (written over provisioned data) of the FlashArray host. |
| Size                    | The total capacity of the FlashArray host.                                       |
| Thin Provision [Ratio]  | The ratio of the dynamically reserved storage space on the FlashArray.           |

### **NetworkMetrics**

This view displays information about the network interfaces in the PureStorage FlashArray.

| Column Name               | Description                                                              |
|---------------------------|--------------------------------------------------------------------------|
| Maximum Transmission Unit | The Maximum Transmission Unit size (in bytes) of the FlashArray network. |

|                  |                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface Status | The NIC (network interface card) status of the FlashArray network. You can set up the threshold for operational status using a numeric value between 0 and 2. Each number is assigned an operational status value of supported components, as follows: <ul style="list-style-type: none"> <li>• Enabled: 0</li> <li>• Disabled: 1</li> <li>• Unknown: 2</li> </ul> |
| Port Speed       | The port speed (in bits) of the FlashArray network.                                                                                                                                                                                                                                                                                                                |

### **VolumesMetrics**

This view displays information about the performance and capacity of the volumes in the PureStorage FlashArray.

| Column Name            | Description                                                                              |
|------------------------|------------------------------------------------------------------------------------------|
| Data Reduction [Ratio] | The data reduction ratio (written over provisioned data) of the FlashArray volume.       |
| Output / Second        | The number of bits written per second on the FlashArray volume.                          |
| Write / second         | The total number of write requests processed per second on the FlashArray volume.        |
| Avg IO SIZE            | The average size (in kilobytes) of the input/output operations on the FlashArray volume. |
| Snapshots              | The total capacity (in gigabytes) of the snapshots on the FlashArray Volume.             |
| Total IOPS             | The total number of input/output operations per second of the FlashArray volume.         |
| Total Bandwidth        | The bandwidth consumed by the FlashArray volume.                                         |
| Read / Second          | The total number of read requests processed per second on the FlashArray volume.         |
| Inputs / Second        | The number of bits read per second on the FlashArray volume.                             |
| Thin Provision [Ratio] | The ratio of the dynamically reserved storage space on the FlashArray volume.            |
| Read Latency           | The average arrival to completion time for a FlashArray read operation.                  |
| Write Latency          | The average arrival to completion time for a FlashArray write operation.                 |

## **Router-Switch Unified Dashboard**

The Router-Switch Unified Dashboard provides predefined list views for monitoring the status of network resources (interfaces, memory, and CPU).

### **Contents**

#### **Required Data Sources in the snmpcollector Probe**

The following table contains the monitors that you must activate in the snmpcollector probe to see data in the Router-Switch Unified Dashboard.

| Dashboard Chart       | QoS                           | Target/Source |
|-----------------------|-------------------------------|---------------|
| Network Device Health | QOS_AVAILABILITY_AVAILABILITY | Availability  |



|                           |                                |              |
|---------------------------|--------------------------------|--------------|
| Network Device Health     | QOS_REACHABILITY_REACHABILITY  | Reachability |
| Network Device Health     | QOS_CPU_UTILIZATION            | *            |
| Network Device Health     | QOS-PHYSICALMEMORY_UTILIZATION | *            |
| Interface Utilization In  | QOS_INTERFACE_UTILIZATIONIN    | *            |
| Interface Utilization Out | QOS_INTERFACE_UTILIZATIONOUT   | *            |
| Errors In                 | QOS_INTERFACE_PCTERRORSIN      | *            |
| Errors Out                | QOS_INTERFACE_PCTERRORSOUT     | *            |
| Discards In               | QOS_INTERFACE_PCTDISCARDSIN    | *            |
| Discards Out              | QOS_INTERFACE_PCTDISCARDSOUT   | *            |

An asterisk (\*) means that the value for the first entry for the QoS is used.

### Network Device Health

This chart displays information about the availability, reachability, CPU utilization, and memory utilization of network devices over the last 24 hours. Use this chart to view information about the lowest performing network devices.

| Column                  | Description                                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host                    | The IP address of the monitored device. Click this link to view additional information in OC.                                                                                                                                        |
| Availability            | The percent availability of the device within the last hour. Availability is the device up-time reported by the device. <ul style="list-style-type: none"> <li>Green - 100</li> <li>Red - 99 through 0</li> </ul>                    |
| Availability - Last Day | The percent availability of the device over the past 24 hours. <ul style="list-style-type: none"> <li>Green - 100</li> <li>Yellow - 99 through 98</li> <li>Orange - 97 through 95</li> <li>Red - 94 through 0</li> </ul>             |
| Reachability            | The percent reachability of the device within the last hour. Reachability is the connectivity of the probe to the device over time. <ul style="list-style-type: none"> <li>Green - 100</li> <li>Red - 99 through 0</li> </ul>        |
| Reachability - Last Day | The percent reachability of the device over the past 24 hours. <ul style="list-style-type: none"> <li>Green - 100</li> <li>Yellow - 99 through 97</li> <li>Orange - 96 through 94</li> <li>Red - 93 through 0</li> </ul>             |
| CPU                     | The percent utilization of the device CPU within the last hour. <ul style="list-style-type: none"> <li>Green - 0 through 50</li> <li>Yellow - 51 through 70</li> <li>Orange - 71 through 80</li> <li>Red - 81 through 100</li> </ul> |

|        |                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Memory | The percent utilization of the device memory within the last hour. <ul style="list-style-type: none"> <li>Green - 0 through 50</li> <li>Yellow - 51 through 70</li> <li>Orange - 71 through 80</li> <li>Red - 81 through 100</li> </ul> |
| Alarm  | The alarms for the device.                                                                                                                                                                                                              |

### **Interface Utilization In**

This chart displays information about interface percent utilization for inbound network traffic over the last 24 hours. Use this chart to view information about the highest utilized interfaces.

| Column         | Description                                                                                                                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device         | The name of the monitored device. Click this link to view additional information in OC.                                                                                                                                                                                            |
| Target         | The name of the device interface. Click this link to view additional information in OC.                                                                                                                                                                                            |
| Utilization In | The percent utilization for inbound network traffic that is detected by the interface within the past hour. <ul style="list-style-type: none"> <li>Green - 0 through 65</li> <li>Yellow - 66 through 75</li> <li>Orange - 76 through 90</li> <li>Red - 91 through 100</li> </ul>   |
| Last Day       | The percent utilization for inbound network traffic that is detected by the interface over the past 24 hours. <ul style="list-style-type: none"> <li>Green - 0 through 65</li> <li>Yellow - 66 through 75</li> <li>Orange - 76 through 80</li> <li>Red - 81 through 100</li> </ul> |
| Alarm          | Alarms for inbound network traffic percent utilization thresholds.                                                                                                                                                                                                                 |

### **Interface Utilization Out**

This chart displays information about interface percent utilization for outbound network traffic over the last 24 hours. Use this chart to view information about the highest utilized interfaces.

| Column          | Description                                                                                                                                                                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device          | The name of the monitored device. Click this link to view additional information in OC.                                                                                                                                                                                           |
| Target          | The name of the device interface. Click this link to view additional information in OC.                                                                                                                                                                                           |
| Utilization Out | The percent utilization for outbound network traffic that is detected by the interface within the past hour. <ul style="list-style-type: none"> <li>Green - 0 through 65</li> <li>Yellow - 66 through 75</li> <li>Orange - 76 through 90</li> <li>Red - 91 through 100</li> </ul> |

|          |                                                                                                                                                                                                                                                                                     |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Last Day | The percent utilization for outbound network traffic that is detected by the interface over the past 24 hours. <ul style="list-style-type: none"> <li>Green - 0 through 65</li> <li>Yellow - 66 through 75</li> <li>Orange - 76 through 90</li> <li>Red - 91 through 100</li> </ul> |
| Alarm    | Alarms for outbound network traffic percent utilization thresholds.                                                                                                                                                                                                                 |

### **Errors In**

This chart displays information about the inbound packet errors that are associated with an interface over the last 24 hours. Use this chart to view information about the interfaces with the highest percentage of errors.

| Column    | Description                                                                                                                                                                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device    | The name of the monitored device. Click this link to view additional information in OC.                                                                                                                                                                                  |
| Target    | The name of the device interface. Click this link to view additional information in OC.                                                                                                                                                                                  |
| Errors In | The number of inbound packet errors that are detected by the interface within the past hour. <ul style="list-style-type: none"> <li>Green - 0 to 0.5</li> <li>Yellow - 0.6 through 0.8</li> <li>Orange - 0.9 through 0.99</li> <li>Red - 1 through 100</li> </ul>        |
| Last Day  | The number of inbound packet errors that are detected by the interface over the past 24 hours. <ul style="list-style-type: none"> <li>Green - 0 through 0.5</li> <li>Yellow - 0.6 through 0.8</li> <li>Orange - 0.9 through 0.99</li> <li>Red - 1 through 100</li> </ul> |
| Alarm     | Alarms for inbound packet error thresholds.                                                                                                                                                                                                                              |

### **Errors Out**

This chart displays information about the outbound packet errors that are associated with an interface over the last 24 hours. Use this chart to view information about the interfaces with the highest percentage of errors.

| Column     | Description                                                                                                                                                                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device     | The name of the monitored device. Click this link to view additional information in OC.                                                                                                                                                                                 |
| Target     | The name of the device interface. Click this link to view additional information in OC.                                                                                                                                                                                 |
| Errors Out | The number of outbound packet errors that are detected by the interface within the last hour. <ul style="list-style-type: none"> <li>Green - 0 through 0.5</li> <li>Yellow - 0.6 through 0.8</li> <li>Orange - 0.9 through 0.99</li> <li>Red - 1 through 100</li> </ul> |

|          |                                                                                                                                                                                                                                                                                   |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Last Day | The number of outbound packet errors that are detected by the interface over the past 24 hours. <ul style="list-style-type: none"> <li>• Green - 0 through 0.5</li> <li>• Yellow - 0.6 through 0.8</li> <li>• Orange - 0.9 through 0.99</li> <li>• Red - 1 through 100</li> </ul> |
| Alarm    | Alarms for outbound packet error thresholds.                                                                                                                                                                                                                                      |

### **Discards In**

This chart displays information about the inbound packets that are discarded by an interface over the last 24 hours. Use this chart to view information about the interfaces with the highest percentage of discards.

| Column      | Description                                                                                                                                                                                                                                                                 |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device      | The name of the monitored device. Click this link to view additional information in OC.                                                                                                                                                                                     |
| Target      | The name of the device interface. Click this link to view additional information in OC.                                                                                                                                                                                     |
| Discards In | The number of inbound packets that are discarded by the interface within the last hour. <ul style="list-style-type: none"> <li>• Green - 0 through 0.5</li> <li>• Yellow - 0.6 through 0.8</li> <li>• Orange - 0.9 through 0.99</li> <li>• Red - 1 through 100</li> </ul>   |
| Last Day    | The number of inbound packets that are discarded by the interface over the past 24 hours. <ul style="list-style-type: none"> <li>• Green - 0 through 0.5</li> <li>• Yellow - 0.6 through 0.8</li> <li>• Orange - 0.9 through 0.99</li> <li>• Red - 1 through 100</li> </ul> |
| Alarm       | Alarms for inbound packet discard thresholds.                                                                                                                                                                                                                               |

### **Discards Out**

This chart displays information about the outbound packets that are discarded by an interface over the last 24 hours. Use this chart to view information about the interfaces with the highest percentage of discards.

| Column       | Description                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device       | The name of the monitored device. Click this link to view additional information in OC.                                                                                                                                                                                    |
| Target       | The name of the device interface. Click this link to view additional information in OC.                                                                                                                                                                                    |
| Discards Out | The number of outbound packets that are discarded by the interface within the last hour. <ul style="list-style-type: none"> <li>• Green - 0 through 0.5</li> <li>• Yellow - 0.6 through 0.8</li> <li>• Orange - 0.9 through 0.99</li> <li>• Red - 1 through 100</li> </ul> |

|          |                                                                                                                                                                                                                                                                      |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Last Day | The number of outbound packets that are discarded by the interface over the past 24 hours. <ul style="list-style-type: none"> <li>Green - 0 through 0.5</li> <li>Yellow - 0.6 through 0.8</li> <li>Orange - 0.9 through 0.99</li> <li>Red - 1 through 100</li> </ul> |
| Alarm    | Alarms for outbound packet discard thresholds.                                                                                                                                                                                                                       |

## SAP\_Basis DB2 Database Unified Dashboard

The sap\_basis DB2 Database Unified Dashboard provides predefined list views to monitor the health and performance of the DB2 Database in the SAP landscape.

### Contents

#### NOTE

: If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### SAP\_Basis DB2 Database Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the SAP\_Basis DB2 Database dashboard. An asterisk (\*) means that this QoS brings data for all targets for which it is applicable.

| QoS                       | Subkey/Target |
|---------------------------|---------------|
| QOS_SAP_DB2_AVAILABILITY  | *             |
| QOS_SAP_DB2_DAILY_GROWTH  | *             |
| QOS_SAP_DB2_DATABASE_SIZE | *             |
| QOS_SAP_DB2_USED_SPACE    | *             |

For more information about configuring probes, see the documentation for each probe.

### DB2 Database Summary

This table displays information about the DB2 Database statistics. Use this chart to view information about the DB2 database performance.

| Column Name           | Description                                                                     |
|-----------------------|---------------------------------------------------------------------------------|
| Database Availability | The percentage availability of DB2 database.                                    |
| Daily Growth          | The growth in utilized memory space in the DB2 database since the previous day. |
| Database Size         | The total size of DB2 database.                                                 |
| Database Used Space   | The total size of currently utilized space in the DB2 database.                 |

## SAP\_Basis HANA Database Unified Dashboard

The sap\_basis HANA Database Unified Dashboard provides predefined list views to monitor the health and performance of the HANA Database in the SAP landscape.

### Contents

#### NOTE

: If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### SAP\_Basis HANA Database Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the SAP\_Basis DB2 Database dashboard. An asterisk (\*) means that this QoS brings data for all targets for which it is applicable.

| QoS                                           | Subkey/Target |
|-----------------------------------------------|---------------|
| QOS_SAP_HANA_SCHEMA_DELTA_RECORDS             | *             |
| QOS_SAP_HANA_DISK_VOLUME_SIZE                 | *             |
| QOS_SAP_HANA_DISK_VOLUME_USED_SPACE           | *             |
| QOS_SAP_HANA_HOST_TOTAL_IO_TIME               | *             |
| QOS_SAP_HANA_HOST_CPU_USER_TIME               | *             |
| QOS_SAP_HANA_HOST_CPU_BUSY                    | *             |
| QOS_SAP_HANA_HOST_TOTAL_COUNT                 | *             |
| QOS_SAP_HANA_HOST_IDLE_COUNT                  | *             |
| QOS_SAP_HANA_HOST_FREE_PHYSICAL_MEMORY        | *             |
| QOS_SAP_HANA_HOST_USED_PHYSICAL_MEMORY        | *             |
| QOS_SAP_HANA_HOST_FREE_SWAP_SPACE             | *             |
| QOS_SAP_HANA_HOST_USED_SWAP_SPACE             | *             |
| QOS_SAP_HANA_HOST_EFFECTIVE_ALLOCATION_SIZE   | *             |
| QOS_SAP_HANA_HOST_MEMORY_ACTUAL_USED_SIZE     | *             |
| QOS_SAP_HANA_HOST_MEMORY_ALLOCATION_PEAK_SIZE | *             |
| QOS_SAP_HANA_SERVICE_PENDING_REQUEST          | *             |
| QOS_SAP_HANA_SERVICE_RESPONSE_TIME            | *             |
| QOS_SAP_HANA_SERVICE_STATUS                   | *             |
| QOS_SAP_HANA_SERVICE_COORDINATOR_TYPE         | *             |
| QOS_SAP_HANA_SERVICE_REQUESTS_PER_SEC         | *             |
| QOS_SAP_HANA_SERVICE_PROCESS_CPU_USAGE        | *             |
| QOS_SAP_HANA_SERVICE_PROCESS_MEMORY           | *             |
| QOS_SAP_HANA_SERVICE_AVAILABLE_MEMORY         | *             |
| QOS_SAP_HANA_SERVICE_TOTAL_MEMORY             | *             |
| QOS_SAP_HANA_SHARED_MEMORY_USED_PCT           | *             |

| QoS                                       | Subkey/Target |
|-------------------------------------------|---------------|
| QOS_SAP_HANA_SERVICE_LOG_MISSING          | *             |
| QOS_SAP_HANA_SERVICE_LOG_BACKUP           | *             |
| QOS_SAP_HANA_SERVICE_DATA_SNAPSHOT        | *             |
| QOS_SAP_HANA_SERVICE_COMPLETE_DATA_BACKUP | *             |
| QOS_SAP_HANA_MAX_PEAK_MEMORY_USED         | *             |

For more information about configuring probes, see the documentation for each probe.

### **Schema Summary**

This table displays information about the SAP HANA schemas. Use this chart to view information about the records residing on the schema.

| Column Name                                      | Description                                                   |
|--------------------------------------------------|---------------------------------------------------------------|
| Number of documents in delta for complete schema | The total number of records in delta for the complete schema. |

### **Disk Summary**

This table displays information about the SAP HANA disks. Use this chart to view information about the disks on the host and at file system level.

| Column Name       | Description                                      |
|-------------------|--------------------------------------------------|
| Used Volume Size  | The total size of data and log volumes.          |
| Total Volume Size | The total disk space used on the host hard disk. |

### **Host Memory Performance**

This table displays information about the host memory performance. Use this chart to view information about the memory utilization by the system and peak memory utilization.

| Column Name                 | Description                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------|
| Free Physical Memory        | The total amount of free physical memory on the host.                                     |
| Used Physical Memory        | The total used physical memory on the host.                                               |
| Free Swap Memory            | The total free swap memory on the host.                                                   |
| Used Swap Memory            | The total used swap memory on the host.                                                   |
| Size of Memory Pool         | The size of the memory pool for all SAP HANA processes.                                   |
| Memory Pool in Actual Use   | The amount of memory from the memory pool that is currently in use by SAP HANA processes. |
| Memory Allocation Peak size | The highest memory pool allocation to the HANA system.                                    |

## Host Summary

This table displays information about the host summary. Use this chart to view information about the host performance.

| Column Name            | Description                                       |
|------------------------|---------------------------------------------------|
| Total IO Time          | The aggregated IO time statistics for the volume. |
| Total CPU System Time  | The total CPU system time used by all processes.  |
| CPU Busy               | The total percentage of CPU utilization.          |
| Total Connection Count | The number of current connections per instance.   |
| Idle Connection Count  | The number of idle connections per instance.      |

## Services Summary

This table displays information about the SAP HANA services. Use this chart to view information about the performance of internal services and how the requests are handled.

| Column Name                               | Description                                                                                                                                       |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Pending Requests                          | The total number of pending requests for the connection to the HANA service.                                                                      |
| Request Response Time                     | The average request response time for the last 1000 requests.                                                                                     |
| Service Status                            | The operational state of the SAP HANA system. Possible values are (0 - No, 1 - Yes, 2 - Unknown, 3 - Starting, 4 - Stopping)                      |
| Coordinator type in distributed landscape | The state of the coordinator type of the Dynamic Tiering Service. Possible values are (0 - Master, 1 - Slave, 2 - Standby, 3 - None, 4 - Unknown) |
| Requests Per Second                       | The average of last 1000 requests.                                                                                                                |

## CPU and Memory Performance

This table displays information about the CPU and memory performance. Use this chart to view information about the overall performance of the HANA system.

| Column Name          | Description                                                |
|----------------------|------------------------------------------------------------|
| CPU Usage            | The total CPU usage by the current process.                |
| Logical Memory Usage | The logical memory usage by the service.                   |
| Total Memory Size    | The total allocation limit for all processes.              |
| Total Memory Usage   | The total size of available memory.                        |
| Shared Memory Used   | The amount of shared pool memory that is currently in use. |



## Log and Data Backup Status

This table displays information about the log and data Backup status. Use this chart to view information about data and log backups that are the key components for HANA system performance.

| Column Name                 | Description                                                                                                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Missing Status          | The state of missing log backups at a particular instance of time. Possible values are (0 - successful, 1 - Failed, 2 - Running, 3 - Cancel Pending, 4 - Cancelled)           |
| Log Backup Status           | The state of the SAP HANA redo log backups at a particular instance of time. Possible values are (0 - successful, 1 - Failed, 2 - Running, 3 - Cancel Pending, 4 - Cancelled) |
| Data Snapshot Status        | The state of the Storage snapshot at a particular instance of time. Possible values are (0 - successful, 1 - Failed, 2 - Running, 3 - Cancel Pending, 4 - Cancelled)          |
| Complete Data Backup Status | The complete data backup of HANA system which includes data and log. Possible values are (0 - successful, 1 - Failed, 2 - Running, 3 - Cancel Pending, 4 - Cancelled)         |

## DB Usage Summary

This table displays information about the SAP HANA database usage.

| Column Name          | Description                             |
|----------------------|-----------------------------------------|
| Max Peak Used Memory | The highest used memory value recorded. |

## SAP\_Basis NetWeaver Unified Dashboard

The sap\_basis NetWeaver Unified Dashboard provides predefined list views to monitor the health and performance of SAP NetWeaver.

### Contents

#### NOTE

: If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### SAP\_Basis NetWeaver Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the SAP\_Basis NetWeaver dashboard. An asterisk (\*) means that this QoS brings data for all targets for which it is applicable.

| QoS                                        | Subkey/Target |
|--------------------------------------------|---------------|
| QOS_SAP_NW_KERNEL_APP_THREAD_COUNT         | *             |
| QOS_SAP_NW_KERNEL_AVG_MS_PROCESS_TIME      | *             |
| QOS_SAP_NW_KERNEL_CURRENT_SECURITY_SESSION | *             |
| QOS_SAP_NW_KERNEL_CURRENT_HTTP_SESSION     | *             |

| QoS                                          | Subkey/Target |
|----------------------------------------------|---------------|
| QOS_SAP_NW_KERNEL_LOGGED_IN_USER             | *             |
| QOS_SAP_NW_KERNEL_SYSTEM_THREADS_COUNT       | *             |
| QOS_SAP_NW_KERNEL_THREAD_POOL_USAGE          | *             |
| QOS_SAP_NW_KERNEL_CONC_GC_RATIO              | *             |
| QOS_SAP_NW_KERNEL_GC_RATIO                   | *             |
| QOS_SAP_NW_KERNEL_GC_SPIN_HEAP               | *             |
| QOS_SAP_NW_KERNEL_GC_SPIN_PERM               | *             |
| QOS_SAP_NW_PERFORMANCE_CPU_UTILIZATION       | *             |
| QOS_SAP_NW_PERFORMANCE_FREE_DISK_SPACE       | *             |
| QOS_SAP_NW_PERFORMANCE_FREE_DISK_SPACE_GB    | *             |
| QOS_SAP_NW_PERFORMANCE_MEMORY_UTILIZATION    | *             |
| QOS_SAP_NW_PERFORMANCE_TOTAL_DISK_SPACE_GB   | *             |
| QOS_SAP_NW_SERVICES_ALL_REQUEST_COUNT        | *             |
| QOS_SAP_NW_SERVICES_AVAILABLE_MEMORY         | *             |
| QOS_SAP_NW_SERVICES_USED_MEMORY              | *             |
| QOS_SAP_NW_SERVICES_UNSUCCESSFUL_LOGON_COUNT | *             |
| QOS_SAP_NW_KERNEL_AVG_MS_PROCESS_TIME        | *             |

For more information about configuring probes, see the documentation for each probe.

### Kernel Summary

This table displays information about the NetWeaver Kernel statistics. Use this chart to view information about the current system statistics for the internal processes.

| Column Name               | Description                                             |
|---------------------------|---------------------------------------------------------|
| Active Threads            | The total number of currently active system threads.    |
| Average Process Time      | The average processing time of the message server.      |
| Current Security Sessions | The total number of currently active security sessions. |
| Current HTTP Sessions     | The total number of currently active HTTP sessions.     |
| Logged-In Users           | The total number of logged-in users.                    |
| System Threads            | The total number of currently active system threads.    |
| Thread Pool Usage         | The ratio of active threads count to maximum pool size. |

### **Kernel JVM Summary**

This table displays information about the NetWeaver Kernel JVM statistics. Use this chart to view information about the heap performance.

| Column Name                        | Description                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Concurrent GC Ratio                | The ratio of the time spent during garbage collection in comparison with the overall runtime of the JVM during the last five minutes.                          |
| GC Ratio                           | The ratio of time spent on garbage collector to JVM runtime during last five minutes.                                                                          |
| GC Spinning Due to Java Heap       | The count of concurrent garbage collector spins due to heap above threshold during last five minutes.                                                          |
| GC Spinning Due to Perm Generation | The number of times the concurrent garbage collector spinned due to the permanent generation being above the corresponding threshold during last five minutes. |

### **Performance Summary**

This table displays information about the NetWeaver Performance statistics. Use this chart to view information about the utilization statistics of disk and memory.

| Column Name        | Description                                        |
|--------------------|----------------------------------------------------|
| CPU Utilization    | The total CPU utilization.                         |
| Free Disk Space    | The percentage of free disk space.                 |
| Free Disk Space GB | The total free disk space.                         |
| Memory Utilization | The total system memory utilization.               |
| Total Disk Space   | The total free space for every instance directory. |

### **Services Summary**

This table displays information about the NetWeaver services statistics. Use this chart to view information about the internal functioning and request handling.

| Column Name                 | Description                                                     |
|-----------------------------|-----------------------------------------------------------------|
| All Requests Count          | The total number of requests received since server startup.     |
| Java Available Memory       | The total memory available for the JAVA instance.               |
| Java Used Memory            | The total memory utilized by the JAVA instance.                 |
| Unsuccessful Logon Attempts | The number of unsuccessful login attempts since server startup. |
| Average Processing Time     | The average request processing time.                            |

## **SAP\_Basis Oracle Database Unified Dashboard**

The sap\_basis Oracle Database Unified Dashboard provides predefined list views to monitor the health and performance of the Oracle Database in the SAP landscape.

### **Contents**

**NOTE**

: If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**SAP\_Basis Oracle Database Required Data Sources**

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the SAP\_Basis Oracle Database dashboard. An asterisk (\*) means that this QoS brings data for all targets for which it is applicable.

| QoS                                              | Subkey/Target |
|--------------------------------------------------|---------------|
| QOS_SAP_ORACLE_AVAILABILITY                      | *             |
| QOS_SAP_ORACLE_DATABASE_SIZE                     | *             |
| QOS_SAP_ORACLE_USED_SPACE                        | *             |
| QOS_SAP_ORACLE_DAILY_GROWTH                      | *             |
| QOS_SAP_ORACLE_LAST_SUCCESSFUL_UPDATE_STATISTICS | *             |
| QOS_SAP_ORACLE_LAST_SUCCESSFUL_BACKUP            | *             |
| QOS_SAP_ORACLE_LAST_BACKUP_STATUS                | *             |
| QOS_SAP_ORACLE_BUFFER_CACHE                      | *             |
| QOS_SAP_ORACLE_LIBRARY_CACHE                     | *             |
| QOS_SAP_ORACLE_TRANSACTION_LOCK_AGE              | *             |
| QOS_SAP_ORACLE_ARCHIVING_LAST_STATUS             | *             |
| QOS_SAP_ORACLE_ARCHIVING_DEST_FULL               | *             |
| QOS_SAP_ORACLE_FREE_TABLE_SPACE                  | *             |
| QOS_SAP_ORACLE_USED_TABLE_SPACE                  | *             |

For more information about configuring probes, see the documentation for each probe.

**Oracle Database Summary**

This table displays information about the Oracle Database statistics. Use this chart to view information about the database performance.

| Column Name                           | Description                                                                        |
|---------------------------------------|------------------------------------------------------------------------------------|
| Availability                          | The percentage availability of Oracle database.                                    |
| DB Size                               | The total size of Oracle database.                                                 |
| Used Space                            | The total size of currently utilized space in the Oracle database.                 |
| Daily Growth                          | The growth of utilized memory space in the Oracle database since the previous day. |
| Last Successful Update Statistics Run | The total number of days since the last successful Oracle database update.         |
| Last Successful DB Backup             | The total number of days since the last successful Oracle database backup update.  |
| Last DB Backup Status                 | The status of the last backup.                                                     |

## Oracle Database Performance

This table displays information about the health and performance of Oracle Database.

| Column Name                         | Description                                                                  |
|-------------------------------------|------------------------------------------------------------------------------|
| Buffer Cache Hit Ratio              | The percentage of utilized Oracle buffer cache                               |
| Library Cache Hit Ratio             | The percentage of utilized Oracle library cache.                             |
| Exclusive Transaction Lock Age      | The longest time a transaction lock has been held in exclusive mode.         |
| Archiving Status                    | The total number of databases in No Archive Log status.                      |
| Archiver Destination Remaining Size | The number of Archive logs that will still fit into the archiving directory. |

## Oracle Tablespace Details

This table displays information about the Oracle tablespace. Use this chart to view information about the storage space.

| Column Name             | Description                                                 |
|-------------------------|-------------------------------------------------------------|
| Tablespace - Free Space | The amount of free space in the Oracle table space.         |
| Tablespace - Used Space | The percentage of utilized space in the Oracle table space. |

## SAP\_Basis Unified Dashboard

The sap\_basis Unified Dashboard provides predefined list views to monitor the health and performance of the SAP landscape.

### Contents

#### NOTE

: If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### SAP\_Basis Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the SAP\_Basis dashboard. An asterisk (\*) means that this QoS brings data for all targets for which it is applicable.

| QoS                                       | Subkey/Target |
|-------------------------------------------|---------------|
| QOS_SAP_INSTANCE_STATUS                   | *             |
| QOS_SAP_AS_MEMORY_SIZE_OF_EXTENDED_MEMORY | *             |
| QOS_SAP_AS_MEMORY_HEAP_SIZE               | *             |
| QOS_SAP_OS_COLLECTOR_STATE                | *             |
| QOS_SAP_AS_CPU_UTILIZATION                | *             |
| QOS_SAP_AS_PAGE_IN                        | *             |
| QOS_SAP_AS_PAGE_OUT                       | *             |

| QoS                                    | Subkey/Target |
|----------------------------------------|---------------|
| QOS_SAP_RESPONSE_TIME_DIALOG           | *             |
| QOS_SAP_DB_REQUEST_TIME                | *             |
| QOS_SAP_DB_FRONT_END_RESP_TIME         | *             |
| QOS_SAP_LOAD_GEN_TIME                  | *             |
| QOS_SAP_WPS_IN_PRIV_MODE               | *             |
| QOS_SAP_WP_RESTARTS                    | *             |
| QOS_SAP_DIALOG_UTILISATION             | *             |
| QOS_SAP_R3ABAP_SHORT_DUMPS             | *             |
| QOS_SAP_AS_BUFFER_HIT_RATIO            | *             |
| QOS_SAP_AS_BUFFER_SWAP                 | *             |
| QOS_SAP_SPOOL_SERVICE_STATUS           | *             |
| QOS_SAP_SPOOL_SERVICE_WAIT_TIME        | *             |
| QOS_SAP_SPOOL_SERVICE_UTILISATION      | *             |
| QOS_SAP_SERVICES_ALLOCATED_MEMORY      | *             |
| QOS_SAP_SYSTEM_THREADS_COUNT           | *             |
| QOS_SAP_CURRENT_HTTP_SESSION           | *             |
| QOS_SAP_PERFORMANCE_AVG_RESP_TIME      | *             |
| QOS_SAP_AS_LAN_ERRORS_IN               | *             |
| QOS_SAP_AS_LAN_ERRORS_OUT              | *             |
| QOS_SAP_AS_FILE_FREE_SPACE             | *             |
| QOS_SAP_AS_FILE_PERCENTAGE_USED        | *             |
| QOS_SAP_RFC_CPICERR_ERROR              | *             |
| QOS_SAP_RFC_SYSFAIL_ERROR              | *             |
| QOS_SAP_RFC_SYSLOAD_ERROR              | *             |
| QOS_SAP_RFC_IN_TOTAL_CALLS             | *             |
| QOS_SAP_SHARED_MEMORY_FOR_ALL_VMS      | *             |
| QOS_SAP_VM_NUMBER_IN_POOL              | *             |
| QOS_SAP_VM_AVAILABLE                   | *             |
| QOS_SAP_VM_HEAP_SIZE                   | *             |
| QOS_SAP_VM_EFFECTIVE_CPU_USAGE         | *             |
| QOS_SAP_VM_MAX_GC_RATE                 | *             |
| QOS_SAP_VM_SHARED_MEMORY_FRAGMENTATION | *             |
| QOS_SAP_ICM_CACHE_ENTRIES_USED         | *             |
| QOS_SAP_ICM_CACHE_SIZE_USED            | *             |
| QOS_SAP_ICM_NO_OF_THREAD               | *             |
| QOS_SAP_ICM_NO_OF_CONNECTIONS          | *             |
| QOS_SAP_ICM_QUEUE_LEN                  | *             |
| QOS_SAP_AS_LAN_PACKETS_IN              | *             |
| QOS_SAP_AS_LAN_PACKETS_OUT             | *             |
| QOS_SAP_NUMBER_CONCURRENT_USERS        | *             |

For more information about configuring probes, see the documentation for each probe.

### **ICM Communication**

This table displays information about various parameters to monitor the status of ICM and to detect any possible errors.

| Column Name           | Description                                                   |
|-----------------------|---------------------------------------------------------------|
| Cache Entries Used    | The percentage utilization of HTTP Server cache entries.      |
| Cache Size Used       | The total used memory of the HTTP Server cache.               |
| Number of Threads     | The total number of worker threads that are currently active. |
| Number of Connections | The number of connections that are currently open.            |
| Queue Length          | The total number of entries in the request queue of ICM.      |

### **System Availability**

This table displays information about the availability of the monitored SAP Systems and instances.

| Column Name                | Description                         |
|----------------------------|-------------------------------------|
| SAP System Instance Status | The status of SAP system instances. |

### **SAP OS Collector**

This table displays information about the operating system resources such as utilization of physical disks for a SAP instance.

| Column Name          | Description                                                                            |
|----------------------|----------------------------------------------------------------------------------------|
| Extended Memory Size | The total size of extended memory in the system.                                       |
| Heap Memory size     | The percentage utilization of heap memory.                                             |
| OS Collector State   | The status of the OS collector.                                                        |
| CPU Utilization      | The total CPU utilized by the system related activities at the Operating System level. |
| Memory Page In       | The total number of pages paged in.                                                    |
| Memory Page Out      | The total number of pages paged out.                                                   |

### **ABAP System Performance**

This table displays the information about different SAP tasks to be monitored for the performance of a system. .

| Column Name             | Description                                                       |
|-------------------------|-------------------------------------------------------------------|
| Response Time Dialog    | The average Response Time in Dialog Mode.                         |
| DB Request Time         | The average Database Response time in Dialog Mode.                |
| Front End Response Time | The average Frontend Response time in Dialog Mode.                |
| Load Generation time    | The average Load Generation time in Dialog Mode.                  |
| Priv WP Number          | The number of Dialog (DIA) Work processes in <b>Private</b> mode. |
| WP Restart              | The number of Dialog (DIA) Work Processes that restarted.         |

| Column Name           | Description                                                |
|-----------------------|------------------------------------------------------------|
| Dialog Utilisation    | The percentage utilization of Dialog (DIA) Work Processes. |
| Short Dumps Frequency | The total number of Short Dumps in ABAP per minute.        |

### **SAP Buffer**

This table displays information about the SAP Buffer. Use this chart to ensure that there is more hit ratio for the buffers and less swaps for efficient performance of the SAP system.

| Column Name      | Description                                                                  |
|------------------|------------------------------------------------------------------------------|
| Buffer Hit Ratio | The measure of buffer quality.                                               |
| Buffer Swap      | The buffered objects swapped due to more memory requirement for new objects. |

### **Spool Service Status**

This table displays information about the status of the Output Server. Use this chart to view information about the utilization of the spool system.

| Column Name                | Description                                              |
|----------------------------|----------------------------------------------------------|
| Spool Service Status       | The service status for an output server.                 |
| Spool Service Wait Time    | The wait time for spool services.                        |
| Work Processes Utilization | The percentage utilization of Background Work Processes. |

### **Java System Performance**

This table displays information about memory configuration for a SAP instance. Use this chart to view information about the Java monitoring of SAP Landscape

| Column Name                         | Description                                            |
|-------------------------------------|--------------------------------------------------------|
| Java VM Allocated Memory            | The total amount of Memory allocated to Java Services. |
| Kernal - System Thread Count        | The total number of currently active system threads.   |
| Service - Current HTTP Session      | The total number of currently active HTTP sessions.    |
| Performance - Average Response Time | The average response time of the SAP system.           |

### **LAN Performance**

This table displays information about the Utilization Capacity of the SAP system. Use this chart to view information about the number of data packets in error during receiving and sending process.

| Column Name          | Description                                                                |
|----------------------|----------------------------------------------------------------------------|
| Error in Packets In  | The errors per second for the data packets sent by the server.             |
| Error in Packets Out | The errors per second for the data packets received by the server.         |
| Packets In           | The total number of incoming packets per second to a LAN of a host system. |
| Packets Out          | The total number of outgoing packets per second to a LAN of a host system. |



## **File System Overview**

This table displays information about File System performance on the SAP system. Use this chart to view information about the available storage space in your file systems.

| Column Name             | Description                                                      |
|-------------------------|------------------------------------------------------------------|
| File System Free Space  | The free amount of hard disk space.                              |
| File System Utilization | The total utilized disk space for the file system in percentage. |

## **ALE/Doc Monitoring**

This table displays information about the transactional RFC and queued RFC. Use this information to view the data transfer between different systems.

| Column Name                         | Description                                        |
|-------------------------------------|----------------------------------------------------|
| tRFC Calls w/Communication Errors   | The total number of calls with status CPICERR.     |
| tRFC Calls w/Execution Errors       | The total number of calls with status SYSFAIL.     |
| tRFC Calls w/o RFC Server Resources | The total number of calls with status SYSLOAD.     |
| tRFC/qRFC Total Calls               | The total number of calls in the ARFCRSTATE table. |

## **Virtual Machine Controller**

This table displays information about the status of the Java virtual machines (VMs) in the VM Container on the SAP Server. Use this information to manage the VM Container and the individual VMs at runtime.

| Column Name                 | Description                                                             |
|-----------------------------|-------------------------------------------------------------------------|
| Shared Memory               | The total shared memory for all VMs.                                    |
| Total Number of VMs         | The total number of VMs in the pool.                                    |
| VMs Available               | The total number of available VMs.                                      |
| Java Heap Size              | The total size of java heap for each VM.                                |
| Effective CPU Usage         | The average of effective CPU utilization for garbage collection of VMs. |
| Max GC Rate                 | The maximum frequency of garbage collector runs of individual VMs.      |
| Shared Memory Fragmentation | The percentage of fragmentation of shared memory.                       |

## **Logged In Users**

This table displays information about the total number of currently logged-in users on the same SAP client.

| Column Name      | Description                                                       |
|------------------|-------------------------------------------------------------------|
| Concurrent Users | The total number of currently logged-in users on the same client. |

## **Server Unified Dashboard**

The Server Unified Dashboard provides predefined list views with information about server performance, such as CPU, memory, disk space usage, and server load.

## Contents

### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### Server Required Data Sources

The table contains the probes and QoS metrics required for the preconfigured Server dashboard.

| Probe | QoS Required                                                                        |
|-------|-------------------------------------------------------------------------------------|
| cdm   | QOS_CPU_USAGE<br>QOS_PROC_QUEUE_LEN<br>QOS_DISK_USAGE_PERC<br>QOS_MEMORY_PERC_USAGE |

### Current Server Performance

| Column             | Description                                    |
|--------------------|------------------------------------------------|
| Host               | Name of the server.                            |
| CPU Usage Last 6hr | Percent of CPU consumed over the last 6 hours. |
| CPU Usage          | Percent of CPU in use.                         |
| Memory Usage       | Percent of memory in use.                      |

### Server Load 1 hour average

| Column                     | Description                                              |
|----------------------------|----------------------------------------------------------|
| Host                       | Name of the server.                                      |
| 1 hr Avg CPU Usage         | Average percent of CPU consumed during the past hour.    |
| 1 hr Avg Proc Queue Length | Average number of processes queued during the past hour. |

### Server Disk Space Usage

| Column       | Description                     |
|--------------|---------------------------------|
| Host         | Name of the server.             |
| Disk         | Disk being monitored.           |
| Percent Used | Percent of disk space consumed. |

## Storage Unified Dashboard

The Storage unified dashboards provide out of the box dashboards with key performance and capacity information for storage devices.

You can use this data to spot potential performance issues and get an early warning of potential capacity issues and avoid downtime. The storage dashboard provides a unified view of various types of storage devices. The storage devices supported include the following:

- EMC Celerra series
- EMC Clariion series
- EMC VNX series
- EMC VMAX/DMX series

**Contents**

**NOTE**

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**Storage Required Data Sources**

The table contains the probes and QoS metrics required for the preconfigured Storage dashboard.

| Probe                                                                                                            | QoS Required                                                   |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| clariion                                                                                                         | QOS_STORAGE_NUMBER_OF_DEVICES                                  |
| netapp                                                                                                           | QOS_STORAGE_DISK_CAPACITY                                      |
| celerra                                                                                                          | _STORAGE_SP_BLOCKS_READ_PER_SECOND                             |
| vmax                                                                                                             | _STORAGE_DISK_READ                                             |
| ibm                                                                                                              | System Statistics.Disk Read                                    |
| <b>Note:</b> Not all of these probes are required. The reports look for one or more of the probes if they exist. | _STORAGE_DISK_READ_KB_PER_SEC                                  |
|                                                                                                                  | System Statistics.Disk Read                                    |
|                                                                                                                  | _STORAGE_SP_BLOCKS_READ_PER_SECOND<br>SP B                     |
|                                                                                                                  | _STORAGE_SP_BLOCKS_READ_PER_SECOND<br>SP A                     |
|                                                                                                                  | _STORAGE_SP_BLOCKS_READ_PER_SECOND<br>SP A                     |
|                                                                                                                  | _STORAGE_SP_BLOCKS_READ_PER_SECOND<br>SP B                     |
|                                                                                                                  | _STORAGE_SP_BLOCKS_READ_PER_SECOND<br>SP A                     |
|                                                                                                                  | _STORAGE_DISK_READ<br>System Statistics.Disk Read              |
|                                                                                                                  | _STORAGE_DISK_READ<br>System Statistics.Disk Read              |
|                                                                                                                  | _STORAGE_DISK_READ<br>System Statistics.Disk Read              |
|                                                                                                                  | _STORAGE_DISK_WRITE<br>System Statistics.Disk Write            |
|                                                                                                                  | _STORAGE_DISK_WRITE_KB_PER_SEC<br>System Statistics.Disk Write |

```
_STORAGE_SYMM_DISK_KB_WRITE_PER_SEC
_STORAGE_SYMM_DISK_KB_WRITE_PER_SEC
_STORAGE_DISK_WRITE
 System Statistics.Disk Write
_STORAGE_DISK_WRITE
 System Statistics.Disk Write
_STORAGE_DISK_WRITE
 System Statistics.Disk Write
_STORAGE_IOPS
 System Statistics.IOPS
_STORAGE_SP_READ_IOPS
 SP A
_STORAGE_SP_WRITE_IOPS
 SP A
_STORAGE_SP_WRITE_IOPS
 SP A
_STORAGE_SP_READ_IOPS
 SP A
_STORAGE_SP_WRITE_IOPS
 SP A
_STORAGE_SP_READ_IOPS
 SP A
_STORAGE_SP_WRITE_IOPS
 SP B
_STORAGE_SP_READ_IOPS
 SP B
_STORAGE_SP_WRITE_IOPS
 SP A
_STORAGE_SP_READ_IOPS
 SP A
_STORAGE_SP_WRITE_IOPS
 SP B
_STORAGE_SP_READ_IOPS
 SP B
_STORAGE_SP_WRITE_IOPS
 Unknown
_STORAGE_SP_READ_IOPS
 Unknown
_STORAGE_SP_WRITE_IOPS
 SP B
_STORAGE_SP_WRITE_IOPS
 SP A
```

|                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| _STORAGE_SP_READ_IOPS<br>SP B<br>_STORAGE_SP_READ_IOPS<br>SP A<br>_STORAGE_SP_READ_IOPS<br>SP B<br>_STORAGE_SP_WRITE_IOPS<br>SP B<br>_STORAGE_SP_READ_IOPS<br>SP A<br>_STORAGE_SP_WRITE_IOPS<br>SP A<br>_STORAGE_IOPS<br>System Statistics.IOPS<br>_STORAGE_IOPS<br>System Statistics.IOPS<br>_STORAGE_IOPS<br>System Statistics.IOPS |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Storage IOPS**

This view displays the I/O performance of a storage system as the number of I/O operations per second. This performance metric is critical to understanding bottlenecks or throughput in a storage array system.

| Chart        | Description                                                                                  |
|--------------|----------------------------------------------------------------------------------------------|
| Storage IOPS | This chart portrays the overall Number of I/O operations per second for every storage array. |

**Storage IO Data Rate**

This view displays the overall data bandwidth measured as average disks read and write (I/O) data rate in kilobits (Kb) per second of all discovered storage systems.

| Chart               | Description                                                                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disks Reads Kb/sec  | This displays overall disk data reads in Kb per sec for each discovered and monitored storage system. This indicates storage bandwidth and speed of Data access.   |
| Disks Writes Kb/Sec | This displays overall disk data writes in Kb per sec for each discovered and monitored storage system. This indicates storage bandwidth and speed of Data storage. |

**Storage Systems Status**

This view displays the status of all discovered storage systems.

| Column          | Description                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
| Storage Systems | This lists the host or controller IP address of host name of all discovered and monitored storage systems.                 |
| Alarm Status    | This shows the alarms from all discovered and monitored storage systems with standard color scheme pertaining to severity. |

## Number of Storage Devices

This list view displays the number of storage devices in each discovered storage system.

| Column                | Description                                                                              |
|-----------------------|------------------------------------------------------------------------------------------|
| Storage Systems       | This lists the host name or IP address of each discovered and monitored storage system.  |
| Storage Array         | This lists the storage array names from the above storage systems.                       |
| Total Storage Devices | This lists the number of logical storage devices i.e. LUNs in the above storage systems. |

## Storage Systems Physical Disks

This list view displays the number of physical disks in each discovered storage system.

| Columns           | Description                                                                                                                                         |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage Systems   | This lists the host name or IP address of each discovered and monitored storage system.                                                             |
| Physical Storage  | This lists the storage array or chassis/enclosure name of each discovered and monitored storage system.                                             |
| Total Disks Count | This lists the number of physical disks discovered in each storage array or chassis/enclosure name of each discovered and monitored storage system. |

## Vblock Unified Dashboard

The Vblock Unified Dashboard provides six predefined list views with performance and status information about Vblock Infrastructure Platforms.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

**Vblock Required Data Sources**

The table contains the probes and QoS metrics required for the preconfigured Vblock dashboard.

| Probe                                                                                                                                                                       | QoS Required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vmware<br>clariion<br>cisco_ucs<br>interface_traffic<br><b>Note:</b> Not all of these probes are required.<br>The reports look for one or more of the probes if they exist. | QOS_INTERFACE_TRAFFIC<br>IN-Vethernet1Nexus 1K<br>IN-Vethernet2Nexus 1K<br>IN-Vethernet3Nexus 1K<br>IN-Vethernet4Nexus 1K<br>IN-Vethernet5Nexus 1K<br>IN-Vethernet6Nexus 1K<br>IN-Vethernet7Nexus 1K<br>IN-Vethernet8Nexus 1K<br>IN-Vethernet9Nexus 1K<br>IN-Vethernet10Nexus 1K<br>IN-Vethernet12Nexus 1K<br>IN-Vethernet15Nexus 1K<br>IN-Vethernet17Nexus 1K<br>IN-Vethernet18Nexus 1K<br>IN-Vethernet19Nexus 1K<br>IN-Vethernet20Nexus 1K<br><br>QOS_INTERFACE_TRAFFIC<br>OUT-Vethernet1Nexus 1K<br>OUT-Vethernet2Nexus 1K<br>OUT-Vethernet3Nexus 1K<br>OUT-Vethernet4Nexus 1K<br>OUT-Vethernet5Nexus 1K<br>OUT-Vethernet6Nexus 1K<br>OUT-Vethernet7Nexus 1K<br>OUT-Vethernet8Nexus 1K<br>OUT-Vethernet9Nexus 1K<br>OUT-Vethernet10Nexus 1K<br>OUT-Vethernet12Nexus 1K<br>OUT-Vethernet15Nexus 1K<br>OUT-Vethernet17Nexus 1K<br>OUT-Vethernet18Nexus 1K<br>OUT-Vethernet19Nexus 1K<br>OUT-Vethernet20<br>QOS_STORAGE_SP_PCT_BUSY<br>SP A<br>SP B |

QOS\_STORAGE\_FAST\_CACHE\_PCT\_DIRTY\_SPA  
FAST Cache

QOS\_STORAGE\_FAST\_CACHE\_PCT\_DIRTY\_SPB  
FAST Cache

QOS\_STORAGE\_SP\_PCT\_DIRTY  
SP A

QOS\_STORAGE\_FAST\_CACHE\_PCT\_DIRTY\_SPB  
FAST Cache

QOS\_STORAGE\_FAST\_CACHE\_PCT\_DIRTY\_SPA  
FAST Cache

QOS\_STORAGE\_TP\_PERCENT\_SUBSCRIBED  
DQA-FC-01  
DQA-GP-01  
Prod-GP-01  
Test\_Pool

QOS\_STORAGE\_TP\_PERCENT\_AVAILABLE  
DQA-FC-01  
DQA-GP-01  
Prod-GP-01  
Test\_Pool

QOS\_STORAGE\_TP\_PERCENT\_FULL  
DQA-FC-01  
DQA-GP-01  
Prod-GP-01  
Test\_Pool

QOS\_STORAGE\_TP\_SUBSCRIBED\_CAPACITY  
DQA-FC-01

QOS\_STORAGE\_TP\_AVAILABLE\_CAPACITY  
DQA-FC-01  
DQA-GP-01  
Prod-GP-01  
Test\_Pool



QOS\_STORAGE\_TP\_SUBSCRIBED\_CAPACITY  
DQA-GP-01  
Prod-GP-01  
Test\_Pool

QOS\_STORAGE\_TP\_CONSUMED\_CAPACITY  
DQA-FC-01  
DQA-GP-01  
Prod-GP-01  
Test\_Pool

QOS\_STORAGE\_TP\_USER\_CAPACITY  
DQA-FC-01  
DQA-GP-01  
Prod-GP-01  
Test\_Pool

QOS\_UCS\_POWER  
Consumed Power (sys/chassis-1/blade-1/board/power-  
stats)  
Consumed Power (sys/chassis-1/blade-6/board/power-  
stats)  
Consumed Power (sys/chassis-1/blade-5/board/power-  
stats)  
Consumed Power (sys/chassis-1/blade-7/board/power-  
stats)  
Consumed Power (sys/chassis-1/blade-8/board/power-  
stats)

QOS\_UCS\_POWER  
Consumed Power (sys/chassis-2/blade-1/board/power-  
stats)  
Consumed Power (sys/chassis-2/blade-2/board/power-  
stats)  
Consumed Power (sys/chassis-2/blade-3/board/power-  
stats)  
Consumed Power (sys/chassis-2/blade-4/board/power-  
stats)  
Consumed Power (sys/chassis-2/blade-5/board/power-  
stats)  
Consumed Power (sys/chassis-2/blade-6/board/power-  
stats)  
Consumed Power (sys/chassis-2/blade-7/board/power-  
stats)  
Consumed Power (sys/chassis-2/blade-8/board/power-  
stats)

QOS\_UCS\_POWER  
Consumed Power (sys/chassis-3/blade-6/board/power-  
stats)  
Consumed Power (sys/chassis-3/blade-7/board/power-  
stats)  
Consumed Power (sys/chassis-3/blade-8/board/power-  
stats)  
Consumed Power (sys/chassis-3/blade-5/board/power-  
stats)

QOS\_UCS\_TEMPERATURE  
Ambient Temperature (sys/chassis-2/slot-1/stats)

QOS\_UCS\_TEMPERATURE  
Ambient Temperature (sys/chassis-2/slot-1/stats)

|                                       |                                                    |
|---------------------------------------|----------------------------------------------------|
| QOS_UCS_PERFORMANCE                   | Available Memory (sys/switch-A/sysstats)           |
| QOS_UCS_PERFORMANCE                   | Available Memory (sys/switch-B/sysstats)VSC101F140 |
| QOS_UCS_PERFORMANCE                   | Available Memory (sys/switch-A/sysstats)VSC101F140 |
| QOS_UCS_PERFORMANCE                   | Available Memory (sys/switch-B/sysstats)           |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-1/fan-2/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-2/fan-2/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-3/fan-1/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-3/fan-2/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-1/fan-1/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-1/fan-2/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-2/fan-2/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-3/fan-1/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-3/fan-2/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-2/fan-module-1-1/fan-1/stats)   |
| QOS_UCS_FAN_SPEED                     | Speed (sys/chassis-1/fan-module-1-1/fan-1/stats)   |
| QOS_MEMORY_PERC_USAGE                 | Resources.MemoryOverallUsage (% of MemoryMaxUsage) |
| QOS_CPU_USAGE                         | Resources.CPUOverallUsage (% of CPUMaxUsage)       |
| QOS_MEMORY_PERC_USAGE                 | Memory Usage                                       |
| QOS_CPU_USAGE                         | CPU Usage (Average/Rate)                           |
| QOS_NETWORK_BYTES_RECEIVED_PER_SECOND | Network Data Receive Rate                          |
| QOS_NETWORK_BYTES_SENT_PER_SECOND     | Network Data Transmit Rate                         |
| QOS_DISK_READ_REQUEST                 | Disk Read Requests                                 |
| QOS_DISK_WRITE_REQUEST                | Disk Write Requests                                |
| QOS_DISK_READ                         | Disk Read Rate                                     |
| QOS_DISK_WRITE                        | Disk Write Rate                                    |
| QOS_DISK_LATENCY                      | Disk Latency                                       |

|  |                                                                                                                                                                                                                                                                      |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | QOS_DS_DISK_FREE<br>QOS_VMWARE_VARIABLE<br>PowerState<br>QOS_MEMORY_PERC_USAGE<br>GuestMemoryUsage (in % of Memory)<br>QOS_MEMORY_PERC_USAGE<br>HostMemoryUsage (in % of Memory)<br>QOS_COUNTER<br>VMCountActive<br>VMCount<br>QOS_MEMORY_PERC_USAGE<br>Memory Usage |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Vblock Storage Performance**

This view displays health and thin pool usage information for the EMC Clariion Storage component of the Vblock Infrastructure Platform.

| Chart                                    | Description                                                                                                                                            |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage Processors (SP) Utilization in % | Percent of SP A and SP B utilization for the entire Vblock Infrastructure Platform storage processed through SP A and SP B.                            |
| Dirty Cache % (Fast Cache)               | Dirty cache as a percent of total for each storage processor in the Clariion component of the Vblock Infrastructure Platform.                          |
| Thin Pool Usage %                        | Percent of allocated thin pool that is subscribed for each thin pool in the Clariion component of the Vblock Infrastructure Platform.                  |
| Thin Pool Capacity in GB                 | Thin pool capacity, in GB, for subscribed and available capacities for each thin pool in the Clariion component of the Vblock Infrastructure Platform. |

**Vblock UCS Performance**

This view displays environment and power information for the Cisco Unified Computing System (UCS) component of the Vblock Infrastructure Platform.

| Chart                                  | Description                                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Consumed Power                         | Number of watts of consumed power for each blade server in each UCS chassis.                                    |
| Temperature                            | Ambient temperature in Celsius for each blade server in each UCS chassis.                                       |
| Fabric Interconnect - Available Memory | Number of megabytes of available memory for each UCS Fabric Interconnect in the Vblock Infrastructure Platform. |
| Fan Speed                              | Fan speed, in RPM, for each fan in each fan module of each UCS chassis.                                         |

**Vblock Nexus Switch Performance**

This view displays network throughput information for the Cisco Nexus Virtual Switch component of the Vblock Infrastructure Platform.

| Chart                    | Description                                                                                     |
|--------------------------|-------------------------------------------------------------------------------------------------|
| Network Traffic Incoming | Number of incoming bytes per second for each virtual Ethernet port in the Nexus Virtual Switch. |
| Network Traffic Outgoing | Number of outgoing bytes per second for each virtual Ethernet port in the Nexus Virtual Switch. |

**Vblock Host Summary**

This view displays performance information about virtual hosts resources.

| Column          | Description                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------|
| VMware Host     | Name of the host in the Vblock Infrastructure Platform.                                                         |
| VM Count Active | Number of virtual machines active on the host.                                                                  |
| VM Count        | Number of virtual machines configured on the host.                                                              |
| CPU Usage       | Percent of CPU in use.<br>0 to 94.99 = Green<br>95 to 96.99 = Yellow<br>97 to 98.99 = Orange<br>99 to 100 = Red |
| Memory Usage    | Percent of memory in use.<br>0 to 69.99 = Green<br>70 to 89.99 = Yellow<br>90 to 100 = Red                      |

**Vblock Datastore Freespace**

This view displays performance and status information about virtual datastore resources.

| Column           | Description                                                                                |
|------------------|--------------------------------------------------------------------------------------------|
| Host             | The host where the datastore resides in the Vblock Infrastructure Platform.                |
| Datastore Name   | The name of the datastore.                                                                 |
| Free Space       | Percent of free disk space available.                                                      |
| Datastore Status | Amount of free space in the datastore.<br>Very low = 0-2%<br>Low = 2.1-5%<br>OK = 5.1-100% |

**Vblock Guest Summary**

This view displays performance and status information about virtual guest resources.

| Column | Description                                                                                        |
|--------|----------------------------------------------------------------------------------------------------|
| Guest  | Lists the virtual machines (guests) configured in your Vblock Infrastructure Platform environment. |

|                   |                                                                                                              |
|-------------------|--------------------------------------------------------------------------------------------------------------|
| Power Status      | Whether the guest is powered on, off, or on standby.                                                         |
| CPU Usage         | Number of megahertz of CPU consumed by the guest.                                                            |
| Memory Usage      | Percent of memory consumed on the guest. This could exceed 100 percent if additional resources are consumed. |
| Host Memory Usage | Percent of memory consumed on the host.                                                                      |
| Alarm             | Lists alarms for the guest.                                                                                  |

## VCloud Unified Dashboard

The VCloud Unified Dashboard provides six predefined list views for monitoring Virtual Data Centers (VDCs). The first three list views monitor memory, CPU, and storage on the organizational VDCs. The last three list views monitor memory, CPU, and storage on the provider VDCs. For organizational VDCs the usages are displayed as percent of the limit. For the provider VDCs the usages are displayed as percent of the capacity.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### VCloud Required Data Sources

The table contains the probes and QoS metrics required for the preconfigured VCloud dashboard. The UMP Dashboards template, found in the vcloud probe configuration UI, includes these QoS measurements and is provided to assist you in configuring the vcloud probe for the dashboard.

| Probe  | QoS Required                  |
|--------|-------------------------------|
| vcloud | QOS_ORG_VDC_STORAGE_USED_PCT  |
|        | QOS_PROV_VDC_MEMORY_USED_PCT  |
|        | QOS_PROV_VDC_CPU_USED_PCT     |
|        | QOS_PROV_VDC_STORAGE_USED_PCT |
|        | QOS_ORG_VDC_MEMORY_USED_PCT   |
|        | QOS_ORG_VDC_CPU_USED_PCT      |

### VCloud Organization VDCs CPU Used Percent

This view displays CPU usage information for your organization's virtual datacenters (VDCs).

| Column                            | Description                                                                                                                                                        |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VCloud Director Host              | IP address or name of host where the VMware vCloud Director software is running.                                                                                   |
| VCloud Director Organization VDCs | Name of the organization VDC managed by the vCloud Director.                                                                                                       |
| CPU Used Last Hour Percent        | CPU (as percent of limit) used during the last hour for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red |

|                                |                                                                                                                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU Used Last 24 Hours Percent | CPU (as percent of limit) used during the last 24 hours, displayed in 1-hour increments, for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### **VCloud Organization VDCs Memory Used Percent**

This view displays memory usage information for your organization's virtual datacenters (VDCs).

| Column                            | Description                                                                                                                                                                                                |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VCloud Director Host              | IP address or name of host where the VMware vCloud Director software is running.                                                                                                                           |
| VCloud Director Organization VDCs | Name of the organization VDC managed by the vCloud Director.                                                                                                                                               |
| Memory Used Last Hour Percent     | Memory (as percent of limit) used during the last hour for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red                                      |
| Memory Used Last 24 Hours Percent | Memory (as percent of limit) used during the last 24 hours, displayed in 1-hour increments, for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red |

### **VCloud Organization VDCs Storage Used Percent**

This view displays storage usage information for your organization's virtual datacenters (VDCs).

| Column                             | Description                                                                                                                                                                                                 |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VCloud Director Host               | IP address or name of host where the VMware vCloud Director software is running.                                                                                                                            |
| VCloud Director Organization VDCs  | Name of the organization VDC managed by the vCloud Director.                                                                                                                                                |
| Storage Used Last Hour Percent     | Storage (as percent of limit) used during the last hour for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red                                      |
| Storage Used Last 24 Hours Percent | Storage (as percent of limit) used during the last 24 hours, displayed in 1-hour increments, for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red |

**VCloud Provider VDCs CPU Used Percent**

This view displays CPU usage information for the virtual datacenters (VDCs) you use that are provided by your cloud services provider.

| Column                         | Description                                                                                                                                                                                                |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VCloud Director Host           | IP address or name of host where the VMware vCloud Director software is running.                                                                                                                           |
| VCloud Director Provider VDCs  | Name of the provider VDC managed by the vCloud Director.                                                                                                                                                   |
| CPU Used Last Hour Percent     | CPU (as percent of capacity) used during the last hour for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red                                      |
| CPU Used Last 24 Hours Percent | CPU (as percent of capacity) used during the last 24 hours, displayed in 1-hour increments, for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red |

**VCloud Provider VDCs Memory Used Percent**

This view displays memory usage information for the virtual datacenters (VDCs) you use that are provided by your cloud services provider.

| Column                            | Description                                                                                                                                                                                                   |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VCloud Director Host              | IP address or name of host where the VMware vCloud Director software is running.                                                                                                                              |
| VCloud Director Provider VDCs     | Name of the provider VDC managed by the vCloud Director.                                                                                                                                                      |
| Memory Used Last Hour Percent     | Memory (as percent of capacity) used during the last hour for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red                                      |
| Memory Used Last 24 Hours Percent | Memory (as percent of capacity) used during the last 24 hours, displayed in 1-hour increments, for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red |

## VCloud Provider VDCs Storage Used Percent

This view displays storage usage information for the virtual datacenters (VDCs) you use that are provided by your cloud services provider.

| Column                             | Description                                                                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VCloud Director Host               | IP address or name of host where the VMware vCloud Director software is running.                                                                                                                               |
| VCloud Director Provider VDCs      | Name of the provider VDC managed by the vCloud Director.                                                                                                                                                       |
| Storage Used Last Hour Percent     | Storage (as percent of capacity) used during the last hour for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red                                      |
| Storage Used Last 24 Hours Percent | Storage (as percent of capacity) used during the last 24 hours, displayed in 1-hour increments, for the systems in the VDC.<br>0 to 70 = Green<br>70 to 80 = Yellow<br>80 to 90 = Orange<br>90 and above = Red |

## VNX Unified Dashboard

The VNX Unified Dashboard provides predefined list views for monitoring the performance of File CPU, IO in block storage performance, file storage summary, block storage IO performance. It also provides a list view to monitor the file storage systems. The VNX dashboard uses metrics from both celerra and clariion probes.

### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### Contents

### VNX Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the VNX dashboard.

| QoS                           | Subkey/ Target |
|-------------------------------|----------------|
| QOS_DMSS_IDLE_CPU_PERCENT     | *              |
| QOS_STORAGE_RAW_FREE_CAPACITY | *              |
| QOS_STORAGE_RAW_USED_CAPACITY | *              |
| QOS_STORAGE_CFG_FREE_CAPACITY | *              |
| QOS_STORAGE_CFG_USED_CAPACITY | *              |
| QOS_STORAGE_SP_IOPS           | *              |



An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

#### NOTE

For more information on configuring probes, see the documentation for each probe.

### **File CPU Performance**

This chart displays information about all the Data Mover System Stats (DMSS) which are being monitored. This chart displays information on the CPU idle time in percentage.

| Column Name         | Description                                                       |
|---------------------|-------------------------------------------------------------------|
| CPU Idle Percentage | Displays the Data Mover System Stats CPU idle time in percentage. |

### **File Storage Summary**

This chart lets you identify the available and used capacity of the raw storage and file system memory of the systems which are being monitored.

| Column Name                   | Description                                       |
|-------------------------------|---------------------------------------------------|
| Raw Storage Free Capacity     | Displays the total raw disk free capacity.        |
| Raw Storage Used Capacity     | Displays the total raw disk used capacity.        |
| File System Free Capacity     | Displays the total configured disk free capacity. |
| File System Utilized Capacity | Displays the total configured disk used capacity. |

### **Block Storage IO Performance**

This chart displays the performance of the input output in the storage system being monitored.

| Column Name         | Description                                                        |
|---------------------|--------------------------------------------------------------------|
| Block IO per Second | Displays the total number of read and write operations per second. |

## **Weblogic Unified Dashboard**

When you monitor applications that run using the Weblogic server, you might encounter issues such as memory leaks and CPU overload. The Weblogic Unified Dashboard enables you to monitor the server components such as JVM heap size, thread count, memory and CPU usage.

### **Contents**

#### NOTE

If the Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and configured so that required the QoS metrics, subkeys and targets are activated.

### **Weblogic Required Data Sources**

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the Weblogic dashboard.

| QoS                       | Subkey/Target |
|---------------------------|---------------|
| QOS_JAVA_HEAP_SIZE        | *             |
| QOS_WEBLOGIC_MEMORY_USAGE | *             |
| QOS_WEBLOGIC_CPU_USAGE    | *             |
| QOS_WEBLOGIC_THREADCOUNT  | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

### **CPU Usage**

This chart displays information about the CPU usage that enables you to monitor whether the CPU load is within threshold.

| Column Name | Description                                |
|-------------|--------------------------------------------|
| CPU Usage   | Percentage of CPU used by Weblogic server. |

### **Memory Heap Size**

This chart displays information about the Memory Heap Size enabling you to detect memory leaks.

| Column Name      | Description                                              |
|------------------|----------------------------------------------------------|
| Memory Heap Size | Maximum size in bytes upto which the Java heap can grow. |

### **Memory Usage**

This chart displays information about the memory usage.

| Column Name  | Description                                |
|--------------|--------------------------------------------|
| Memory Usage | Percentage of used memory and free memory. |

### **Thread Count**

This chart displays information about the Thread Count. Monitoring the thread count is useful in case a thread has been running for longer than required time or if it is stuck in a loop and is consuming memory.

| Column Name  | Description                            |
|--------------|----------------------------------------|
| Thread Count | Average number of threads in the pool. |

## **Websphere MQ Unified Dashboard**

IBM WebSphere MQ (WMQ) is a messaging application for enabling communication between heterogeneous application of an organization network. Your application can connect WMQ to send or receive messages using different protocols, processors, and operating systems. WMQ enables communication in both sender-receiver and publisher-subscriber modes. WMQ consists of a messaging queue, which is an application program, for sharing messages between

applications. The WebSphere MQ also contains channels, queue managers (QMs) for managing multiple message queues and other related components.

The WebSphere MQ Unified Dashboard provides predefined list views for monitoring health of Queue Manager, Channels, Queues, Topics, and Subscriptions.

## Contents

### NOTE

If your Unified Dashboard is not populating with data, make sure all required data sources for the Unified Dashboard are enabled. The required probe must be deployed and must be configured so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

### WebSphere MQ Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the WebSphere MQ dashboard.

| QoS                                        | Subkey/Target |
|--------------------------------------------|---------------|
| QOS_QUEUE_MANAGER_CONNECTION_COUNT         | *             |
| QOS_QUEUE_MANAGER_CHANNEL_INITIATOR_STATUS | *             |
| QOS_QUEUE_MANAGER_UP_TIME                  | *             |
| QOS_QUEUE_MANAGER_COMMAND_SERVER_STATUS    | *             |
| QOS_CHANNEL_BYTES_RECEIVED                 | *             |
| QOS_CHANNEL_BYTES_SENT                     | *             |
| QOS_CHANNEL_MCA_STATUS                     | *             |
| QOS_CHANNEL_MESSAGE_COUNT                  | *             |
| QOS_CHANNEL_UP_TIME                        | *             |
| QOS_CHANNEL_CHANNEL_STATUS                 | *             |
| QOS_CHANNEL_IN-DOUBT_STATUS                | *             |
| QOS_QUEUE_CURRENT_DEPTH                    | *             |
| QOS_QUEUE_OPEN_INPUT_COUNT                 | *             |
| QOS_QUEUE_OPEN_OUTPUT_COUNT                | *             |
| QOS_QUEUE_UNCOMMITTED_MESSAGE_COUNT        | *             |
| QOS_QUEUE_ON_QUEUE_TIME                    | *             |
| QOS_QUEUE_OLDEST_MESSAGE_AGE               | *             |
| QOS_QUEUE_UTILIZATION                      | *             |
| QOS_QUEUE_INHIBIT_GET_STATUS               | *             |
| QOS_QUEUE_INHIBIT_PUT_STATUS               | *             |
| QOS_TOPIC_PUBLISH_COUNT                    | *             |
| QOS_TOPIC_SUBSCRIPTION_COUNT               | *             |
| QOS_TOPIC_NUMBER_OF_MESSAGES               | *             |
| QOS_TOPIC_NUMBER_OF_PUBLISHES              | *             |
| QOS_SUBSCRIPTION_NUMBER_OF_MESSAGES        | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe is known to return only one value.

For more information on configuring probes, see the documentation for each probe.

### **Queue Manager Health**

This chart displays information about all Queue Managers which are being monitored. This chart displays information on queue manager availability and performance for identifying appropriate reason.

| Column Name              | Description                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connection Count         | Current number of connections to the queue manager.                                                                                                   |
| Channel Initiator Status | Status of the channel initiator, which can be one of the following:<br>0: Not running<br>1: Initializing<br>2: Initialized and running<br>3: Stopping |
| Command Server Status    | Status of the command server, which can be one of the following:<br>0: Down<br>1: Up                                                                  |
| Up Time                  | Queue manager up time. This value is always NULL for WebSphere MQ 7.0.1.10.                                                                           |

### **Channel Health**

This chart lets you identify the factors that can affect the channel health and performance. This chart also displays the operational status of all the channels.

| Column Name             | Description                                                                                                                                                                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bytes Received          | Number of bytes received since it is last connected.                                                                                                                                                                                                                                               |
| Bytes Sent              | Number of bytes sent since it is last connected.                                                                                                                                                                                                                                                   |
| Message Count           | Number of messages sent or received.                                                                                                                                                                                                                                                               |
| Channel Up Time         | Channel up time in minutes by calculating the difference between current time and when the channel is last connected.                                                                                                                                                                              |
| Channel Status          | Current state of the channel. The channel status code depends on the coding scheme selected on the probe GUI. Refer the websphere_mq probe documentation for detailed status codes.                                                                                                                |
| MCA Status              | Status of Message Channel Agent (MCA), which can be one of following:<br>0: Stopped<br>3: Running                                                                                                                                                                                                  |
| Channel In-Doubt Status | Indicates the in doubt status of the channel. A channel is in doubt state after sending the acknowledgment request of batch messages status and before the acknowledgment is received. This column displays one of the following values:<br>0: Channel is not in doubt.<br>1: Channel is in doubt. |

## Queue Health

This chart displays values of the most common metrics for monitoring the queue health. For example, monitor the queue depth and identify if messages are not reaching to a queue or a queue is not processing the messages further.

| Column Name                    | Description                                                                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Queue Depth                    | Number of messages in the queue.                                                                                                        |
| Application Count Put Messages | Number of applications that are currently connected to the queue to put messages on the queue.                                          |
| Application Count Get Messages | Number of applications that are currently connected to the queue to get messages on the queue.                                          |
| Uncommitted Message Count      | Number of uncommitted changes (puts and gets) pending for the queue.                                                                    |
| Message Time on Queue          | Time duration for which a message is on the queue.                                                                                      |
| Oldest Message Age             | Age of the oldest message on the queue.                                                                                                 |
| Queue Utilization              | Capacity utilization of the queue which is calculated as $(\text{Current Depth}/\text{Maximum Depth}) * 100$ .                          |
| Inhibit Get Status             | Indicates if the get operations are allowed or inhibited on the queue, which can be one of the following:<br>0: Allowed<br>1: Inhibited |
| Inhibit Put Status             | Indicates if the put operations are allowed or inhibited on the queue, which can be one of the following:<br>0: Allowed<br>1: Inhibited |

### NOTE

The metric value for some targets remains blank, as the metric is not applicable for the target. For example, if Remote Queue is the target then only Inhibit Put Status column has value, rest all columns remain blank. Refer the probe configuration GUI and view the monitors list for each queue type.

## Topic Health

This chart helps analyzing topic health by displaying metric values of messages and subscriptions, which are related to the topic.

| Column Name         | Description                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------|
| Publish Count       | Number of applications, which are currently publishing messages to the topic.                 |
| Subscription Count  | Number of topic subscribers including durable subscribers, which are currently not connected. |
| Number of Messages  | Number of messages put to the specified subscriber destination.                               |
| Number of Publishes | Number of publishes made by this publisher.                                                   |

## Subscription Health

This chart monitors the subscription health by displaying Number of Messages metric value for all monitored subscriptions.

| Column Name        | Description                                           |
|--------------------|-------------------------------------------------------|
| Number of Messages | Number of messages put to the subscriber destination. |

## Websphere Unified Dashboard

The Websphere Unified Dashboard provides predefined list view for monitoring System Information.

### Contents

#### Websphere Required Data Sources

This table lists the probes, QoS metrics, and subkeys or targets that must be activated to populate data in the Websphere dashboard.

| QoS                        | Subkey/Target |
|----------------------------|---------------|
| QOS_WEBSPHERE_CPU_USAGE    | *             |
| QOS_WEBSPHERE_MEMORY_USAGE | *             |
| QOS_WEBSPHERE_THREADCOUNT  | *             |

An asterisk (\*) means that the value for the first entry for the QoS is used. The asterisk should only be used when the QoS metric for a probe returns only one value.

#### System Information

This chart displays information about the System Information:

| Column Name | Description                                 |
|-------------|---------------------------------------------|
| CPU Usage   | Percentage of CPU used by websphere server. |
| Memory      | Percentage of used memory and free memory.  |
| ThreadCount | Average number of threads in the pool.      |

## XenServer Unified Dashboard

The XenServer Unified Dashboard provides predefined list views for monitoring the XenServer virtualization enabled systems (VM). The views include information about storage, CPU, and memory metrics.

### Contents

#### NOTE

If your Unified Dashboard is not populating with data, verify that all required data sources are enabled. You must deploy and configure the required probe so that required QoS metrics and subkeys or targets are activated. For more information, see the help topic on required data sources for the Unified Dashboard.

#### Required Data Sources

The table contains the probes and QoS metrics that are required for the preconfigured XenServer dashboard.

**NOTE**

The OC Dashboards template includes some of the required QoS measurements, but not all. Verify that you enabled in the probe all the measurements that are listed here.

| Chart                      | QoS Required                                                 |
|----------------------------|--------------------------------------------------------------|
| Host CPU Metrics           | QOS_CPU_SPEED<br>QOS_XEN_CPU_UTIL                            |
| VM CPU Metrics             | QOS_XEN_CPU_UTIL                                             |
| Disk Metrics               | QOS_XEN_DISK_READ<br>QOS_XEN_DISK_WRITE<br>QOS_DISK_SPACE_GB |
| Disk Usage Percent Metrics | QOS_XEN_DISK_USAGE_PERC                                      |
| Host Memory Metrics        | QOS_XEN_MEMORY_PERC_USAGE                                    |
| Network Metrics            | QOS_XEN_NETWORK_TX_KBPS<br>QOS_XEN_NETWORK_RX_KBPS           |
| VM Memory Metrics          | QOS_MEM_MB                                                   |

**Host CPU Metrics**

This chart displays information about the Host CPU metrics for the managed system.

| Column                       | Description                              |
|------------------------------|------------------------------------------|
| Host CPU Speed               | The CPU speed of the host.               |
| Host CPU Average Utilization | The average CPU utilization of the host. |

**VM CPU Metrics**

This chart displays information about the VM CPU metrics for the managed system.

| Column                     | Description                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------|
| VM CPU Average Utilization | The average CPU utilization for the VM<br>Green = 0.00 - 60.99<br>Orange = 61.00 - 80.101<br>Red = 81.00 - 102.0 |

**Disk Metrics**

This chart displays information about the host or target disk metrics for the managed system.

| Column                    | Description                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------|
| Read throughput           | Read throughput for the selected device during the selected interval that is measured in kilobytes  |
| Write throughput          | Write throughput for the selected device during the selected interval that is measured in kilobytes |
| Virtual Block Device Size | The size of the virtual disk that is measured in gigabytes                                          |

**Disk Usage Percent Metrics**

This chart displays information about the disk usage percent metrics for the managed system.

| Column             | Description                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Disk Usage Percent | The percentage of available disk space that is used<br>Green = 0.00 - 60.99<br>Orange = 61.00 - 80.101<br>Red = 81.00 - 102.0 |

**Host Memory Metrics**

This chart displays information about the host memory metrics for the managed system.

| Column              | Description                                                                                                     |
|---------------------|-----------------------------------------------------------------------------------------------------------------|
| Free Memory         | The amount of memory that is free                                                                               |
| Total Memory        | The total amount of memory                                                                                      |
| Percent Used Memory | The percentage of memory that is used<br>Green = 0.00 - 60.99<br>Orange = 61.00 - 80.101<br>Red = 81.00 - 102.0 |

**Host Network Metrics**

This chart displays information about the host or target network metrics for the managed system.

| Column     | Description                                     |
|------------|-------------------------------------------------|
| Network Tx | Transmitted kilobytes for the network interface |
| Network Rx | Received kilobytes for the network interface    |

**VM Memory Metrics**

This chart displays information about the VM memory metrics for the managed system.

| Column        | Description                                                                   |
|---------------|-------------------------------------------------------------------------------|
| Free Memory   | The memory used as reported by the guest agent, which is measured in kilobits |
| Total Memory  | The memory that is currently allocated to the VM, measured in bytes           |
| Used Memory   | The used memory in megabits per second                                        |
| Actual Memory | The memory that is actually available to be assigned to VMs from the host     |
| Target Memory | Dynamically set memory target for memory available to this VM                 |



---

## Integrating Other Products

---

You can integrate CA UIM with other products for customized monitoring solutions.

### **Log Analytics**

Log Analytics streamlines the log analysis process and helps you troubleshoot faster and more effectively by:

- Collecting and aggregating logs from multiple sources (individual servers, devices, and applications). You can gain insights from data using analytics dashboards.
- Providing out-of-the-box dashboards (blueprints) based on the collected data for supported log types and patterns.
- Providing full text search on all the stored log files.
- Performing near real-time and historical search on all the log data from one centralized location.
- Performing a periodic query of the log data and sending notifications (alarm, email, and snmp) when matches are found. You can also save and schedule a log query or pattern to receive notifications when a match is found.

### **CA Application Delivery Analysis**

CA Application Delivery Analysis provides a consistent and common set of service quality metrics that can help prove the performance of applications delivered over the network, validate the impact of changes and solve problems faster. It can provide your organization with an in-depth understanding of application response time and how the network impacts the end-use, helping you ensure an optimal experience and improve application performance management.

### **CA Cloud Monitor**

The CA Cloud Monitor allows you to access the online service that monitors your sites, servers, and applications 24 hours a day, 7 days a week.

### **CA Cloud Service Management**

CA Cloud Service Management is a full-featured service management solution. CA Cloud Service Management provides action-based workflows in accordance with ITIL standards that allow you to coordinate incident response and proactive IT management.

### **CA Network Flow Analysis**

CA Network Flow Analysis is a network traffic monitoring solution that can help you optimize your network infrastructure for better application performance. With enhanced visibility into your network's applications, hosts, conversations and QoS information, you can proactively manage your network to reduce outages, solve problems faster and ensure efficient and cost-effective operations.

### **Flow Analysis**

Flow Analysis is designed to track all network traffic and provide an enterprise-wide view of your flow data. This visibility can help your organization make network performance decisions.

### **CA SiteMinder**

CA SiteMinder can provide your organization enterprise-class secure single sign-on (SSO) and flexible identity access management so that your organization can authenticate users and control access to Web applications and portals.

## CA Spectrum

CA Spectrum is a services and infrastructure management system that monitors the state of managed elements. Spectrum collects and stores status information from these elements, such as fault and performance data. CA Spectrum continually analyzes this information to track conditions within the computing infrastructure. If an abnormal condition is detected, the product isolates it, alerts you to it and presents the possible causes of the condition and solutions to correct it.

## DX Operational Intelligence

DX Operational Intelligence enables IT operations teams to make smarter, faster decisions for enhancing user experience and improving IT service quality and capacity through cross-domain contextual intelligence. Built on an open, powerful engine, DX Operational Intelligence provides users with comprehensive insights by ingesting and analyzing a diverse data set including metric, topology, text, and log data. The machine learning–driven analytics, along with out-of-the-box visualization and correlation, helps drive a superior user experience and deliver significant operational efficiencies.

The DX Operational Intelligence Gateway (oi\_connector) probe integrates CA Unified Infrastructure Management (UIM) and DX Operational Intelligence (DOI). You can configure the oi\_connector probe to send data to DX Operational Intelligence. The CA Digital Operational Intelligence Gateway (oi\_connector) achieves the following:

- Store UIM alarms, inventory, metrics (QoS), and UIM groups in DX Operational Intelligence
- Build Dashboards with the alarms, QoS and inventory information
- (Optional) Store Spectrum alarms and inventory in DX Operational Intelligence

Refer [oi\\_connector \(DX Operational Intelligence Gateway\) Release Notes](#) for more information.

## UIM 20.3.0 Integrations Support

This section highlights the Integration support for the other CA products.

| Integration     | Version                                                                     | UIM Probe Version                        |
|-----------------|-----------------------------------------------------------------------------|------------------------------------------|
| Spectrum        | 10.4.2.x                                                                    | Spectrumgtw 8.68                         |
| APM             | 20.2                                                                        | apm_bridge : 1.03hf6, oi_connector v1.38 |
| DOI             | 20.2                                                                        | apm_bridge : 1.03hf6, oi_connector v1.38 |
| NFA             | 10.0.4                                                                      | nfa_inventory 1.42                       |
| ADA             | 11.1.2 (0-flash)                                                            | ada_inventory 1.41                       |
| CA Service Desk | 17.2                                                                        | Sdgtw 2.23                               |
| SOI             | 4.2 (SO14226-flash patch)<br>Catalyst Container 3.4.3 + UIM Connector 3.9.2 |                                          |
| Unified CABI    | Jasper Version : 7.1.1                                                      | cabi_external 4.20                       |
| CapMan          | 2.9.4                                                                       | capman_da 2.95                           |

## Integrate CA Application Delivery Analysis

Using the **ada\_inventory** probe, you can configure CA UIM to display certain CA Application Delivery Analysis (ADA) metrics.

The following ADA metrics are available in the OC:

- Performance by Network – Packet Loss
- Hosted Applications – Data Transfer Time
- Total Bytes vs Retransmitted Bytes
- Server Connection Time
- Downstream Dependencies
- Server Response Time
- Incidents
- Total Sessions vs Refused Sessions
- Investigations
- Total Transaction Time

For more information, see the following topics:

- CA Unified Infrastructure Management [ADA](#) Probe on the Probes Documentation Space - Information on how to configure the ada\_inventory probe.
- [ADA Documentation Space](#) - Information about CA Application Delivery Analysis

## Integrate CA Automic

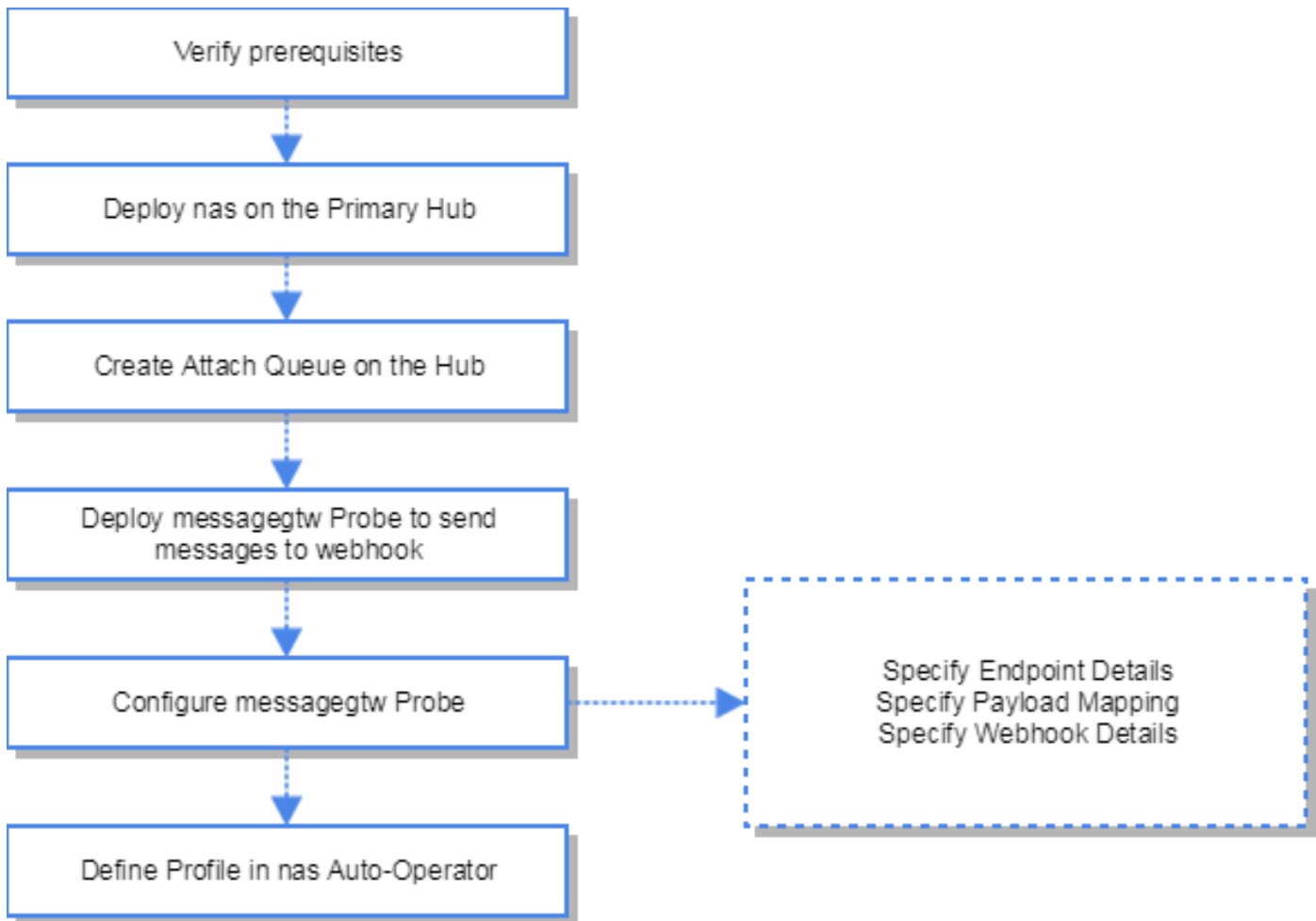
CA Digital Experience Insights / UIM combined with Automic Service Orchestration offers predictive analytics to help solve complex IT problems like performance, capacity, configuration issues to be detected proactively (before they impact users) and remediated automatically.

The CA UIM-CA Automic integration is achieved using the messagegtw probe which publishes UIM alarms to an Automic endpoint that is configured in the messagegtw probe, using webhooks.

When CA UIM raises an alarm for disk full warning, the message is passed on to Automic where a specific job is run to clear the cache for the disk directory. You can also define/ configure other parameters from CA UIM to be sent as part of the message/ alarm that is sent to Automic.

The CA Unified Infrastructure Management messagegtw (Message Gateway) probe is used to publish CA UIM alarms to an external application using webhooks. A webhook is a simple notification message using an HTTP POST to an external application. In CA UIM, a webhook is triggered based on the occurrence of an alarm.

### Basic workflow to configure messagegtw for an endpoint

**Figure 27: Configure messagegtw****Contents:****Overview**

When an event occurs in nas, it publishes to a queue on the hub. The messagegtw probe listens to the messages and alarms from nas through a queue that you create on the hub. You also need to configure the same queue on the messagegtw probe. The messagegtw probe makes an HTTP request to the URL configured for the webhook and posts the message to the configured webhook.

You can deploy the probe on a primary hub, secondary hub, or a robot. You can choose to configure multiple webhooks to receive the message and alarms from messagegtw.

The nas auto operator GUI is now enhanced to support webhooks. The new action type “webhooks” will work for running instances of the messagegtw and invokes a callback on that probe to see what webhooks or outbound rest integrations you have configured to allow you to create an Auto-Operator to point to a specific webhook.

The probe supports multiple instances of the messagegtw such that you can configure multiple probes across hubs and robots based on your environment. You can then create Auto-Operator profiles from nas for webhooks, filter the alarms, and publish to the specific instance of the messagegtw you want to publish to, by specifying the directory path of the robot or hub where the messagegtw probe is deployed.

You need to create an Auto-Operator profile in nas, using which you can filter the alarm and messages to be published through messagegtw. For more information, see the 'webhook' action type in nas auto-operator profiles.

The messagegtw probe GUI allows you to configure the webhook, and map nas and messagegtw fields. Messages that you add are sent to the webhook. In the messagegtw GUI, listeners are the webhooks listening to messagegtw probe. You can create multiple profiles under listeners. All the listener profiles that you create listen to messagegtw probe.

### **Prerequisites**

- Deploy nas on the Primary Hub.  
You need to deploy the nas auto-operator for webhook on the primary hub, to configure webhook auto operator profile. This is required to be done on the primary hub, because data\_engine probe is on the primary hub.

### **Create a Hub Attach Queue**

CA UIM components use queues to pass messages. Create an attach queue in the hub to publish messages from messagegtw to the webhooks you configure.

#### **Follow these steps:**

1. On the robot, open the hub probe configuration and go to **Queue List**.
2. In the Queue List Configuration table, select **New**.
3. Specify the following required information:
  - **Queue Name** - Enter a unique and descriptive name. For usability, use a name similar or identical to the subject. You specify the queue name when configuring the webhook in the messagegtw probe.

#### **NOTE**

Ensure that the queue name you specify while creating the attach queue, is the same as the queue name you specify in the **messagegtw configuration, webhook, queue name** field.

- **Active** - Select *active* for the queue to be available immediately.
- **Type** - Select *attach*.
- **Hub Address** (get queues) - Address of the hub that has the corresponding attach queue.
- **Subject** (attach queues) - Enter the subject probe\_messagegtw.

#### **NOTE**

A dialog prompting you to restart the probe to enable the changes is displayed. Select Yes to restart the hub probe.

### **Configure messagegtw Probe**

After you install the probe, configure the probe setup using the messagegtw probe Admin Console.

#### **Follow these steps:**

1. Deploy the **messagegtw** probe on a Primary or Secondary hub, or a robot.
2. Select the **messagegtw** probe from the Probes tab and select **Configure**.  
The default probe information is displayed.
3. (Optional) In the Probe Configuration section, specify Log level, and **Save**. The default log level is 1.

#### **NOTE**

: Log as little as possible during normal operation to minimize disk consumption, and increase the amount of detail when debugging.

4. Select **Webhook, Options, Clone**. We recommend you to create a custom webhook configuration based on the default or sample configuration.
5. Select **Submit** and **Close**.

6. In the **EndPoint Details** section, select **New** to configure a new endpoint and specify the following fields: Sample values are displayed in the profile you have cloned.
  - **URL:** Specify the endpoint url of the webhook where messagegtw will post the messages. Obtain this URL from the external application API Token.
  - **AUTH\_METHOD:** Specify the authentication method. You may select Basic or None. messagegtw supports only Basic Authentication. If you want to post your Webhooks to a service requiring authentication, use Basic HTTP authentication by modifying your URL from https://my.example.com to https://username:password@my.example.com.
  - **USER\_NAME:** Specify a username for the endpoint.
  - **PASSWORD:** Specify a password for the endpoint.
  - (Optional) **respkey = \$.run\_id.** Adding this key allows you to retrieve the Job/Ticket ID and store it in the alarm.
7. In the **Payload Mapping** section, you can specify your own payload to add your own custom fields to the payload request. For a sample payload, view [Sample Payload](#). For a complete list of alarm and computer system variables, view Alarm and System Variables.

#### NOTE

The supported payload type is application/json

8. Select **New** to configure the payload mapping to specify the content you want to post to the webhook or the endpoint URL. Specify the Mapping\_key and Mapping\_value, as in the following sample:
  - **tags** – For example, "#alarm", "#cauim", "#\${message.prid}"
  - **external user name** – For example, "CA UIM"
  - **content** – For example, "[\${message.udata.severity}] \${cs.name}(\${cs.ip}).\${ci.description}.\${ci.name}: \${message.udata.message}"
9. In the **Webhook** section, default values are displayed. You can customize the following mandatory fields:
  - **webhook name** – Specify the webhook name.
  - **queue name** – Specify the name of the queue you have created in the hub which messagegtw subscribes to.
  - **attach to queue**– Specify if True or False. Default is True. If True, the queue collects messages for forwarding to a get queue.
  - **send exclusive** – If True, this option publishes the messages to the first configured endpoint URL. When set to False, the messages are sent to all the webhook endpoints at once. Default value is True.
  - **alert on failure** – Generates an alert if messagegtw is unable to publish to the webhook configured. Default value is True.
  - **bulk size** – Specifies the max queue size that is processed by messagegtw. Default value is 10.
  - **(Optional) hub\_address** – If messagegtw is deployed in the secondary hub, specify the primary hub address. For example, *hub\_add = /domain/primary\_hub/robot/hub*
10. Delete the sample webhook configuration before restarting the probe. Navigate to **Webhook, Options**, and select **Delete**.
11. After you have made the configuration changes, restart the probe.  
The messagegtw probe now publishes messages from nas to the webhooks you have configured.

#### Sample Payload

```
<payload>
 content = "[${message.udata.severity}] ${cs.name}(${cs.ip}).${ci.description}.
 ${ci.name}: ${message.udata.message}"
 external_user_name = "CA_UIM"
 tags = ["#alarm", "#cauim", "#${message.prid}"]
</payload>
```

## Alarm and System Variables

You can specify your own payload to add your own custom fields to the payload request. Specify your own custom payload, using the following alarm and computer system variables.

| Variable   | Type    | Meaning                                                                                            |
|------------|---------|----------------------------------------------------------------------------------------------------|
| rowid      | Integer | Indicates the row ID. Example: 1                                                                   |
| event_type | Integer | Indicates the event type. Example: 16                                                              |
| nimid      | String  | Indicates the alarm message-id. For example, YP39028984-19824                                      |
| nimts      | Integer | Indicates the message timestamp, when it was originally sent. For example, 1534444449              |
| arrival    | Integer | Indicates the timestamp when the Nimsoft Alarm Server received the alarm. For example, 1534444450  |
| severity   | String  | Indicates the name of the severity level. For example, critical                                    |
| level      | Integer | Indicates the severity level of the alarm. For example, 5                                          |
| prevlevel  | Integer | Indicates the previous severity level of the alarm. For example, 5                                 |
| subsys     | String  | Indicates the message text. Indicates the alarm subsystem. For example, Controller                 |
| message    | String  | Indicates the message text. For example, Test alarm from controller on computer-8462               |
| source     | String  | Indicates the IP address of the system that sent the alarm. For example, 10.131.144.22             |
| hostname   | String  | Indicates the hostname of the system that sent the alarm. For example, computer-8462               |
| sid        | String  | Indicates the subsystem ID in the Nimsoft Alarm Server. For example, 1.2.2.1                       |
| domain     | String  | Indicates the name of the domain the Robot is in. For example, computer-8462_domain                |
| hub        | String  | Indicates the Hub the robot belongs to. For example, computer-8462_hub                             |
| nas        | String  | Indicates the name of the Hub, nas belongs to. For example, computer-8462_hub                      |
| robot      | String  | Indicates the name of the Robot that sent the alarm. For example, computer-8462                    |
| origin     | String  | Indicates the system name of the hub in which the robot is present. For example, computer-8462_hub |
| prid       | String  | Indicates the probe ID. For example, controller                                                    |
| supp_key   | String  | Indicates the suppression key (often contains the checkpoint). For example, test_alarm             |

|                    |         |                                                                                                         |
|--------------------|---------|---------------------------------------------------------------------------------------------------------|
| suppcount          | Integer | Indicates the number of times this alarm has been suppressed. For example, 43                           |
| supptime           | Integer | Indicates the timestamp of the last suppression of this message. For example, 1536050909.               |
| tz_offset          | String  | Indicates the sending system time zone offset in seconds compared to UTC. For example, -19800           |
| visible            | Boolean | Indicates whether the alarm has been made invisible to account users.                                   |
| dev_id             | Text    | The ID of the IP addressable device that is associated with the entity for which the alarm was created. |
| met_id             | Text    | The ID of the metric, if any, for which the alarm was created.                                          |
| profile            | Text    | Indicates the nas Auto-Operator profile name.                                                           |
| aots               | Integer | Indicates the Auto-Operator execution timestamp.                                                        |
| webhook            | Text    | Indicate the name of the webhook.                                                                       |
| ci.caption         | Text    | Indicates the caption of the configurable item.                                                         |
| ci.name            | Text    | Indicates the name of the configurable item.                                                            |
| ci.type            | Text    | Indicates the type of the configurable item.                                                            |
| ci.description     | Text    | Indicates the description of the configurable item.                                                     |
| metric.description | Text    | Indicates the description of the metric.                                                                |
| metric.unit        | Text    | Indicates the unit of the metric.                                                                       |
| device.id          | Text    | Indicates the unique id of the device.                                                                  |
| device.ip          | Integer | Indicates IP address of the device.                                                                     |
| device.name        | Text    | Indicates the name of the device.                                                                       |
| device.probe       | Text    | Indicates the name of the probe on the device.                                                          |
| cs.id              | Text    | Indicates the unique ID of the Computer system.                                                         |
| cs.key             | Text    | Indicates the key for the computer system.                                                              |
| cs.dedicated       | Text    | Indicates whether the Computer system is Virtual or Physical.                                           |
| cs.state           | Text    | Indicates the state of the Computer system. Active = 1; Inactive = 0                                    |
| cs.name            | Text    | Indicates the name of the Computer system.                                                              |
| cs.domain          | Text    | Indicates the domain in which the Computer system resides.                                              |
| cs.origin          | Text    | Indicates the origin / tenant details of the computer system.                                           |



|                   |      |                                                                                                                        |
|-------------------|------|------------------------------------------------------------------------------------------------------------------------|
| cs.ip             | Text | Indicates the IP Address of the Computer system.                                                                       |
| cs.os_type        | Text | Indicates the type of OS of the Computer system. For example, UNIX / Windows                                           |
| cs.os_name        | Text | Indicates the name of the Operating system of the Computer System. For example, Linux, Cent / Ubuntu for UNIX, Windows |
| cs.os_version     | Text | Indicates the version of the Operating system of the computer system.                                                  |
| cs.os_description | Text | Indicates the description of the Operating system of the computer system.                                              |
| cs.maintenance    | Text | Indicates if the computer system is in maintenance.                                                                    |

**NOTE**

For Oracles databases, parameters with ci, and cs, should be capitalized. For example, ci.name should be CI.NAME in Oracle databases.

**Define Profile in nas Auto-Operator**

On the, nas IM config, *Auto-Operator* tab, it is possible to configure the auto-operator with profiles containing selection criteria for various fields, such as severity level(s), subsystem Id, message string etc. When an alarm event passes the selection criteria as well as the action time, an action is triggered.

The Auto-Operator aids the administrator in managing alarms by matching rules (alarm severity, alarm message text, subsystem ID) to assign an alarm to a person or group, and to send messages (email or text) when a specific rule is met. Create and define a profile in Auto-Operator for webhook. Specify the instance of messagegtw to which the queue is posted.

For more information see [nas Auto-Operator, Creating or Editing a Profile, Action Types, webhook](#).

**Follow these steps:**

1. On the robot, open IM nas configuration, and go to Auto-Operator.
2. Right-click **New** to create a profile.

### 3. Specify the following required fields:

- – **Action type** - Select *webhook* (Specifies that the auto-operator sends a message to the configured webhooks).
- **Path to Messagegtw Probe** - Specify the path of the hub or robot where the messagegtw probe is deployed and configured. The nas auto-operator profile publishes to the instance of the messagegtw probe that you specify here.
- **Webhook Name** - Select the webhook from the drop-down. The webhook is populated based on the webhooks that are configured in the selected instance of the messagegtw probe.
- **Subject** - Specifies the message queue name. This field is auto populated based on the webhook you select.
- **More Properties** - Specify any additional property or metadata that you want to send to the messagegtw.

### Use case for CA UIM-Automic Integration

Use Case: Self Remediation through the UIM-Automic integration: Disk clean-up & thereby preventing a DB from crashing.

An alarm is configured, in CA UIM to indicate free disk space on the server has dropped below pre-configured threshold. Because of low disk space, applications and databases may stop functioning properly and even the OS may crash which

will lead to service interruption. In response to such alarms, a cleanup of the disk is to be performed proactively before it affects the business by Automatic.

#### Prerequisites:

- The host machine is monitored by UIM and has Automatic deployed for WA.
- Create a new job object type in Automatic to clear the cache for specified disk directory on the target system.

**A job is used to define processing steps in a target system. It can be used independently, in a group, or within a workflow. The script is processed in a specific way in the object type "Job". Depending on the JCL (Job Control Language) and the script elements, an executable job is generated for the respective target system and transmitted via file transfer. The AE Script (if existing) and the JCL lines are processed and subsequently, the JCL is sent to the target system. AE Script is never sent to the target system.**

When CA UIM raises an alarm for disk full warning, the message is passed on to Automatic where a specific job is run to clear the cache for the disk directory. You can also define/ configure other parameters from CA UIM to be sent as part of the message payload that is sent to Automatic. When a disk full alarm is generated on CA UIM, messagegw sends a POST request mapping the UIM variables that generated the alarm, to field names in Automatic. An Automatic Job ID is returned as response. CA UIM attaches this JOB ID to the alarm, using the OC Edit URL Actions. Execute the Launch URL action, from OC to trigger the JOB ID in Automatic. Automatic executes the job to clear the cache for the specified disk on the target system.

#### Example: URL and Payload to send Message to Automatic

```
http://hostname-a15090:8088/ae/api/v1/100/executions
```

The following json format is accepted by Automatic:

```
{
 "object_name": "JOBP.DISK_SPACE",
 "inputs": {
 "DISK#": "C",
 "DNSNAME#": "domain.name.xx",
 "IP#": "10.0.0.1"
 }
}
```

You would need to map the fields names in the Automatic job object to the CA UIM variables:

| CA Automatic                                                                                  | CA UIM                                                           |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| <b>DISK</b><br>Specify the disk directory.                                                    | <b>ci.name</b><br>Indicates the name of the configurable item.   |
| <b>DNSNAME</b><br>Specify the Domain Name Server Name.                                        | <b>cs.name</b><br>Indicates the name of the Computer system.     |
| <b>IP</b><br>Specify the IP address of the target system whose disk space you are monitoring. | <b>cs.ip</b><br>Indicates the IP Address of the Computer system. |

Once you have mapped the filed/ variables, use the following sample payload

```
<payload>
object_name = "JOBP.DISK_SPACE"
inputs = {"DISK#" : "${ci.name}", "DNSNAME#" : "${cs.name}", "IP#" : "${cs.ip}"}
</payload>
```

Expected Response are, **Custom 1 = url\_field** and **Custom 2= run\_id\_field**. These are appended to the messagegw configuration on a successful POST request.

To get the status of the job in Automic, if the run\_id returned, follow these steps:

The screenshot displays the CA Unified Infrastructure Management interface. The main window shows a list of alarms, with one alarm selected. The 'Edit URL Actions' dialog box is open, showing the configuration for a new URL action named 'automic'. The URL field is set to a placeholder for custom fields. The 'Launch URL Action' button is visible in the alarm details view. The 'Actions' menu is open, showing the 'Edit URL Actions...' option.

1. In OC, select the monitored device, **Actions, Edit URL Actions**.
2. By default, Custom\_1 and Custom\_2 fields return the the url\_field and run\_id\_field. Specify a **Name** for the new URL action and click **Save**.
3. Click the **Launch URL Action** button (for the selected device) to check the status of the job in Automic.

Sample response of the status for Job ID using Launch URL Action > Name specified during Edit URL Actions.

```
{
 "name" : "JOBP.DISK_SPACE",
 "type" : "JOBP",
 "run_id" : 1934790,
 "status" : 1900,
 "status_text" : "ENDED_OK - ended normally",
 "runtime" : 0,
 "activation_time" : "2018-09-24T22:42:59Z",
 "start_time" : "2018-09-24T22:43:00Z",
 "end_time" : "2018-09-24T22:43:00Z",
 "parent" : 0,
 "user" : "AUTOMIC/AUTOMIC",
 "estimated_runtime" : 1,
 "alias" : "JOBP.DISK_SPACE"
}
```

}

## Integrate CA Network Flow Analysis

Using the `nfa_inventory` probe, you can configure CA UIM to display certain CA Network Flow Analysis information.

The following views are available in the details of the **Device Interface View**:

- Stacked Protocol Trend - In
- Stacked Protocol Trend - Out
- Top Hosts
- Top Conversations

The following views are available in the OC:

- Stacked ToS Trend In
- Stacked ToS Trend Out
- Top Hosts per ToS
- Top Conversations per ToS

For more information, see the following topics:

- [nfa\\_inventory](#) probe on the Probes Documentation Space - Information about how to configure the `nfa_inventory` probe.
- [NFA](#) - Documentation on CA Network Flow Analysis.
- [View Interface Data](#) - Information about using the Advanced tab and Device Interface View in OC.

## Integrate CA Service Desk

When integrated, you can create incident tickets in CA Service Desk that are based on CA UIM alarms. Generating these incidents helps your service desk users take immediate corrective actions when CA UIM alarms are generated.

To integrate CA Service Desk and CA UIM, deploy and configure the CA ServiceDesk Gateway (`casdgtw`) probe. The `casdgtw` probe performs the following actions:

- Tests the network access to the CA Service Desk (CASD) application.
- Tests the login sessions on the CASD application.
- Creates incidents in the CASD application that are based on UIM alarms.
- Updates incident activity logs in the CASD application when the associated UIM alarm updates.
- Closes the incident when the corresponding alarm is acknowledged.
- Acknowledges the alarm when the corresponding incident is closed in the CASD application.

For more information, refer to the [casdgtw](#) probe documentation on the Probes Documentation Space.

## Integrate CA Service Operations Insight

You can integrate your UIM data into CA Service Operations Insight using the CA UIM Catalyst connector.

The CA UIM Connector performs the following tasks:

- Collects data such as configuration items, alerts, and status from CA UIM.
- Processes and transforms the data into the OC format using a connector policy.
- Dispatches the information to CA SOI.

For more information, see the [CA Service Operations Insight documentation](#).

## Compatibility Information

The following table provides the compatibility information for CA UIM, CA SOI, Container, and the connector:

|                   |                                                                            |
|-------------------|----------------------------------------------------------------------------|
| Connector         | UIM 3.9.2                                                                  |
| Release Date      | 13 Sep 2019                                                                |
| CA UIM Version    | CA Unified Infrastructure Management (UIM) 9.0.2, 9.2.0, 20.1.0 and 20.3.0 |
| Container         | Catalyst Container                                                         |
| Container Version | 3.4.3                                                                      |
| CA SOI Version    | 4.2 (Patch SO09444)                                                        |

## Integrate CA UIM, CA Spectrum, and CA SOI

The integration between CA UIM, CA Spectrum, and CA SOI is an extension of the CA UIM - CA Spectrum integration. After you integrate CA UIM and CA Spectrum, you can use the information that is provided by this integration in CA SOI. For more information, see the topic [Integrate CA UIM, CA Spectrum, and CA SOI](#).

## Integrate CA SiteMinder

This scenario describes how a security administrator configures the Operator Console (OC) to be protected by SiteMinder. Using SiteMinder with OC provides greater security for your organization. In addition, you can implement single sign-on access to OC and other web applications.

### Contents

### Prerequisites

#### WARNING

Do not attempt to perform the procedures in this scenario unless you are proficient with CA UIM Monitor, CA SiteMinder, and directory administration.

Ensure that the following prerequisites have been met before using the instructions in this scenario:

- CA UIM Monitor (UIM and OC) 7.5 or higher are installed and configured.
- CA SiteMinder r12.51 or higher is installed with an operational Secure Proxy Server.
- An LDAP directory exists for SiteMinder authentication and for linking to CA UIM Monitor. The following directory services are supported:
  - Novell® eDirectory (TM) 8.8 SP1 (20114.57) and a Novell® KDC (Key Distribution Center) server
  - SUN Java Directory Server v5.2
  - Windows 2008 and Windows 2012 Active Directory.

### Verify LDAP Mapping

The following table identifies the user and group attributes that must map between your directory and the UIM hub and OC. The attributes designated with an asterisk (\*) are the required mappings for OC. It is recommended that you determine these attributes in your directory service before continuing.

Refer to this table as needed as you perform the steps in the following sections.

| Description      | UIM Hub Mapping | OC Mapping                      | LDAP Example             |
|------------------|-----------------|---------------------------------|--------------------------|
| Group identifier | filter_group    | ldap.import.group.search.filter | objectClass=groupOfNames |

|                   |                            |                                |                           |
|-------------------|----------------------------|--------------------------------|---------------------------|
| Group name        | attr_grp_name              | groupName                      | cn                        |
| Group member      | attr_grp_member_name       | user                           | member                    |
| Group description | attr_grp_description       | description                    | description               |
| User identifier   | ---                        | ldap.import.user.search.filter | objectClass=inetOrgPerson |
| *Username         | ---                        | screenName                     | cn                        |
| *User Password    | ---                        | password                       | userPassword              |
| *User firstname   | attr_usr_firstname         | firstName                      | givenName                 |
| *User lastname    | attr_usr_lastname          | lastName                       | sn                        |
| *User email       | attr_usr_mail, filter_user | emailAddress                   | mail                      |

### **Configure LDAP on the Hub Probe**

Configure the hub probe to forward login requests to your LDAP server, and to access the container with user groups.

#### **Follow these steps:**

1. Log into Infrastructure Manager and locate the hub probe.
2. Press the <Ctrl> key as you right-click the hub probe, and then select Raw Configure.
3. Expand the ldap section, and expand the templates section.
4. Select the appropriate directory service, and edit the value of key filter\_user to (&<loginAttribute>=\$loginname)).
5. Depending on the directory service you are using, you may need to update the values of other keys to match your directory. Attributes that may be of particular importance are as follows:
  - filter\_group
  - filter\_user
  - attr\_grp\_name
  - attr\_grp\_member\_name
  - attr\_grp\_description
  - attr\_usr\_firstname
  - attr\_usr\_lastname
  - attr\_usr\_mail
6. Click OK to commit your changes.  
The hub probe restarts.
7. In Infrastructure Manager, right-click on the hub probe and select Configure.
8. In the lower right of the General tab, select Settings.
9. In the LDAP tab, do the following:
  - a. Select Direct LDAP.
  - b. Select LDAP Authentication.
  - c. In the Server Name field, enter the <IP\_address:port> of LDAP server.
  - d. Select the appropriate directory service from the Server Type drop-down menu.
  - e. Select LDAP > UIM from the Authentication Sequence drop-down menu.
  - f. In the User field, enter the distinguished name (DN) of a directory user with administrative privileges.
  - g. Provide a distinguished name (DN) in the Group Container (DN) and User Container (DN) fields as appropriate.

### **Link ACLs to LDAP Groups**

Use the following steps to link ACLs to LDAP groups.

#### **Follow these steps:**

1. In Infrastructure Manager, select Security >Manage Access Control List.

2. Make a selection from the Access Control List, and click the Set LDAP Group button.
3. Select an LDAP group from list.
4. Select or de-select permissions in the list if desired.

### **Modify the Portal Configuration to Enable SiteMinder**

Use the following steps to edit the portal-ext.properties file to map your directory to OC.

#### **NOTE**

The steps in this section use the directory attribute *mail* as the <loginAttribute>. If <loginAttribute> is not *mail*, certain lines must be edited differently as indicated. In addition, line numbers in the portal-ext.properties file are provided, but may vary slightly from the line numbers in your portal-ext.properties file.

#### **Follow these steps:**

1. In Infrastructure Manager, deactivate the wasp probe.
2. On the OC system, open the following file for editing:  
<OC\_installation>\probes\service\wasp\webapps\ROOT\WEB-INF\classes\portal-ext.properties
3. Modify line 12 as follows:

```
company.security.auth.type=emailAddress
```

#### **NOTE**

: If <loginAttribute> is not *mail*, modify line 12 as follows:

```
company.security.auth.type=screenName
```

4. Comment out lines 16 and 17 as follows:  
#auth.pipeline.pre=com.firehunter.ump.auth.NmsAuth  
#auth.pipeline.enable.liferay.check=false
5. Uncomment lines 188 through 191 as follows:  
ldap.base.provider.url.0=ldap://<server:port>  
ldap.base.dn.0=ou=example,o=com  
ldap.security.principal.0=<DN of directory user>  
ldap.security.credentials.0=<password>
6. Uncomment lines 195 and 196 as follows:  
ldap.auth.search.filter.0=(mail=@email\_address@)  
ldap.import.user.search.filter.0=(objectClass=inetOrgPerson)

#### **NOTE**

: If <loginAttribute> is not *mail*, modify line 195 as follows:

```
ldap.auth.search.filter.0=(<loginAttribute>=@screen_name@)
```

7. Uncomment line 199 as follows:  
ldap.import.method=user
8. Uncomment lines 201 through 203, and modify the mapping as appropriate for your directory:  
ldap.user.mappings.0=screenName=cn\npassword=userPassword\nemailAddress=mail\nfirstName=givenName\nlastName=sn\ngroup=ou  
ldap.import.group.search.filter.0=(objectClass=groupOfNames)  
ldap.group.mappings.0=groupName=cn\ndescription=description\nuser=member

#### **NOTE**

: If <loginAttribute> is not *mail*, modify the screenName mapping in line 201 as follows:



```
screenName=<loginAttribute>
```

9. Save the portal-ext.properties file, and reactivate the wasp probe.

### **Verify OC Resources are Protected in SiteMinder Policy Server**

Use the following steps to guide you in verifying that your OC resources are protected.

#### **Follow these steps:**

1. Log into the Policy Server Admin UI.
2. Create a new agent for OC, for example, *<UIM\_agent>*.
3. Create a new Agent Configuration Object (ACO) by copying the SPS ACO, and naming it *<nimsoft\_ACO>*.
4. Modify the default agent name key:
 

```
DefaultAgentName: <nimsoft_agent>
```
5. Optionally modify and enable the log and trace parameters.
6. Define an Application or Domain Policy to protect the OC resources, using the agent you just created (*<UIM\_agent>*).
  - a. The directory used for SiteMinder authentication is the same as that defined in the UIM Hub and in the portal.
  - b. The specific URLs to protect are as follows:
    - /web\*
    - /documents\*
    - /user\*
    - /group\*
  - c. Create a response of type WebAgent-HTTP-Header-Variable. Select User Attribute as the Attribute Kind. Use the Variable Name UMP\_USER, and the Attribute Name *<loginAttribute>*.

#### **NOTE**

This response should be enabled for all resources.

### **Edit the Secure Proxy Server Configuration**

Use the steps in this section to create a new web agent and define the virtual host for the OC server.

#### **NOTE**

Do not allow direct access to the OC server. Access should be controlled by firewall rules or other means.

#### **Follow these steps:**

1. Log into the Secure Proxy Server (SPS) host.
2. Follow the steps in the section "Web Agent Settings for the Default Virtual Host" in the [CA SiteMinder Secure Proxy Server Administration Guide](#) to copy the existing agent configuration file.
3. Issue the following commands:
 

```
cd C:\Program Files (x86)\CA\secure-proxy\proxy-engine\conf\defaultagent\
copy WebAgent.conf NimsoftWebAgent.conf
```
4. Modify the file NimsoftWebAgent.conf as follows:
 

```
AgentConfigObject="<nimsoft_ACO>"
ServerPath="ServerPath_nimsoft"
AgentIdFile="C:\Program Files (x86)\CA\secure-proxy\proxy-engine\conf\defaultagent
\NimsoftWebAgentId.dat"
```
5. Edit the SPS server.conf file in the directory C:\Program Files (x86)\CA\secure-proxy\proxy-engine\conf, and add a VirtualHost entry for OC at the end of the file:
 

```
Nimsoft UMP Virtual Host
<VirtualHost name="nimsoftump">
```

```
The hostname the user sees in their browser
hostnames="user.visible.hostname.com"
redirectrewritablehostnames="ALL"
enableredirectrewrite="yes"
enablerewritecookiedomain="yes"
enableproxypreservehost="yes"
<WebAgent>
 sminitfile="C:\Program Files (x86)\CA\secure-proxy\proxy-engine\conf\defaultagent
\NimsoftWebAgent.conf"
</WebAgent>
</VirtualHost>
```

6. Edit the proxyrules.xml in the directory C:\Program Files (x86)\CA\secure-proxy\proxy-engine\conf, and add a rule to forward requests to the OC server:

```
<nete:proxyrules xmlns:nete="http://www.ca.com/">
 <nete:cond type="host">
 <nete:case value="user.visible.hostname.com:80">
 <nete:forward>http://nimsoft.ump.hostname.com$0>
 </nete:case>
 <nete:default>
 <nete:forward>http://some.other.host.com/404.html>
 </nete:default>
 </nete:cond>
</nete:proxyrules>
```

7. Restart the SiteMinder Proxy Engine Windows service.
8. Verify that you can access OC via the virtual host defined previously in this section.

## Integrate DX NetOps Spectrum

This article provides an overview of the integration between DX NetOps Spectrum and UIM.

### Contents

#### DX NetOps Spectrum - UIM Integration Compatibility Matrix

Before you start your integration with DX NetOps Spectrum, ensure that you meet the version requirements that are described in the [compatibility matrix](#).

#### **WARNING**

From CA Spectrum v10.1.2, the SNMP Gateway probe and SBGW / Southbound gateway are no longer recommended for alarm synchronization from UIM to DX NetOps Spectrum. We recommend using the Spectrum Gateway (spectrumgtw) probe for alarm synchronization.

We also recommend that you go through the [CA Spectrum-CA UIM Integration using spectrumgtw probe - FACT SHEET](#) to understand the changes to the integration whether you are new to this integration or an existing user.

#### **NOTE**

From CA UIM 8.47 onwards, you no longer have to deploy nisapi separately. The wasp probe which is a core component in UIM contains the nisapi\_service\_host probe functionality. By default, the nisapi package is deployed in wasp as part of the UIM installation or upgrade.

---

## **Port Information**

In previous releases of UIM, the `nisapi_service_host` package was deployed to the `service_host` probe. As of CA UIM release 8.47, the `service_host` probe was deprecated and its functionality was moved to the `wasp` probe. This change has the following implications for your DX NetOps Spectrum integration:

- You no longer have to deploy the `nisapi` separately. By default, your DX NetOpsSpectrum integration uses the `nisapi` package deployed in `wasp` as part of a UIM installation or upgrade.
- You no longer have to keep port 8080 open. This port was used exclusively by the `service_host` probe.

### **NOTE**

The `wasp` probe uses port 80. However, because the `wasp` probe is a core component in UIM, this port should already be open in a properly functioning UIM environment.

## **Integration Instructions**

For the latest integration instructions for UIM and DX NetOps Spectrum, refer to the article [Integrate CA UIM and CA Spectrum](#) in the DX NetOps Spectrum documentation.

# Log Analytics

## **Contents**

### **Business Challenge**

As we move to the next paradigm of infrastructure monitoring, it is important to provide context to infrastructure performance issues as quickly as possible. Log data is an important source of information to troubleshoot problems in your applications or IT infrastructure. However, it is cumbersome to log in to individual servers and to read the log files manually to find the relevant information.

### **Solution**

Log Analytics streamlines the log analysis process and helps you troubleshoot faster and more effectively by:

- Collecting and aggregating logs from multiple sources (individual servers, devices, and applications). You can gain insights from data using analytics dashboards.
- Providing out-of-the-box dashboards (blueprints) based on the collected data for supported log types and patterns.
- Providing full text search on all the stored log files.
- Performing near real-time and historical search on all the log data from one centralized location.
- Performing a periodic query of the log data and sending notifications (alarm, email, and snmp) when matches are found. You can also save and schedule a log query or pattern to receive notifications when a match is found.

### **Benefits**

The following table includes some Log Analytics benefits.

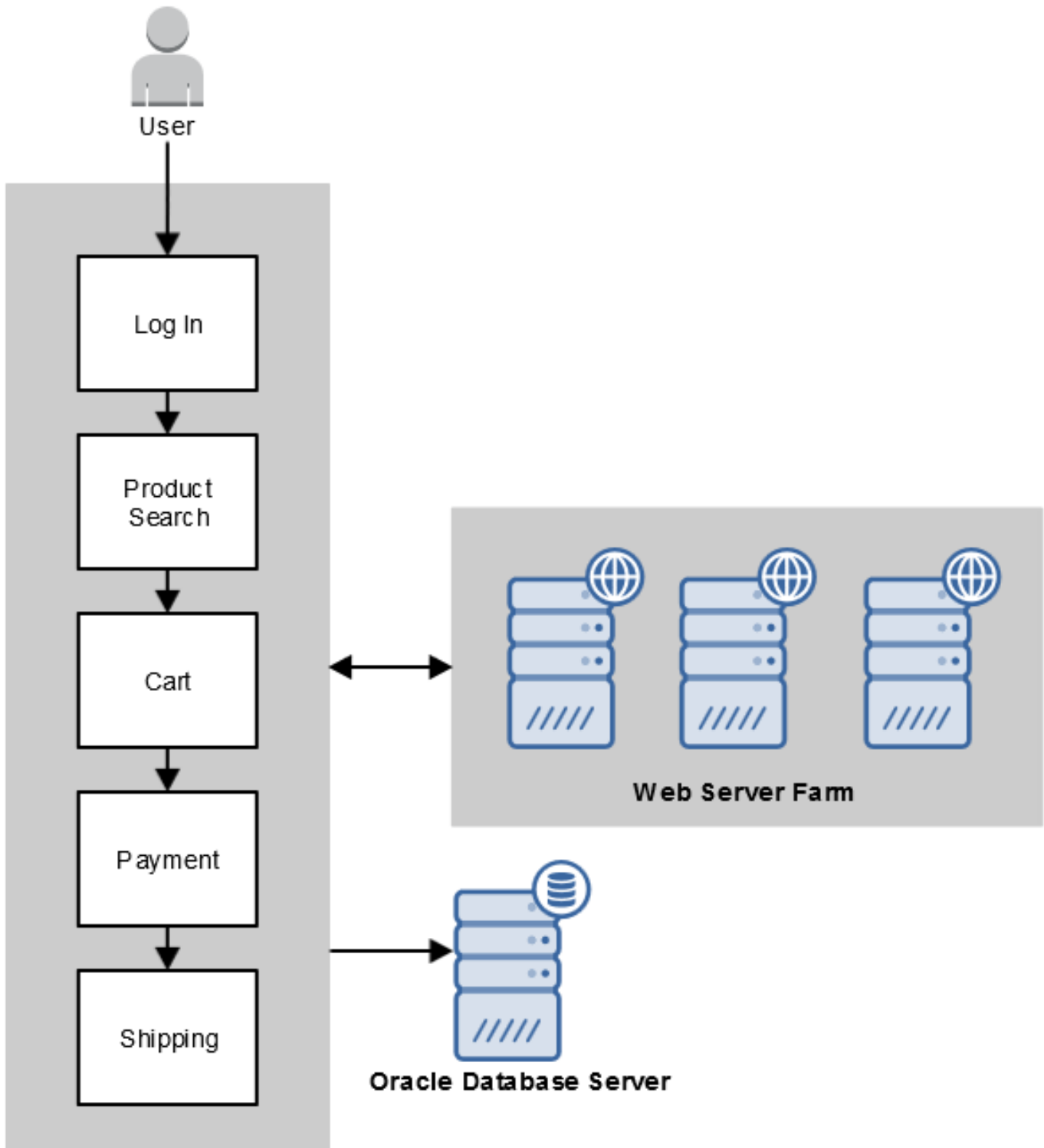
| Benefit                                                                                    | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use routine data to expose larger issues.                                                  | You can use syslog data to answer the following questions: <ul style="list-style-type: none"> <li>• What kinds of events are occurring?</li> <li>• When did the event happen?</li> <li>• Are the events happening in clusters?</li> <li>• Are there any deviations in the events that are occurring?</li> <li>• Which sources are generating the most events?</li> <li>• Which key events are happening the most often?</li> <li>• Are there any security issues occurring?</li> <li>• What severity trends are occurring?</li> </ul> |
| Monitor first-time messages from logs.                                                     | You can monitor initial messages that could potentially predict larger issues (for example, low memory messages).                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Monitor drops and spikes                                                                   | You can detect deviations in the rate of events across technologies, apps, or tools.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Monitor unusual rates of outbound requests and users attempting unusual URL access.        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Monitor syslog events, Windows events, and log information over a configurable time frame. | You can use this data see all the information across a time frame.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Use Logs and performance data for your capacity planning.                                  | You can log baseline average, peak users, and performance metrics to help define capacity utilization.                                                                                                                                                                                                                                                                                                                                                                                                                                |

### **Log Analytics Example: Monitor a Retail Website**

In the following diagram, Log Analytics monitors a retail website. Each service in the diagram is a separate system/server:

Figure 28: Log Analytics - Business Flow Part 1

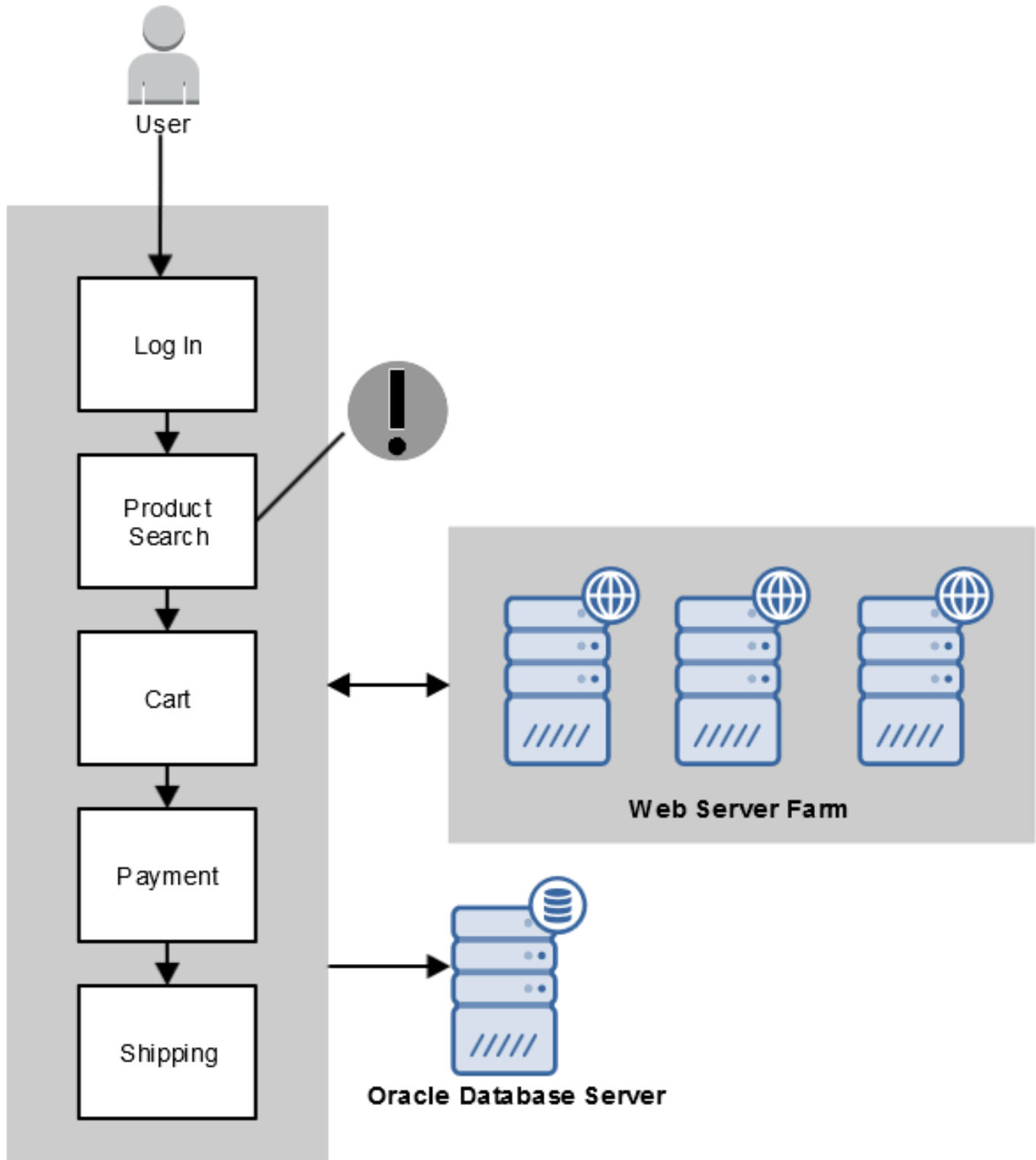
## Log Analytics Monitors a Retail Website



In the following diagram, the product search becomes slow during the course of normal operations.

Figure 29: Business Workflow Part 2

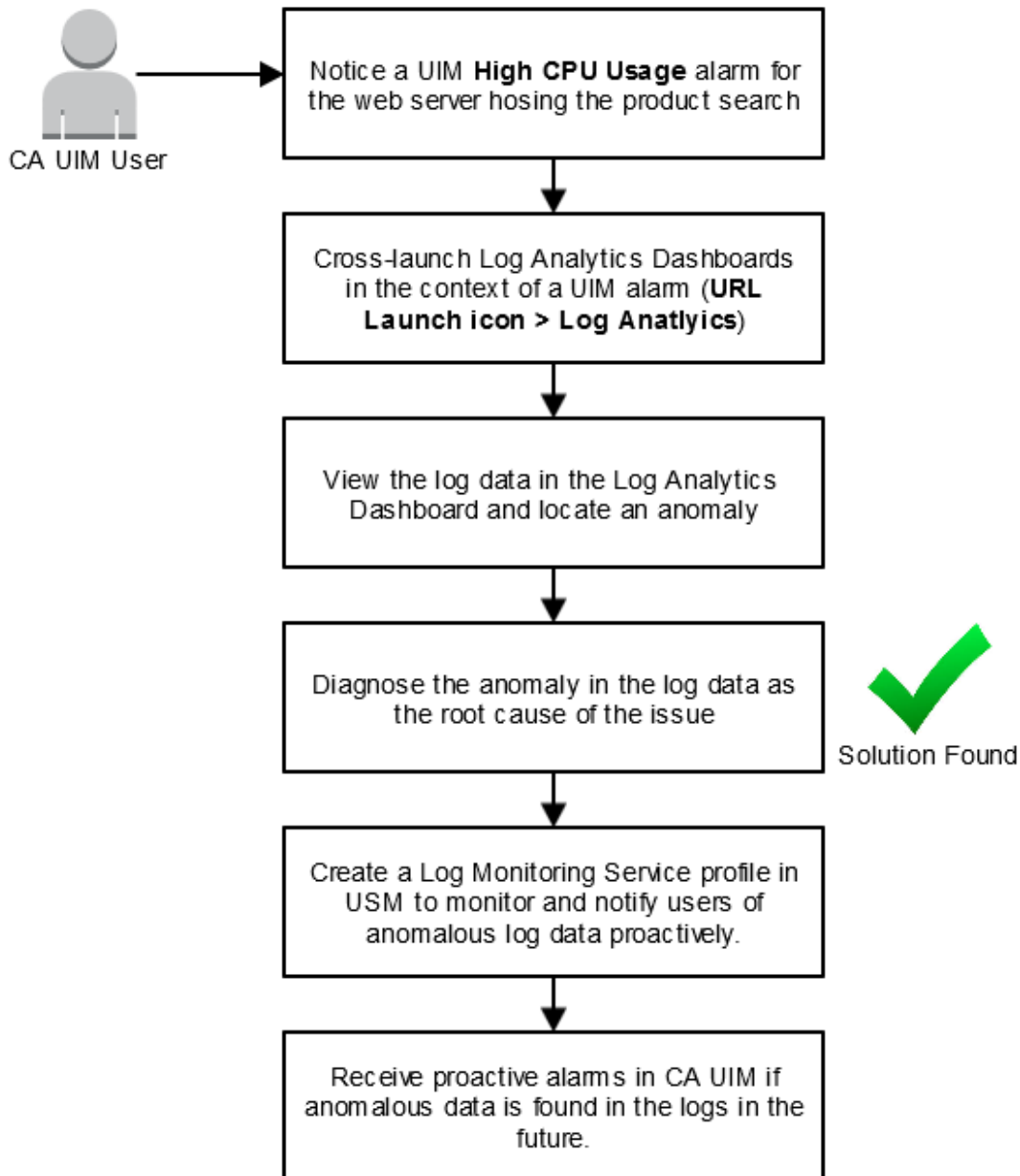
## The Product Search Becomes Slow



The following diagram lists the steps that you can take to use Log Analytics to detect and solve the issue with the product search.

**Figure 30: Business Flow Part 3**

## Log Analytics Detects and Solves the Product Search Issue



### **Required Components**

Log Analytics requires both the [Agile Operations Analytics Base Platform](#), CA UIM, and the following probes:



- Log Forwarder (log\_forwarder)
- AXA Log Gateway (axa\_log\_gateway)
- Log Monitoring Service (log\_monitoring\_service)

The following Agile Operations Analytics components are mandatory for Log Analytics:

- Data Studio (Kibana dashboards)
- Kafka and Zookeeper
- Jarvis (Includes Elasticsearch and Jarvis Ingestion, Verifier, and Indexer components)
- Read Server, UI Server, and RDBMS

### Data Studio

Primary user interface for Log Analytics. Data Studio provides out-of-the-box dashboards for the supported log types, full-text search, and ad-hoc data exploration.

### Log Collector

The AXA Log Collector receives syslog and eventlog data from remote devices over TCP (**Default Port: 6514**) and writes that data to a Kafka topic for further processing by Log Parser. After receiving the log events, the Log Collector validates the Tenant ID in the log message based on a tenant white-list and publishes the valid log data to the Kafka topic. The TCP channel receives syslog and eventlog data without installing any log agent.

Windows Event logs are also received through the syslog channel. You can use the open source tool nxlog to send the event logs through the syslog channel. For more information about configuration, see the [Agile Operations Analytics Base Platform](#) documentation.

### Log Parser

Log Parser receives log data from Kafka, parses the log data, extracts relevant fields, transforms the log data in to JSON format, and sends to Jarvis/Elasticsearch. For each supported log type, specific patterns are defined to parse and transform the data. This configuration is stored in the config files.

Data sent in any unsupported log file format is stored under **generic**. You can search this data in Data Studio but specific fields from the log data are not extracted for generic log type. And, the Out-of-the-box dashboards are not available.

### CA Analytics Platform (Jarvis)

Jarvis is used as the data store and the analytics platform to store the log data. Log ingestion to Jarvis is done by Log Parser. Each type of log data is stored as a separate document\_type in Jarvis.

### Log Forwarder Probe (log\_forwarder)

A light-weight log data collection agent. This component reads log data from log files on the monitored servers or devices and publishes the data to a CA UIM Queue (Default Subject: LOG\_ANALYTICS\_LOGS) through the CA UIM Message Bus. You can deploy and configure this probe using Monitoring Configuration Service (MCS). For more information about configuration, see the [Log Forwarder](#) probe documentation on the Probes Documentation Space.

### AXA Log Gateway Probe (axa\_log\_gateway)

The axa\_log\_gateway probe receives log data from CA UIM through a specific queue (Default Subject: LOG\_ANALYTICS\_LOGS) and writes the data to the Kafka topic (Default: logAnalyticsLogs) for further processing by the Log Parser. For more information, see the [AXA Log Gateway](#) probe documentation on the Probes Documentation Space.

### Log Monitoring Service Probe (log\_monitoring\_service)

This component is implemented as a CA UIM probe and can be configured using MCS or Admin Console (AC). This probe periodically queries log data that is stored in Jarvis and raises notifications based on the predefined queries. You can create one or more profiles. Each profile includes a query to be executed for a particular log type and the interval.

For example, "response\_time:[10 TO \*] AND url:\*ServiceDesk\*" for apache access logs scheduled every 5 minutes. The Monitoring Service queries the Elasticsearch component in Jarvis at the predefined schedule and provides the following output:

- – Match\_Count metric for the count of matches found
- Alarm if the match count exceeds a predefined threshold
- Alarms containing sample matched logs lines (number of sample lines configurable)

The Log Monitoring Service alarms can be forwarded as email or SNMP TRAP using the emailgtw or snmpgtw probe respectively. For more information, see the [Log Monitoring Service](#) probe documentation on the Probes Documentation Space.

### **Port Requirements**

Open the following ports to allow communication between CA UIM and Log Analytics

- AXA Elasticsearch port (default 9200) - Open this port between the Agile Operations Base Platform and the location of the log\_monitoring\_service probe
- AXA Kafka Port (default 9092) - Open this port between the Agile Operations Base Platform and the location of the axa\_log\_gateway probe

### **Deploy Log Analytics**

You can deploy Log Analytics using the associated templates in MCS.

#### **Follow these steps:**

1. Verify that all of the required probes are downloaded to your archive. For more information about downloading probes, see the topic [Download, Update, or Import Packages](#).
2. If necessary, create groups for the devices that you want to collect log data from. For more information about setting up groups, see the topic [Create and Manage Groups in OC](#).
3. Configure the axa\_log\_gateway probe using the **Setup axa\_log\_gateway** MCS template.
4. Deploy the log\_forwarder probe to your target devices using the **Setup log\_forwarder** MCS template.
5. Configure log forwarding for your target devices or services using one or more of the following MCS templates:
  - a. **Log Forwarding** - Configure log forwarding for any type of log file.
  - b. **Apache Log Forwarding** - Configure log forwarding for Apache access logs.
  - c. **Log4j Log Forwarding** - Configure log forwarding for java log4j logs.
  - d. **Catalina Log Forwarding** - Configure log forwarding for Tomcat Catalina logs.
  - e. **Oracle Alert Log Forwarding** - Configure log forwarding for Oracle Alert logs.
6. Configure the log\_monitoring\_service on a robot by using the **Setup log\_monitoring\_service** template.

#### **NOTE**

We recommend using the primary hub robot.

7. Create your desired profiles using the **Log Monitoring Service** template. You can use this template to query the log data that is stored in Jarvis and send alarms based on your defined criteria.
8. **(Optional)** Configure the **Email Gateway (emailgtw)** MCS template to receive email notifications when alarms occur.
9. **(Optional)** Configure the **SNMP Gateway (snmpgtw)** MCS template to receive SNMP notifications when alarms occur.

### **Configure Cross-Launch**

Before you can launch the Log Analytics dashboard from a CA UIM alarm, you must create a URL action to enable cross-launch.

**NOTE**

To launch a custom URL action, you must have the *Launch URL Actions* ACL permission set. With this permission, you can select an alarm, then launch an alarm action from the **Actions** menu.

**Follow these steps:**

1. In OC, select the **Alarms** view.
2. Click the **Actions** menu above the list or table of alarms, then **Edit URL Actions**. The **Edit URL Actions** dialog opens.
3. Click **New URL action**. Specify the name **Log Analytics** and enter the following URL:
 

```
http://<server_host>:<server_port>/mdo/v2/dashboard/loganalytics?query="host:${host}"×tamp=${TIME_LAST}&probe=${PROBE}&customAttributes='${CUSTOM_1}'
```
4. Change the following parameters in the URL:
  - **<server\_host>** - The host name for your [Agile Operations Analytics Base Platform](#).
  - **<server\_port>** - The port that your [Agile Operations Analytics Base Platform](#). The default port is 9080.

After configuring cross-launch, the **Log Analytics Launch** icon appears for each UIM alarm. Clicking this icon opens the Agile Operations Analytics Base Platform log in page. After logging in, you are then redirected to the **Log Analytics Dashboard** in the Data Studio. The following in-context parameters can be passed in the URL:

- **The Log Analytics Dashboard is launched from an alarm generated by the log\_monitoring\_service probe** - The query parameter uses the value provided in the log\_monitoring\_service profile configuration.
- **The Log Analytics Dashboard is launched from an alarm generated by any other probe** - The query parameter uses the host value from the UIM alarm.

**NOTE**

If you have not registered your app, clicking the **Log Analytics Launch** icon redirects you to the app registration page in CA App Experience Analytics.

**More Information**

For more information about deploying Log Analytics, see the following topics:

- The Monitoring Configuration Service topic
- The [Agile Operations Analytics Base Platform](#) documentation.
- The associated probe documentation on the [Probe Documentation Space](#):
  - emailgtw
  - log\_forwarder
  - log\_gateway
  - log\_monitoring\_service
  - snmpgtw

---

## Working with Development Tools

---

Development tools are available to help developers create and manage CA UIM components. Software Development Kits (SDKs) and Application Programming Interfaces (APIs) are available for several different programming languages.

### Contents

#### .NET API

The CA UIM .NET API is developed using Microsoft .NET version 2.0. Classes in the .NET API can be instantiated or inherited by any CLI compliant language, such as C#, Visual Basic .NET, and C++/CLI. The .NET API contains classes for sending alarms and QoS data, making it easy to develop .NET applications that communicate with CA UIM.

- [Download the .NET API Overview as a PDF.](#)
- [Download the HTML API Reference.](#)

#### C SDK

The C SDK allows you to create and modify QoS and alarm messages using the C programming language.

- [Download the C SDK Reference Guide as a PDF.](#)

#### Java SDK

The Java SDK provides classes and methods to modify QoS and alarm messages using the Java programming language.

- [Download the Javadoc for the Java SDK.](#)

#### nas Extensions to Lua

You can use the nas script editor to create and edit scripts using the Lua scripting language. These scripts can be selected to be used by the Auto Operator when processing alarm messages matching the criteria defined for the Auto Operator profile. Scripts can also be run by the Scheduler.

For more information, see the [nas](#) documentation on the Probes Documentation Space.

#### Perl SDK

The Perl SDK allows you to build everything from scripts generating simple alarms to powerful client/server solutions. The Perl SDK modules wrap the Message Bus API functions, making it easier to develop CA UIM probes using Perl.

- [Download the Perl SDK Guide as a PDF.](#)

#### Probe Software Developer Kit Guide

Probe Software Developer Kit Guide is for developers who want to create a monitoring probe that is configurable using Admin Console. See the [Probe Software Developer Kit](#) section on the CA Unified Infrastructure Management Probes site for more information.

#### RESTful Web Service

You can use the RESTful web service interface for CA UIM to access your UIM installation using REST-based web service calls. The RESTful web services are deployed using the uimapi and webservices\_rest probe packages. We recommend that you use the RESTful web services that the uimapi probe package provides, because it includes

the modern Swagger documentation and endpoints to work with the APIs. It encapsulates improvements made over `webservices_rest`.

For more information, see the [Probe Development Tools](#) section of the Probes Documentation Space.

## The NimAlarm Utility

The NimAlarm utility is used to send alarm messages across the UIM Message Bus using the operating system command line.

### Contents

By default, NimAlarm is located in the following locations:

- `<CA UIM installation path>\Nimsoft\bin`
- `<CA UIM installation path>/nimsoft/bin/`

### NimAlarm Options

NimAlarm uses the following command format:

```
nimalarm [-l alarm severity] [-s subsystem ID] [-c checkpoint id] [-d debug level] [-S source] [-i]
[-1 custom field 1] [-2 custom field 2] [-3 custom field 3] [-4 custom field 4]
[-5 custom field 5]
[-t CI type] [-n CI name] [-m CI metric] [-a alarm token] [-V u.data values] "alarm message"
```

- **-l *alarm severity***

(Optional) Defines the alarm severity. The following severities can be set:

- 0 (clear)
- 1 (information)
- 2 (warning)
- 3 (minor)
- 4 (major)
- 5 (critical)

**Default:** 1 (Information)

**Limit:** 0 - 5

- **-s *subsystem ID***

(Optional) Defines the subsystem ID for the alarm. The subsystem ID identifies which part of the system an alert relates to. A list of subsystems and their associated IDs is available in the **Subsystems** tab of the nas configuration GUI.

**Default:** 1.1

- **-c *checkpoint id***

(Optional) Defines the checkpoint ID. The checkpoint ID is also known as the alarm suppression key and is used to clear alarm messages. For more information, see [Clear an Alarm](#).

- **-d *debug level***

(Optional) Defines the logging level of the NimAlarm utility. This option also displays debug messages as the alarm is being sent across the message bus. The following logging levels can be set:

- Level 0- No logging.
- Level 1- Logs any returned alarm messages.
- Level 2- Logs additional warnings.
- Level 3- Logs informational messages.
- Level 4- Logs debugging messages.
- Level 5- Logs tracing/low-level debugging messages.

**Limit:** 0-5

- **-S source**

(Optional) Defines the udata.source field in the alarm PDS. This sets the alarm Source and Hostname.

#### **NOTE**

The source field specified in NimAlarm is not the same as the source in the message header. The message header source is the IP address of the robot. The source added by NimAlarm is the IP address of the device the alarm originated from.

- **-i**

(Optional) Prints the nimid for the alarm in the console after being sent. The nimid is the unique key assigned to an alarm message and can be used to:

- look up alarms in the nas\_transaction\_summary table.
- establish event correlation with products such as CA Service Operations Insight or CA UIM Service Desk.
- change or view the alarm using the nas command interface or Lua extensions.
- **-1 custom field 1**

(Optional) Defines the udata.custom1 field in the alarm PDS. This appears as the Custom 1 field in the alarm message.

- **-2 custom field 2**

(Optional) Defines the udata.custom2 field in the alarm PDS. This appears as the Custom 2 field in the alarm message.

- **-3 custom field 3**

(Optional) Defines the udata.custom3 field in the alarm PDS. This appears as the Custom 3 field in the alarm message.

- **-4 custom field 4**

(Optional) Defines the udata.custom4 field in the alarm PDS. This appears as the Custom 4 field in the alarm message.

- **-5 custom field 5**

(Optional) Defines the udata.custom5 field in the alarm PDS. This appears as the Custom 5 field in the alarm message.

#### **NOTE**

The custom alarm fields are not used in UIM alarm messages by default. They can be optionally added to an alarm message and are useful for adding additional information to alarm messages. For example, you could add the OS type for a device to the Custom 1 field.

- **-t CI type**

(Optional) Defines the CI type. A CI type represents a group of related metric types. For example, the CI type for Disk can contain metrics for throughput, capacity, and free space. CI type is represented by a numeric value. The following example is the CI type for Disk.

**Example:** 1.1

- **-n CI name**

(Optional) Defines the CI name.

**Example:** C:\

#### NOTE

The *-t* and *-n* options are used by the nimbus API to look up the device ID in niscache and insert it into the alarm message. The device ID is a unique identifier for the device an alarm was sent from, and is required for an alarm to properly appear in UMP. You can also add the device ID to test pre-processing rules or Auto-Operators that are using the device ID. CI types and names are located in the UIM database *cm\_configuration\_item* table.

*-t* and *-n* must be used together. If only one is used, the device id is left blank.

- ***-m CI metric type***

(Optional) Defines the CI metric type. The CI metric type is a numeric value that specifies a measurement that is available for a CI type. This value is used by the nimbus API to look up the metric ID in niscache and insert it into the alarm message.

The metric ID is the unique identifier for the metric that originated the alarm. Like the device ID, the metric ID is required to view the alarm in UMP and can be used to test pre-processing rules or Auto-Operators. The following example is the CI metric type for Disk Space.

**Example:** 1.1:10

#### WARNING

The metric ID is looked up independently of the device ID. This means that NimAlarm can accept an inconsistent combination of CI type/name, and metric type. Verify that all of the CI metric values are correct before entering a command.

- ***-a alarm token***

(Optional) Defines the *udata.token* field in the alarm PDS, which sets the internationalization token for the alarm message. For more information on using the internationalization token, see Use a Localized Alarm in UMP.

- ***-V udata values***

(Optional) Defines the *udata.values* field in the alarm PDS, which sets the values that are used in the internationalized alarm messages fetched by the *-a* option. The values are entered as key-value pairs. The key is a variable used in the alarm message, and the value is the corresponding simple value that will be substituted into the alarm message.

**Limits:** There are no limits on the number of key-value pairs entered.

#### WARNING

Do not include spaces between key-value pairs. Including spaces corrupts the argument parsing. The keys must match the alarm tokens set with the *-a* option to work properly with internationalization.

**Example:** `ipAdress=10.238.1.129;robot=myRobotName;`

- ***"alarm message"***

Defines the alarm message. The alarm message must follow all other arguments. An alarm message is still required even when an internationalization token is entered, as the alarm message associated with the token only appears in localized versions of UMP. The text entered as an alarm message appears in all other instances.

**Limits:** The alarm message can include spaces if it is surrounded by quotation marks.

### NimAlarm Command Examples

#### Change the Severity of an Alarm

You can use the NimAlarm utility to change to increase or decrease the severity of an existing alarm using the *-l* option. For example, the following command sends a minor alarm:

```
nimalarm -l 3 "Test Message."
```

To increase the severity of the alarm to critical, enter the following:

```
nimalarm -l 5 "Test Message."
```

### **Clear an Alarm**

You can clear an alarm message with NimAlarm by setting the `-l` option to 0 and inducing the alarm suppression key with the `-c` option. For example, if you create the following message:

```
nimalarm -l 1 -c 12345 "Test Message."
```

You can clear it with the following command:

```
nimalarm -l 0 -c 12345 "Test Message."
```

### **Use a Localized Alarm Message in UMP**

Each alarm message has an associated internationalization token that is used to call the translated version of an alarm message in UMP. The list of English alarm messages and their associated tokens can be found in the `Nimsoft.properties` file, located in the `\Nimsoft\probes\service\wasp\i18n` directory.

Each supported language has its own properties file that contains the localized version of the message and shared token. For example, if you wanted to view the German version of the following English message:

```
as#network.dhcp_responce.dhcp_srv_didnot_response = DHCP server ${hostname} did not
respond
```

You could use the localization token `as#network.dhcp_responce.dhcp_srv_didnot_response` to search for the message in the `Nimsoft_de.properties` folder:

```
as#network.dhcp_responce.dhcp_srv_didnot_response = DHCP-Server ${hostname} hat nicht
geantwortet
```

To test this message in NimAlarm, set the alarm token with the `-V` option:

```
nimalarm -t 2.2.3.1 -n Response -m 2.2.3.1:1 -V
as#network.dhcp_responce.dhcp_srv_didnot_response "DHCP server mySystemHostname did not
respond"
```

#### **NOTE**

The `-t`, `-n`, and `-m` options are required for UMP. If these options are not used, the alarm will not appear.

Additionally, you must set the variable `${hostname}` using the `-a` option:

```
nimalarm -t 2.2.3.1 -n Response -m 2.2.3.1:1 -V
as#network.dhcp_responce.dhcp_srv_didnot_response -a hostname=mySystemHostname "DHCP
server mySystemHostname did not respond"
```

## **Create Custom Scripts for Application Discovery**

Application Discovery is an optional feature that is available with CA UIM. Application Discovery enables users to efficiently discover devices in their environment and to apply monitoring configuration for them using the Monitoring Configuration Service (MCS) in the OC interface. In the Administration dialog of the OC interface, you select which applications that you want the Application Discovery scripts to discover. In the MCS, select which default monitoring



profiles that you want to enable. View the monitoring data in the CA Unified Infrastructure Management visualization components, including OC or the CABI Dashboards for CA Unified Infrastructure Management.

**NOTE**

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

Application Discovery comes with default scripts that determine the discovery of the applications that are running on your system:

- Apache
- IIS
- MySQL
- Microsoft SQL
- Oracle

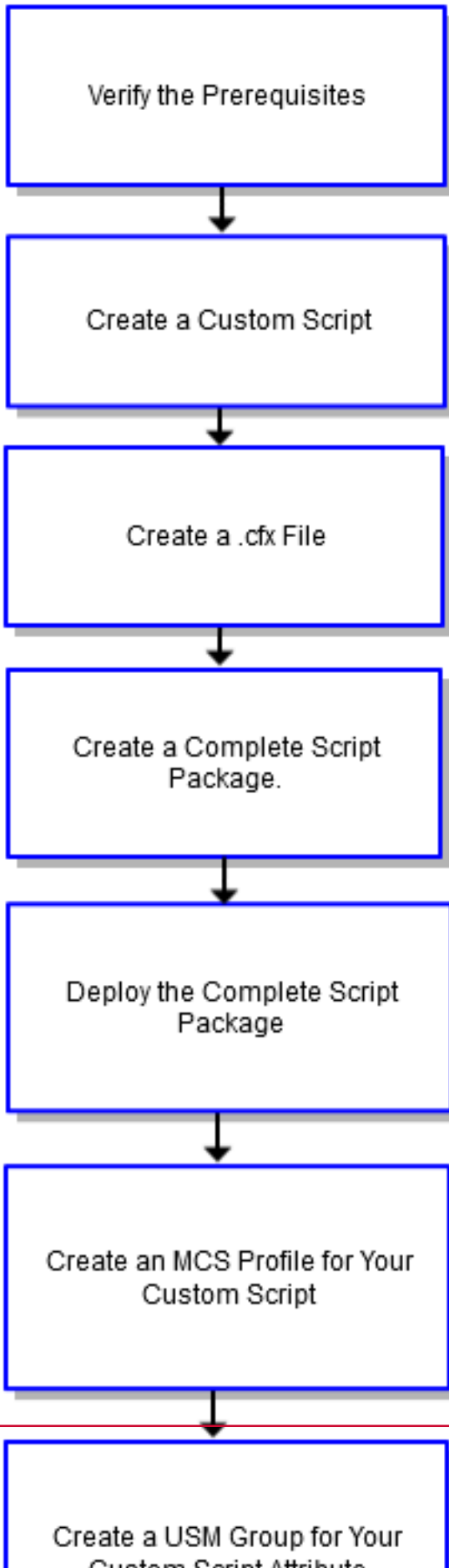
If you are a CA UIM bus user, you can create custom Application Discovery plug-in scripts. Your custom scripts can be either batch or shell scripts.

**WARNING**

Use a high level of caution when creating scripts. Create and use custom scripts only if you are experienced with scripting. Scripts can negatively impact the installation and performance of your CA UIM system.

**Contents****Workflow Diagram**

The following workflow diagram shows the steps that you take to modify/create a script:

**Figure 31: Create a Custom Script for Application Discovery**

---

## **Verify Prerequisites**

To create custom scripts, first verify that you meet all the prerequisites for the Application Discovery feature. For more information, see [Use Application Discovery](#).

## **Create a Custom Script**

Prepare to write successful batch or shell scripts by first understanding the standards that work with the Application Discovery.

## **Understand Key Terms**

### **Attributes**

An attribute is a key value pair that has the form key=value.

### **Keys**

The key name of a property can be A-Z, a-z, 0-9, dot, dash, and underscore. Key names are limited to 150 characters. The maximum number of keys that the plug-in will publish per run is 200.

### **Values**

The value of a property can be anything, except that it cannot contain double quotes. Values are limited to 250 characters.

## **Publishing Phase**

The plug-in encodes the attributes it receives from scripts into device.dev files in the niscache directory. The discovery\_server periodically inspects the niscache files and places any attributes it finds into the CA UIM database. This is the publishing phase.

## **Publishing Attributes**

To publish an attribute, a script echoes or prints a key-value pair to the standard out (stdout). The plug-in accepts as an attribute any key-value pair that follows the correct format. The plug-in throws away any output that does not adhere to the correct format.

For example, if you want to publish a key that is named Application with a value of "Apm," the script sends the following line to standard out:

```
Application=Apm
```

The plug-in processes it, turning it into a key with the following format:

```
UserPropMV.script_filename.keyname
```

If the script is configured to run with the script\_filename "myscript," and the key is named Application with a value of "Apm," then we get:

```
UserPropMV.myscript.Name=Apm
```

Keys are published as properties that you can filter on to create and manage groups in OC. If a script echoes out more than one value for the same key, then it becomes a multivalue property. So, if a script echoes out:

```
echo Name=Apm
echo Name=Apache
```

The plug-in publishes the property as one multi-value property:

```
UserPropMV.myscript.Name=Apm,Apache
```

## **Review the Examples**

### **Batch Script Example**

The batch script example shows how you can use a script to discover systems that are based on whether a system is a 32-bit or 64-bit system.

```
@echo OFF
reg Query "HKLM\Hardware\Description\System\CentralProcessor\0" | find /i "x86" > NUL &&
 set sys_arch=32BIT || set sys_arch=64BIT
if %sys_arch%==32BIT echo Sys_arch=32bit
if %sys_arch%==64BIT echo Sys_arch=64bit
```

### **Code Walk Through**

Line 1 = Do not send output to the command line.

```
@echo OFF
```

Line 2 - Determine whether a system has a 32-bit or 64-bit central processor.

```
reg Query "HKLM\Hardware\Description\System\CentralProcessor\0" | find /i "x86" > NUL &&
 set sys_arch=32BIT || set sys_arch=64BIT@echo OFF
```

Line 3 - If the system architecture is a 32-bit system, then echo out a key value pair with that information: Sys\_arch=32bit.

```
if %sys_arch%==32BIT echo Sys_arch=32bit
```

Line 4 - If the system architecture is a 64-bit system, then echo out a key value pair with that information: Sys\_arch=64bit.

```
if %sys_arch%==64BIT echo Sys_arch=64bit
```

The plug-in processes the standard output of the script (the key value pair, also known as an attribute) and publishes them to the nis\_cache on the nis\_server. The nis\_server creates groups for known applications based on their attributes. The attributes are also stored in the CA UIM database.

### **Shell Script Example**

The shell script example shows how you can use a script to discover systems that are based on their IP addresses.

```
#!/bin/sh
ip_addr=$(hostname --all-ip-addresses)
set -- $ip_addr
echo ip_addr=$1
```

### **Code Walk Through**

Line 1 - This script is a shell script.

```
#!/bin/sh
```

Line 2 - Execute the command, "hostname all IP addresses".

```
ip_addr=$(hostname --all-ip-addresses)
```

Line 3 - Split the variable into component strings, isolating the IP address.

```
set -- $ip_addr
```

Line 4 - Echo out the key value pair, where the variable is filled by the value that the command found. For example, the key value pair: ip\_addr=172.16.0.0.

```
echo ip_addr=$1
```

The plug-in processes the standard output of the script (the key value pair, also known as an attribute) and publishes them to the nis\_cache on the nis\_server. The nis\_server creates groups for known applications based on their attributes. The attributes are also stored in the CA UIM database.

When you are familiar with the standards described above, create your custom script and save it to your local system. You add the script to a complete script package for Application Discovery.

### **Create a .cfx File**

To create a complete script package for Application Discovery, you also need to create a .cfx file. A cfx file modifies the plug-in configuration file at the time of installation to include a new script section. Create a cfx file named, "atr\_publisher.cfx." Give the relevant values for the section header <script1> and filename. Use the default value for interval or enter a relevant value:

```
<variables>
 <scripts>
 <script1>
 filename=filename
 interval=interval
 </script1>
 </scripts>
</variables>
```

### **Configuration Format Explanation**

- • **scripts**  
Do no change or modify the scripts tag.
- **filename**  
Give the file a name. Filenames are limited to the standard 260 characters on Windows and 2047 characters on Unix.
- **interval (script)**  
Specify the interval (seconds) for a single script to set only the interval at which that particular script runs. The default value is the value that is inherited from the interval for the .cfg. If you specify an interval for a script, that interval overrides the .cfg interval. The minimum value is 10. All values are rounded up to the nearest tens. For example, 18 rounds to 20.
- **grace period**  
The default grace\_period value is the value that is inherited from the grace\_period in the .cfg. If you specify a grace\_period for a script, that grace\_period overrides the .cfg grace\_period.

### **Create a Complete Script Package for Application Discovery**

To create a complete custom script package for Application Discovery you:

1. Create the custom script package
2. For *each* OStype section of your custom script package, add your .cfx file .
3. For *each* OStype section of your custom script package, add a dependency on the Attribute Publisher plug-in.

Do steps 1-3 all in the same New Package dialog in the Infrastructure Manager interface.

**TIP**

Tip: For an example of a complete script package for Application Discovery, see the `app_disco_apache` script package in the Archive in IM. Note that the `app_disco_apache` script package and your custom script package are not identical, however. To create your custom script package, follow the steps below.

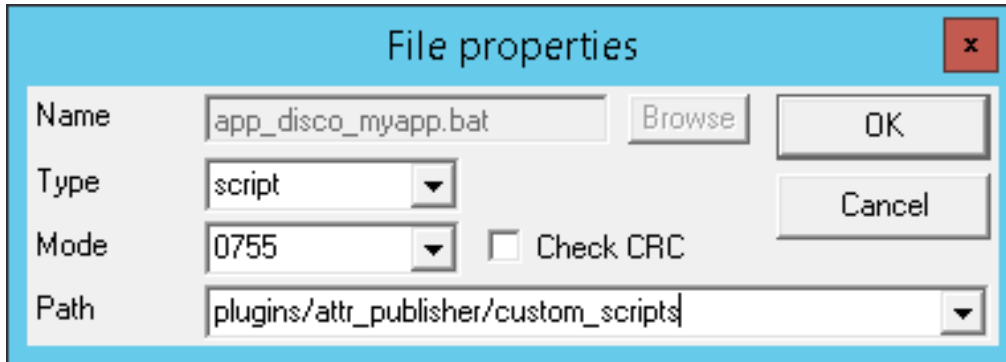
**Create a Script Package****Follow these steps:**

1. In Infrastructure Manager, select Archive, and then right-click anywhere in the top right window.
2. Select **New...**  
A New Package dialog appears.
3. Enter a name and description for your package.
4. In the New Package dialog, above **OStype label**, right-click on the tab outline to create a new tab.
5. Click **Add section...**
6. Give the new section a name.  
For example: windows
7. Specify an **OStype** for this section.
  - a. (Optional) select an **OS**.

8. Click on the **Files** tab.
9. Right-click in the window below the **Files** tab.
10. Select **Add file...**

11. Select **Browse** and browse to your script.
12. Click **OK**.
13. Update the path value so that it is the relative path from the CA UIM installation location to your custom scripts directory.

For example: `plugins/attr_publisher/custom_scripts`



14. Click **OK**.  
You created your custom script package. Next, add your `.cfx` file to your custom script package.

### **Add .cfx Files to the Script Package**

#### **WARNING**

You must add a `.cfx` file for each OStype that you add a section for in the script package. For instance, if you add a section for a Windows OStype and a section for a Unix OStype, you must add a `.cfx` file to both sections in the package.

#### **Follow these steps:**

1. In the same New Package dialog in which you recently created your custom script package, right-click in the window below the **Files** tab.
2. Select **Add file...**
3. Select **Browse** and browse to your `.cfx` file.
4. Click **OK**.  
You added your `.cfx` file to your custom script package. Next, add a dependency on the Attribute Publisher Plug-in to your custom script package.

### **Add Dependencies on the Attribute Publisher Plug-in to the Script Package**

#### **WARNING**

You must add a dependency on the Attribute Publisher for each OStype that you add a section for in the script package. For instance, if you add a section for a Windows OStype and a section for a Unix OStype, you must add a dependency to both sections in the package.

If you do not add a dependency on the Attribute Publisher plug-in to your script package, the Attribute Publisher could fail. When the Attribute Publisher fails, the entire Application Discovery feature is disabled.

#### **Follow these steps:**

1. In the same New Package dialog in which you recently added a `.cfx` file to your custom script package, click on the **Dependencies** tab.
2. Right-click to **Add a Dependency**.
3. A Dependency properties dialog appears.

Dependency properties

Name attr\_publisher

Version 7.90

Build

Type

ge  le  eq

gt  lt  Any

Restart if dependency is updated

Enter or select the options described below:

- a. **Name**  
Enter the name of the Attribute Publisher plug-in:  
attr\_publisher
  - b. **Version**  
Enter the minimum required version number for the robot:  
7.90
  - c. **Build**  
Leave this field blank.
  - d. **Type**  
Select **ge**, which means greater than or equal to.
4. Click **OK** to create the dependency.
  5. Click **OK** again to leave the package editor.



Package: app\_disco\_myapp

Properties

Name: app\_disco\_myapp    Author: Administrator

Description: Demo Test Script    Date: 2/8/2017

Copyright: (C) Copyright 2017    Version: 1.0    No direct install:

Group: Infrastructure    Build: 1    License required:

OS type: windows    OS:

Files | Probe definitions | Environment variables | Dependencies | Miscellaneous


| Name            | Type   | Mode | Path                                  |
|-----------------|--------|------|---------------------------------------|
| app_disco_my... | script | 0755 | plugins/attr_publisher/custom_scripts |

Ok    Cancel    Help

### Deploy the Complete Script Package

You can deploy a package from the local archive of any hub that has the `automated_deployment_engine` probe to any robot in your infrastructure.

#### Follow these steps:

1. In Admin Console, select a hub, and select the **Archive** tab.
2. Do one of the following:
  - Single package – select the inline menu button  to a package, and then select **Deploy**.
  - Multiple packages – select the checkboxes next to multiple packages, and then select **Actions > Deploy**.
3. In the **Hubs** pane, select the check box next to a hub to select all the robots under the hub. Or, drill-down into the hub and select individual robots. To return to the list of hubs, click the back arrow in the middle pane. The **Target Robots** pane updates to show the selected robots.
4. Select **Deploy**.

The page redirects to the **Deployment Activity** tab where you can monitor the deployment.

### **Verify That the Package Deployed**

After a package has been deployed to a robot, if the package is a probe, it is displayed in both the **Installed Packages** tab and the **Probes** tab. If the package is not a probe, it is only displayed in the **Installed Packages** tab.

#### **Follow these steps:**

1. Select the hub, and then select the robot where the probe was deployed.
2. Select the **Installed Packages** tab.

### **Create an MCS Profile for Your Custom Script**

After you deploy a package containing a custom script, you enable the Attribute Publisher plug-in to use it. To enable the Attribute Publisher plug-in to use your script, you create an MCS profile for it.

#### **Follow these steps:**

1. Click the Application Discovery Scripts profile.
2. Click the plus icon to add a script.
3. (Optional) Accept the default value or modify the **Group Profile Priority**.  
For more information about how Group Profile Priority works, see [Monitoring Configuration Service](#).
4. Enter a **Package Name** for your custom script.
5. Enter a **Script Filename** for your custom script.
6. (Optional) Accept the default value or modify the **Interval**.  
The default value is 24 hours.
7. Click **Create** or **Save**.
8. Repeat the process for each script that you want to add.  
An added script profile appears in the MCS navigation tree as a child of the Application Discovery Scripts profile type.

### **Create a Group for Your Custom Script Attribute (Application)**

To monitor devices with the attribute that you discovered using your custom script, create a group for this attribute (application).

**Note:** You must have OC Group Modifications permission to create, edit, and delete groups.

#### **Follow these steps:**

1. In a badge or tree view, click on a container group and select **Add Group** from the **Actions** menu or hover to the right of an existing group and click on the **+** symbol.  
You can only add a new group under an existing container (Parent) group.
2. In the **Properties** tab, edit the settings as needed:
  - **Add Template** - Select a template from the menus in the Report Templates window.
  - **Delete Template** - Select a template and delete it from the list.
  - **Default** - Set a template in the list as the default for group reports.
  - **Group Type** - Select **Container**, **Dynamic**, or **Static**.
  - **Member Type** - Select **System** or **Interface**
  - **Name** - Enter a name for the group.
  - **Description** - Enter a description of the group.
  - **Account** - Select **No Account** if you do not want account contact users to see the group. Or, select an account so that only account contact users assigned to that account or bus users can see the group (account contact users from other accounts cannot see the group).
  - **Filters** - Define a filter to populate the group.
3. Click **Apply Filters** to list discovered systems for a new group.

All listed systems are included when you create a Dynamic group. You must select at least one listed system to create a Static group by selecting it in the **Included** column. You can modify existing groups by changing the filters for a Dynamic group or selecting and deselecting systems from the filtered list for a Static group

4. In the **Report Templates** tab, edit the settings as needed:  
**Note:** No report templates are available for Container or Interface groups.
5. Click **OK** at the bottom of the window.

### **Add a Filter for the Group**

You can set various filter options to select the members for each group you create. Filters for both System and Interface type groups include:

- Boolean operators *and*, *or*, and *not*.
- A pull-down list of previously discovered properties. You can also enter an SQL query from the properties list.  
**Note:** To use the SQL query option, you must be a bus user with Portal Administrator permissions. Also, queries must include the column *cs\_id* for devices and *me\_id* for interfaces.
- A condition list (*is*, *contains*, *starts with*, ...).  
**Note:** The conditions list also contains the option *undefined* for properties without defined values. When the option *undefined* is selected, the values field is disabled.
- A values field.
- For static groups, create the filter and then select which of the listed systems to include in the group. For dynamic groups, create a filter to specify the systems to add to the group. The list of members in the dynamic group is automatically updated every 5 minutes.

#### **Follow these steps:**

- a. Click on the group type in the **Group Type** menu.
- b. Verify that **System** is selected in the **Member Type** field.
- c. In the **Filters** section of the **Properties** tab, select the second pull-down menu and select **SQL**.
- d. Click **Edit Query**.
- e. Enter an SQL query string the dialog. Use a join query with the relevant key name and value to find the attribute for a custom script.

#### **Format:**

```
select distinct cs.cs_id from CM_COMPUTER_SYSTEM cs join CM_COMPUTER_SYSTEM_ATTR a on
a.cs_id=cs.cs_id where a.cs_attr_key like 'UserProp%.YourKey' and a.cs_attr_value='YourValue'
```

#### **Example:**

```
select distinct cs.cs_id from CM_COMPUTER_SYSTEM cs join CM_COMPUTER_SYSTEM_ATTR a on
a.cs_id=cs.cs_id where a.cs_attr_key like 'UserProp%.Port' and a.cs_attr_value='8080'
```

If your query is valid, it returns computer system IDs from the CM\_COMPUTER\_SYSTEM table.

- f. When you have defined the rows for the filter, click the **Apply Filters** button to confirm the results in the **Members** table. Systems that have not yet been added to the group are shaded in gray.  
**Note:** Not all systems that match the filter criteria can be displayed; up to 100 systems that match the filter are displayed. For dynamic groups, all systems that match the filter are included in the group, even if they are not displayed in the **Members** table when you click **Apply Filters**. To view all members in the group, save the group and click on the group in a badge or tree view. For static groups, existing group members are displayed in addition to the filter results. If more than 100 systems match the filter and you do not see the systems that you want to add to the group, you might need to refine the filter criteria so that the systems you want to add are displayed in the **Members** table.
- g. If the filter is for a static group, click the boxes in the **Included** column to select the systems to add to the group.
- h. Click **OK**.
- i. The filter is saved and the systems added to the group are no longer shaded in gray in the **Members** table.

For more information about how to create and manage Application Discovery group monitoring profiles in MCS, see [Use Application Discovery](#).

---

## Create Additional Configuration Profiles for the Group in MCS

### Follow these steps:

1. In OC, navigate to your group.
2. Access the MCS pane.  
The MCS configuration pane appears. The available profile types for each device appear in the middle column of the MCS pane.  
**Note:** The Application Discovery group profiles appear with an orange pause icon that indicates they are in a suspended state. To apply monitoring to a group, accept or modify the default configuration in the profile and then click **Enable**. Once you enable a profile, the suspended icon goes away and a **Save** button replaces the **Enable** button.
3. Click the arrow next to the profile type to expand it. Then, click on the configuration profile for the subgroup.  
For example, Discovered Apache.
4. Accept the default configuration in the profile or modify it.
5. Click **Enable** (or **Save**) at the bottom of each profile to save your changes and to activate the profile.  
**Note:** When you click **Enable**, the profile is active. Thereafter, the **Enable** button goes away and is replaced by a **Save** button. You cannot put the profile back to a suspended state.
6. Repeat steps 1 through 5 as needed.

### TIP

You can use variables in the MCS configuration profiles. For more information, see the topic, Using Variables in Configuration Profiles, at [Manage Monitoring Using MCS Profile Types](#).

---

# Troubleshooting

---

If you experience issues, check these troubleshooting articles and try the recommended actions in the order in which they are described:

## Troubleshooting Admin Console

### Error When Trying to Open a Probe Configuration GUI on a Secondary Hub

**Symptom:**

When I try to open a probe configuration GUI on a secondary hub, I see *Error: Unable to read configuration*. I receive the error code **MONS-021**.

**Solution:**

Deploy the PPM probe to the hub. The PPM probe is required for probe configuration GUI operation.

### How to Find UMP Version

**Symptom:**

I want to know the version number of OC in my CA UIM environment. How can I do so?

**Solution:**

To check the version number for Operator Console (OC), enter "html/version.txt" in your browser address bar, after the UMP "IP/" or "hostname/." For example:

```
http://<UMP_Server_name_or_IP_address>:/html/version.txt
```

A page displays the Version, Build Label, Build Date, and Build Number.

### How to Find Hub Version in Admin Console

**Symptom:**

I want to know the version of the hub in my CA UIM environment. How can I do so in Admin Console?

**Solution:**

To check the version number of a hub, follow these steps:

1. In the left-hand navigation tree, click on the desired machine.
2. In the main window, a table of all probes, including the hub, appears with a header that includes the Version.

### Admin console returning 408 error

**Symptom:** Admin Console returns 408 error on the latest chrome browser. Latest chrome browser enforces the stringent Samesite cookie rule whereas UIM WASP is configured with Samesite Lax.

**Solution:** Follow the below steps to verify and update the samesite settings of the UIM WASP:

On the UIM robot:

1. Deactivate the wasp probe.
2. In the `nimsoft/probes/service/wasp/conf/context.xml`, check for the `sameSiteCookies` parameter.
3. Update it to `<CookieProcessor class="org.apache.tomcat.util.http.Rfc6265CookieProcessor" sameSiteCookies="Lax" />`.
4. If it is not found, add the `sameSiteCookies` parameter with the above value.
5. Activate the wasp probe.

## Troubleshooting Alarm Console

### Contents

#### Alarm Console Loses Filters with Internet Explorer

If you launch the Alarm Console view from a dashboard in Internet Explorer and later reload the page, the Alarm Console loses its filter state and it shows all alarms.

#### No Data Displayed in Alarm Console (MySQL and Oracle)

##### Symptom:

When I log in to UMP as an administrative user, the Alarm Console view does not display any data.

##### Solution:

This situation can occur in large environments with approximately 4000 or more robots, where MySQL or Oracle is the database provider.

You may be able to fix this issue by editing the following parameters in the `<setup>` sections of the `wasp.cfg` and `dashboard_engine.cfg` files:

- In the `wasp.cfg`, increase `nimpool_timeout` from 30 to 90.
- In the `dashboard_engine.cfg`, increase `dyanamic_views` from 60 to 120.

#### \$PASSWORD Substitution in Alarm Console

To use \$PASSWORD substitution in Alarm Console, you must enable it by adding a key to the `wasp.cfg` file.

##### Follow these steps:

1. Locate the `wasp.cfg` file in the following directory:  
`<UMP_installation>\probes\service\wasp\conf`
2. Open `wasp.cfg` in a text editor.
3. In the `webapps/alarmconsole` section, add the following line:  
`enable_password_arg = true`
4. Save and close the `wasp.cfg` file.
5. Restart `wasp`.

## Troubleshooting Dashboards

### Contents

### **Group Details CABI Dashboard View Not Working in UIM 20.3.3**

**Symptom:** In the Dashboard view, when I try to access any group in the Top Groups by Alarm section for the IM Overview CABI dashboard, the OC displays the Group list view instead of the Group details CABI Dashboard view.

**Solution:** To fix this issue, follow these steps:

1. Open the OC wasp.cfg file.
2. Locate the following entries under the `route_dashboard_mapping` section:
  - `path = /public/ca/uim/dashboards/common/container_group_summary`
  - `path = /public/ca/uim/dashboards/common/group_summary`
3. For the above `path` entries, update the `route` parameter value as follows:
  - Replace `route = /groups/0/[groupId]/list` with `route = /groups/0/[groupId]/cabi`
4. Save your changes.
5. Restart wasp.

### **Dashboard 301 Errors When Assigning Metric Data Sources to Gauge Widgets in Solaris**

#### **Symptom:**

You might encounter the following 301 error while a dashboard is retrieving metric data:

```
An error occurred. Message: HTTP 301 Moved Permanently
```

#### **Solution:**

Update the hosts file on the UMP server as follows:

```
127.0.0.1 localhost
```

The path for the hosts file is located in one of the following places:

- `/etc/inet/hosts` or `/etc/hosts` on linux
- `c:\Windows\System32\Drivers\etc\hosts` on Windows

### **Dashboard Queries Time Out During Data Retrieval**

#### **Symptom:**

When dashboards are set to **Live view** mode, widgets can return less data than expected. An error message can appear in the tooltip at runtime:

```
"SQL request timed out after 100 ms."
```

- – "SQL" is the type of data source.
- "100 ms" reflects the value at which the timeout is configured at the time the query is run.

This error occurs when the timeout period is reached before the data request (SQL, probe, dashboard, or other) has finished retrieving data.

#### **Solution:**

Timeout values for data queries can be set to ensure that all data is returned.

The **dataSession** value is set at installation to determine the maximum amount of time for data retrieval for all data sources. The default value is 10000 ms.

The **dataSource** key, which applies to all data source types, can be added. If a value is not specified, the value defaults to 9500 ms.

Other timeout key values also can be set to determine the maximum amount of time for data retrieval for individual data source types:

- **alarmsDS**
- **metricDS**
- **listDS**
- **probeDS**
- **qosDS**
- **slaDS**
- **sqlDS**
- **dashboardDS**

The `dataSource` key sets the maximum data retrieval run time. If a data source type timeout is not set, the value for `dataSource` is used. If the individual data source type value is set higher than the `dataSource` value, the `dataSource` value is likewise used.

All of these timeout values can be set in the **dashboard** web application run under the **wasp** probe, a container for web applications.

**Complete these steps to update the timeout key value or enter other key values:**

1. Locate the **wasp** probe in the probe directory.
2. Select the **Raw Configure** option for the probe.
3. Open the **webapps** folder and locate the **dashboard** web application.
4. Locate the timeouts settings and enter or edit the key values as needed.

## Troubleshooting Infrastructure Manager

### Contents

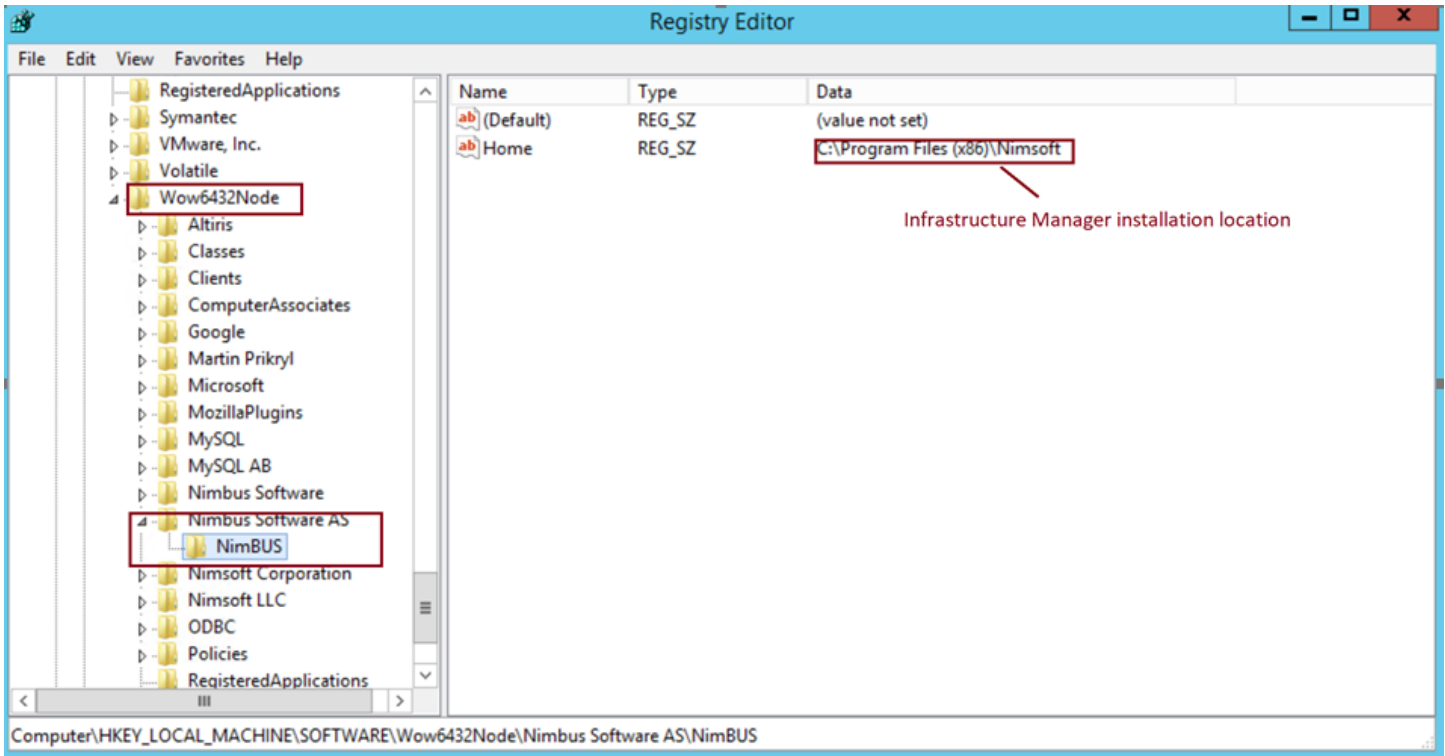
View Log Option is Disabled

**Symptom:** After upgrading from CA UIM 9.0.2 to CA UIM 9.2.0, I find that the **View Log** button is disabled in the **General** tab of the hub configuration UI. Therefore, I am unable to view the hub logs from the IM UI.

**Solution:** This issue is specific to the IM installation. IM tries to find the installation Home directory from the registry `HKLM\SOFTWARE\Nimbus Software AS\NimBUS`. If this is not available, the **View Log** button is disabled in IM, because it cannot find the `LogViewer.exe` file. To resolve this issue, you can follow these steps:

1. Open the Registry Editor (`regedit`) on your Windows computer by using the Windows "run" command utility (`windows + R`).
2. Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node` location in the registry.
3. Create a new key `Nimbus Software AS`.
4. Create the `NimBUS` key under `Nimbus Software AS`.
5. Create the new **String Value** with name as `Home` and the data as `<Infrastructure Manager installation path>` under the `NimBUS` key. The following screenshot shows the information:





Alternatively, you can also use the following method, if required:

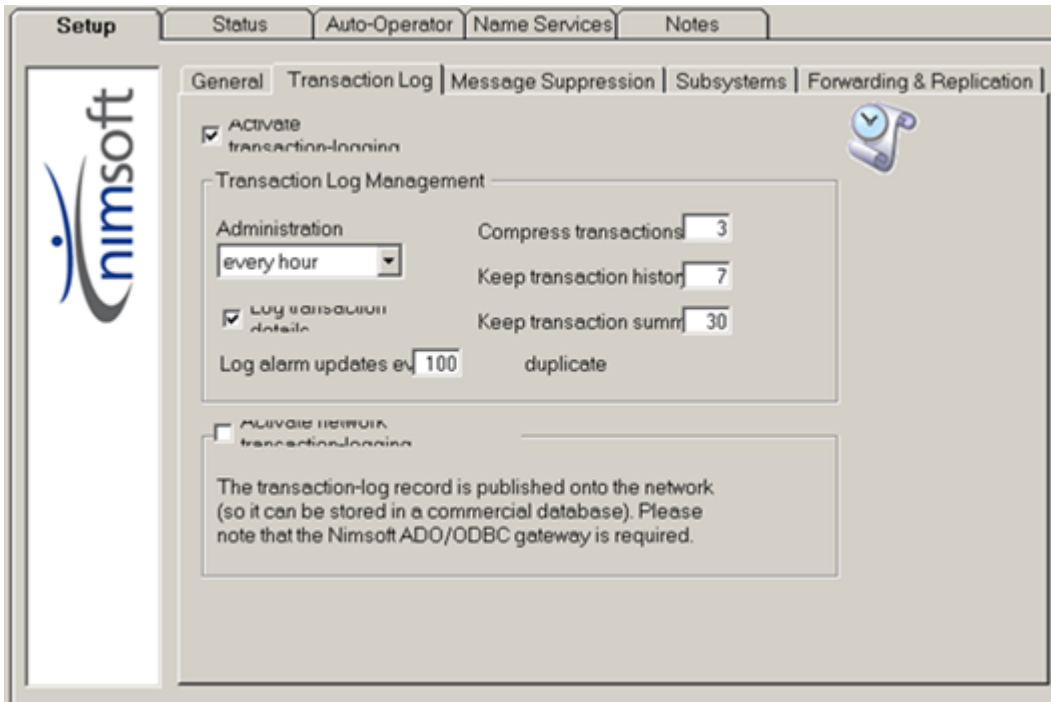
1. Create a new file with the .reg extension, open it in any editing application (for example, Notepad), and paste the following content:
 

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Nimbus Software AS]
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Nimbus Software AS\NimBUS]
"Home"="C:\\Program Files (x86)\\Nimsoft"
```
2. Save the file.
3. Double-click the file to install it. This will create the required keys.

### **Probe GUI Configuration Font Size Issue**

#### **Symptom:**

On Windows 7 systems, the font in some probe configuration GUIs is too large. The following images show the larger text (top image) as compared to normally sized text (bottom image).



**Solution:**

Windows 7 sets the screen resolution to the native resolution of your monitor. If your screen is over a certain resolution, Windows 7 sets the default font size to 120 DPI (dots per inch). This font size is approximately 125 percent of the normal 96 DPI (100 percent). When the system defaults to 125 percent DPI, it also increases the size of all bitmap fonts. Setting the DPI back to 100 percent resizes TrueType fonts, but bitmap fonts remain at the larger size. As a result, larger text appears in some of the probe configuration GUIs.

**NOTE**

This problem does not occur if Windows 7 defaults to 96 DPI (100 percent) when it is first installed.

To resolve this issue, you configure Windows to use the proper font sizes for the bitmap fonts. You can use two methods to configure Windows:

**Change the DPI Settings in Windows 7**

This method is the least technical solution. However, it may produce larger Windows and Icons.

**Complete these steps:**

1. Open the Control Panel.
2. Click **Appearance and Personalization**.
3. Under **Display**, click **Make text and other items larger or smaller**.
4. Select **125%**.
5. Click **Apply**.

**Edit values in the Windows Registry****WARNING**

This method may be technically challenging to some users. Administrator privileges are required to edit registry values.

**Complete these steps:**

1. Open the registry editor by typing "Regedit" in the search control of the Windows Start menu.
2. Browse to "**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts**"
3. Locate **MS Sans Serif 8,10,12,14,18,24**, and change the value from "SSERIFF.FON" to "SSERIFE.FON".

**NOTE**

The last character in this and all other steps is changed from 'F' to 'E'.

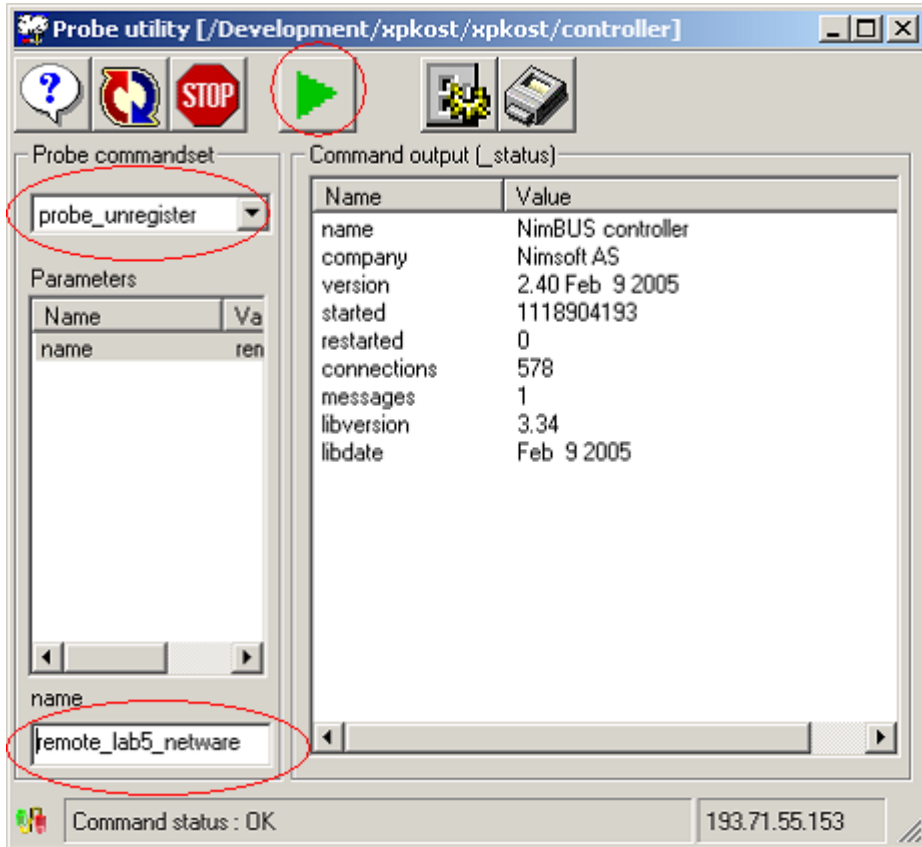
4. Locate **MS Serif 8,10,12,14,18,24**, and change the value from "SERIFF.FON" to "SERIFE.FON".
5. Locate **Courier 10,12,15**, and change the value from "COURF.FON", to "COURE.FON".
6. Reboot Windows, or log out and log in again.

**Unable to Remove Netware Robots from List****Symptom:**

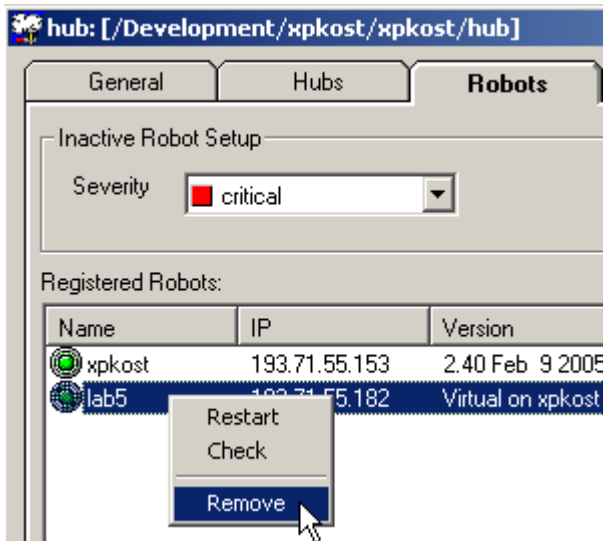
After uninstalling netware robots, several netware robots may still appear on the robot list (found under the robot tab in hub configuration tool), even if the NLMs are uninstalled and the proxy is deleted. If you attempt to manually remove them from the robot list in hub configuration tool, they may reappear after a few seconds.

**Solution:**

1. Start the probe utility on the controller-probe on the robot where the proxy-probe is running by selecting the controller probe in Infrastructure Manager and clicking Ctrl+P.
2. Select: 'probe\_unregister' from the probe commandset drop-down list and enter the name of the machine:  
*remote\_<name of the machine>\_netware*
3. Click the green arrow, as shown in the following image:



4. Remove the robot from the robot list in the hub configuration tool, as shown in the following image:



### The Infrastructure Manager Error Log

During the installation of the Infrastructure Manager, the log file *Nimsoft\_manager.log* is created in the following directory:

*Program Files/Nimsoft/AC/logs*

Events, trace, and error information are written to this log.

When the size of the file exceeds approximately 100 KB, a backup of the file is automatically created. The name of the backup file is `_Nimsoft_manager.log`.

When the backup file is created, the log file `Nimsoft_manager.log` is cleared and starts logging again. The next time the log file is full, the backup file is overwritten.

## **How to Find Hub Version in IM**

### **Symptom:**

I want to know the version of hub in my CA UIM environment. How can I do so in IM?

### **Solution:**

To check the version number of a hub, follow these steps:

1. Right-click the hub probe.
2. From the pull-down menu, select Update Version.
3. A dialog box appears with the current version; hit Cancel unless you wish to update.

## **Unable to Open Probes**

### **Symptom:**

I have been able to log in to Infrastructure Manager I have configured. However, when I try to open a probe (for example, controller, `net_connect`), I get the following error:

```
Cannot create CNimPackageEditor (1) .
```

### **Solution:**

To resolve this issue, follow these steps:

#### **NOTE**

The Microsoft Visual C++ 2008 Redistributable package (`vcredist_x86.exe` and `vcredist_x64.exe`) is required. Download it from [support.nimsoft.com](http://support.nimsoft.com).

1. Uninstall Infrastructure Manager.
2. Delete the Nimsoft folder.
3. Restart your computer.
4. Log in with local administrator rights.
5. Download the IM installer from [support.nimsoft.com](http://support.nimsoft.com).
6. Disable any anti-virus.
7. Right-click and run as administrator to install it.

## **Troubleshooting Operator Console**

#### **NOTE**

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

## **Operator Console (OC) Installing on Primary Hub Instead of UMP Server**

### **Symptom:**

I am upgrading my 8.51, 9.02 , 9.2, or 20.1 environment to 20.3, and the Operator Console (OC) installer is trying to install the OC on the primary hub instead of the UMP server. How can I resolve this issue?

### **Solution:**

The Operator Console searches for the wasp probe and then looks for a file. If it finds the file on the primary hub, the OC is installed on the primary hub. And, you cannot change the installation destination to the UMP server.

If the OC installer tries to deploy the OC on your primary hub, cancel the upgrade and do the following.

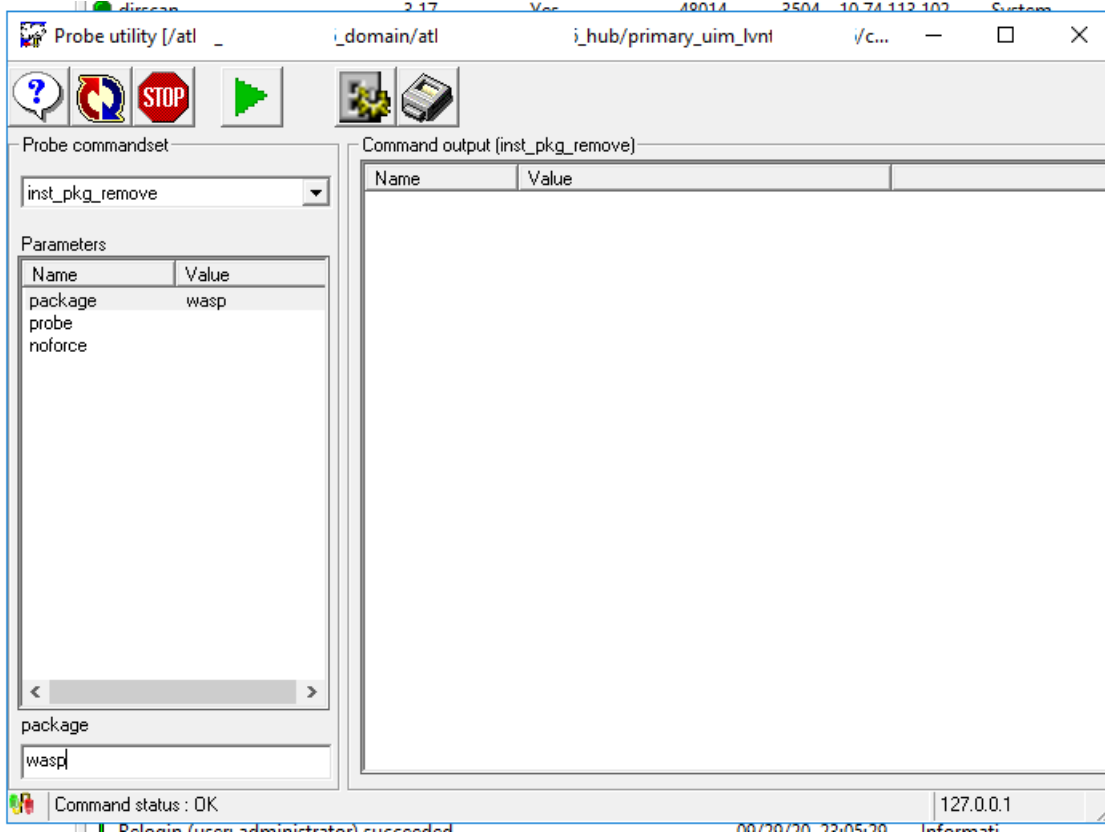
### **NOTE**

This process also works if you have already installed the OC on the primary hub.

1. Take a backup of the wasp.cfg file that is available on the primary hub.
2. Run the wasp uninstaller.
3. In the installed packages list of the controller, check if any UMP/OC-related packages exist. (See step 4 for the list of packages that should be removed.)
  - a. If packages exist, go to Step 4 and uninstall the packages using the probe utility.
  - b. Otherwise, go to Step 11 and delete the wasp folder.
4. From IM, click the primary robot controller probe to highlight it (do not open the UI).

| Probe           | Version | Active | Port  | PID   | IP Address | Group         | Robot Address         | Class      | Description        |
|-----------------|---------|--------|-------|-------|------------|---------------|-----------------------|------------|--------------------|
| cm_data_import  | 20.30   | Yes    | 48024 | 11216 | 10.0.0.1   | Service       | /atlas_lvntest0038... | Probe/P... | CM Data Impo...    |
| controller      | 9.31S   | Yes    | 48000 | 10532 | 10.0.0.1   | Infrastruc... | /atlas_lvntest0038... | Probe/P... | Robot process ...  |
| data_engine     | 20.30   | Yes    | 48021 | 4580  | 10.0.0.1   | SLM           | /atlas_lvntest0038... | Probe/P... | Manages Quali...   |
| dirscan         | 3.17    | Yes    | 48014 | 3504  | 10.0.0.1   | System        | /atlas_lvntest0038... | Probe/P... | File and direct... |
| discovery_agent | 20.30   | Yes    | 48023 | 3376  | 10.0.0.1   | Service       | /atlas_lvntest0038... | Probe/P... | Discovery Agent    |

5. Press Ctrl-p to open the probe utility.
6. Use the inst\_pkg\_remove callback of the controller probe to remove the UMP/OC packages. That is, inst\_pkg\_remove wasp. Find the inst\_pkg\_remove package from the drop-down list.
7. In the package section, enter the package you want to delete.

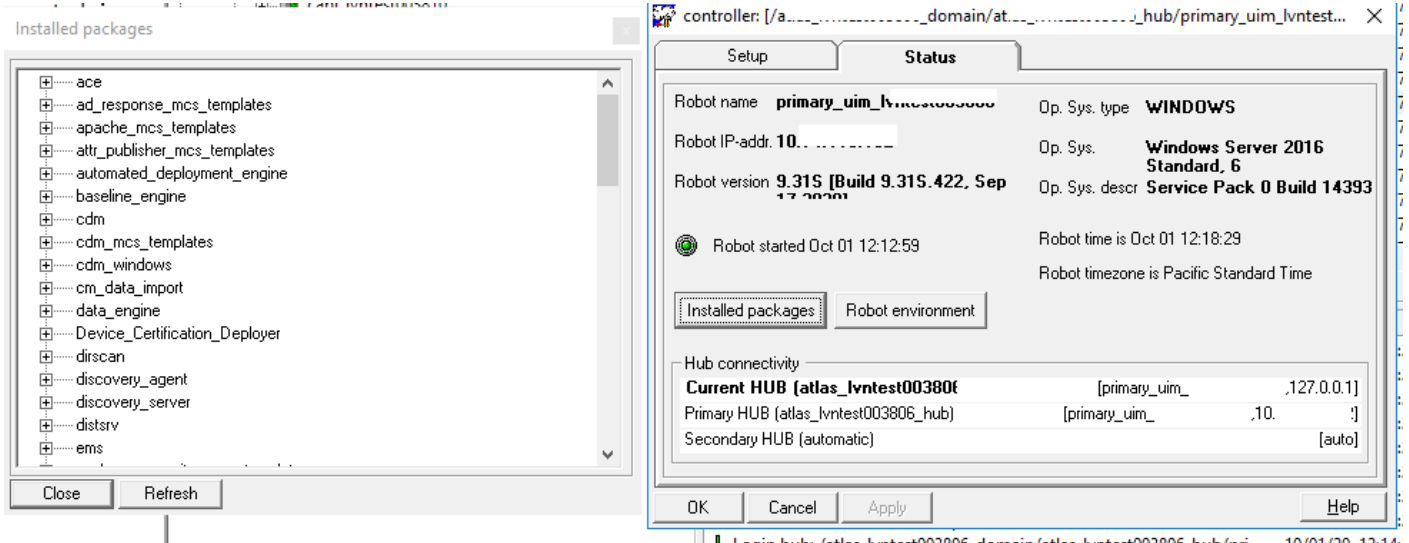


8. Use the probe utility to remove the following probes:

- wasp\_service\_wrapper
- nisapi\_wasp
- ump
- ump\_operatorconsole
- wasp\_alarmviewer\_api
- policy-management-ws
- mcs-ui-app-portlet
- ump\_cabi
- ump\_accountadmin
- ump\_dashboard
- adminconsoleapp
- uimhome
- uimesdplatelemetry
- mps
- wasp

9. If you get an error when you click the run button (play icon), deploy the probe again on the primary hub and then run the `inst_pkg_remove` package.

10. Verify that you have removed the apps by opening the controller UI and accessing the Status tab, Installed packages.



11. Remove the wasp folder from the filesystem.
12. Deploy the wasp, adminconsoleapp, uimhome, and uimesdplatelemetry packages on the primary hub again.
13. If the previous wasp.cfg file has to be reused, then clear the UMP/OC webapps from the webapps section of the .cfg file and replace it.
14. Activate the wasp probe.
15. Run the OC installer again. It should find your UMP server. In the following screenshot, the setup has two UMP servers and the installer selected the secondary UMP server. Allow the installer to run there.



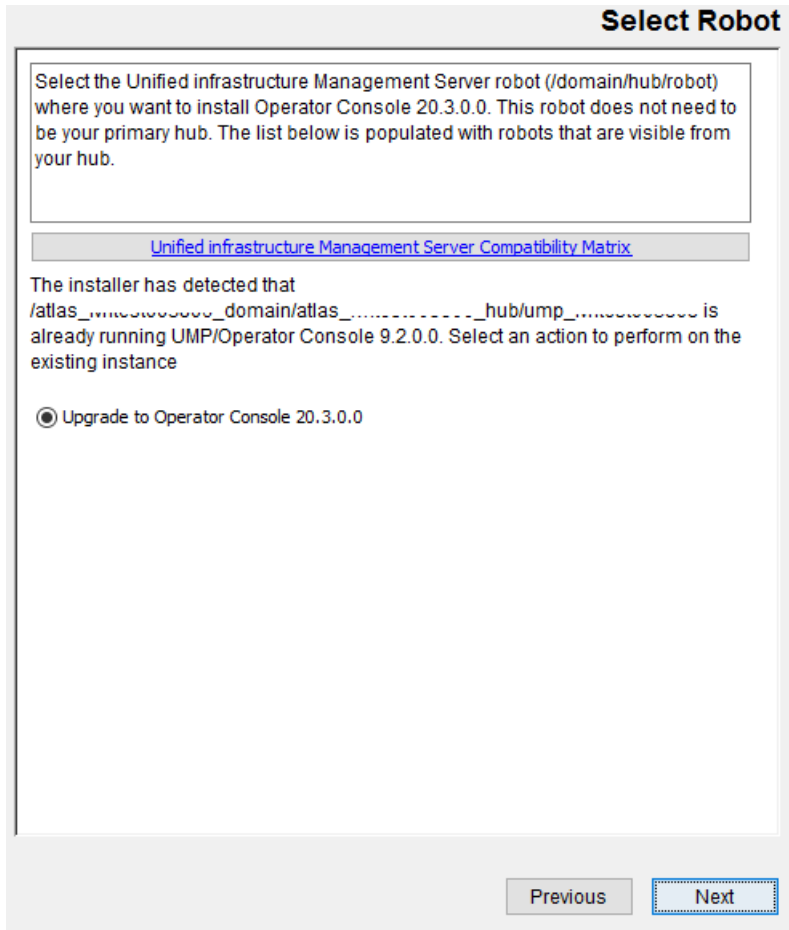
Select the Unified infrastructure Management Server robot (/domain/hub/robot) where you want to install Operator Console 20.3.0.0. This robot does not need to be your primary hub. The list below is populated with robots that are visible from your hub.

[Unified infrastructure Management Server Compatibility Matrix](#)

The installer has detected that /atlas\_ i\_domain/atlas\_.....\_hub/ump2\_!..... is already running UMP/Operator Console 9.2.0.0. Select an action to perform on the existing instance

Upgrade to Operator Console 20.3.0.0

16. After the OC installation on the secondary UMP completes, deactivate the robot on the now secondary OC.
17. Run the OC installer again to upgrade the primary UMP.



18. Activate the secondary OC robot.
19. Verify that the deployment is working on both the servers.

### **CABI Dashboard Not Displaying in OC**

#### **Symptom:**

CABI dashboards are not displaying in OC for all users with all browser types. The System component missing error message is displaying in the OC UI. The wasp.log from OC is as follows:

```
DEBUG [https-jsse-nio-443-exec-7, com.firehunter.ump.utils.ProbeAddress]
Unable to get port_list for robot : null ERROR [https-jsse-nio-443-exec-7,
com.ca.cabi4uim.controllers.CABIController] Unable to initialize cabi probe client: Unable
to communicate with any of the possible cabi probes: cabi,cabi_external
```

The environment details are as follows:

- UIM 20.3 with ump\_operatorconsole v2.06 and CABI v4.30 are on separate robots.
- HTTPS is enabled on both OC and CABI.
- UIM CABI dashboards are working fine with a direct logon to CABIJS.

#### **Solution:**

These steps might help you resolve the issue:

- Download robot\_update\_9.32.zip from [CA Unified Infrastructure Management Hotfix Index](#) and import to the UIM archive.
- On the CABI robot, deploy robot\_update\_9.32.
- On the OC robot, follow these steps:
  - Deactivate the wasp probe.
  - Rename..\Nimsoft\probes\service\wasp\webapps\cabi.
  - Rename..\Nimsoft\probes\service\wasp\work.
  - Deploy robot\_update\_9.32.
  - Deploy ump\_cabi 4.22 and validate that the date modified for ...\\Nimsoft\probes\service\wasp\webapps\cabi.war is updated.
  - Activate the wasp probe.

### **OC Home page Not Loading**

#### **Symptom:**

When I log in to OC 20.3, the OC Home page does not load.

#### **Solution:**

Do not close the page or click any other option. Wait for the OC Home page to load completely; it will load after some time.

### **OC Redirecting to CABI Login Page**

#### **Symptom:**

The OC Home page was not loading when I logged in to OC 20.3. And, when I clicked the Reports option in the left pane, I was redirected to the CABI login page.

#### **Solution:**

Allow the OC Home page to load completely before selecting any other option. OC and CABI are different/separate web applications. For JasperServer to create a session for CABI, the process of loading the Home page allows that to happen. If you select the Reports option before the OC Home page loads, you are *unexpectedly* redirected to the CABI login page. After the Home page is loaded, the session is cached and the redirect to the CABI login page no longer occurs. If the OC session is idle for 15-20 minutes, the CABI session may timeout. In that case, select the Home page and let it load once again.

### **OC Trying to Install on CABI Server**

#### **Symptom:**

In my environment, while upgrading to 20.3.1, the OC installation was trying to install OC on the CABI server. It would not try to install on UMP (not even on primary hub as documented above). During installation, the drop-down was not listing any server where I could install OC. It was not giving me any choice; for example, it was not allowing to install on the UMP server. It was only trying to install on the CABI server.

#### **Solution:**

As a workaround, you can follow these steps:

- Before starting the OC installation, shut down the CABI robot.
- Start the OC installation. The drop-down list now lets you select the UMP server where you can install OC.

### **SLM Groups, Accounts, SLAs Not Visible in OC**

#### **Symptom:**

After upgrading to 20.3.x, I do not see SLM groups, Accounts, or SLAs in OC. I have multiple SLAs and multiple accounts, and they are in the database.

#### Solution:

If there is an SLA alarm with `warning_severity = null`, this issue may occur. This would generate an error that prevents the browser to retrieve the SLM list (in OC) with the accounts and groups. As a workaround, follow these steps:

1. Run the following query on the database:

```
select sla_id from S_SLA_ALARM where warning_severity is null
```

2. Copy the `sla_id` and run the following update query:

```
update S_SLA_ALARM set warning_severity =0 where sla_id =<from the first query>
```

#### NOTE

Repeat the operation for all the `warning_severity` having null value and replace with a 0.

3. Log off and log in again.

The issue should be resolved.

### Data Access Error in Operator Console

#### Symptom:

When I access Operator Console in UIM 20.3.2, I see Data Access Error. UIM 20.3.2 and CABI are configured correctly. Also, when loading the Home page, I see no CABI content (Data Access Error) and noticed 404 errors in the network tab.

#### Solution:

This is a content issue. The data access error is occurring because CABI is missing dashboards. Deploy or redeploy the following packages on the CABI robot:

- `uim_core_dashboard`
- `uim_unified_reporter`

### Auditing Operator Console Logins

#### Symptom:

I upgraded to UIM 20.3.2. I want to monitor external user sign-ins to the portal. Is there a way to collect audit logs from Operator Console that shows sign-ins with timestamps of Account Users and Bus users? Also is there a quick way to see last logon date of account users?

#### Solution:

In 20.3.x, the `User_` table is now the `CM_User_` table. It works the same way. The entries in this table are created each time any user (nimbus user or account user) logs into OC for the first time. However, the `loginDate` and `lastLoginDate` fields are not attributes in the new table. The alternative is monitoring the `wasp.log` with `logmon` for the OC logins as described in the [KB Article](#). Although the KB still references UMP, the `wasp.log` logs the logging attempts.

Examples:

- Administrator logs into OC

`wasp.log`

```
Dec 23 12:36:13:261 DEBUG [http-nio-80-exec-17, com.fr.ump.auth.NmsAuth] Login from request user
{userId=10159, screenName=administrator, emailAddress=administrator@my.nimsoft.com, locale=en_US,
firstName=administrator, middleName=null, lastName=}
```

```
Dec 23 12:36:13:403 DEBUG [http-nio-80-exec-17, com.fr.ump.auth.NmsAuth] User prin
```

```
com.nimsoft.nimbus.probe.service.wasp.auth.NimbusUserPrincipal@2cf24917(administrator) found for 10159
```

- Account user logs in: (**ipxxxxx**)

`wasp.log`

```

Dec 23 12:45:47:211 DEBUG [http-nio-80-exec-12,
 com.nimsoft.nimbus.probe.service.wasp.db.DbPreparedStatement] Query pNJt took: 0.001s
Dec 23 12:45:47:211 DEBUG [http-nio-80-exec-12, com.nimsoft.nimbus.probe.service.wasp.auth.LoginModule]
 ippma03 logged in.
Dec 23 12:45:47:211 DEBUG [http-nio-80-exec-12, com.firehunter.ump.auth.NmsAuth] User: ipxxxxxx, NimBUS
 login milliseconds: 129
Dec 23 12:45:47:215 DEBUG [http-nio-80-exec-12, com.firehunter.ump.auth.NmsAuth] Login from request
 user {userId=10161, screenName=ipxxxxxx, emailAddress=deddkj@rimc.com, locale=en_US, firstName=dicjiod,
 middleName=null, lastName=dsmopc}

```

## Troubleshooting SiteMinder Configuration

If you are experiencing issues with the SiteMinder configuration, check these log files and tools.

| Log File and Tool             | Location             | Path                                                          | Description and Troubleshooting Tips                                                                                                                                                                                                                  |
|-------------------------------|----------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hub.log                       | NMS system           | C:\Program Files (x86)\Nimsoft\hub\hub.log                    | Helps show user and group import into the hub. Adjust the log level in the hub configuration.                                                                                                                                                         |
| portal.log                    | UMP system           | C:\Program Files (x86)\Nimsoft\probes\service\wasp\portal.log | Helps show LDAP activity.                                                                                                                                                                                                                             |
| Web Agent trace log           | SPS system           | The location is defined in ACO.                               | Helps show user authentication activity on the SPS. Debugging is enabled in the proxy rules specification. Helps show the HTTP response that is generated after authentication. Ensure your SPS WebAgent has the TraceConfigFile parameter configured |
| Policy Server Trace Log       | Policy Server system | C:\Program Files (x86)\CA\siteminder\log\smtracedefault.log   | Defined under the Profiler tab in the Policy Server Management Console.                                                                                                                                                                               |
| SiteMinder Test (smtest) tool | Policy Server system | Not Applicable.                                               | Useful for testing policy changes, particularly protection, authentication, and authorization. Displays HTTP-header response information.                                                                                                             |

## Troubleshooting Discovery and the Discovery Wizard

### Contents

#### I Cannot Save My Information

##### Symptom:

I cannot save my authentication profile or range.

##### Solution:

All required fields must have valid entries to save an authentication profile or range. Required fields are outlined in red.

### **I See Messages About Exclude Scopes (Ranges)**

#### **Symptom:**

When I launch the Discovery Wizard, I see the following message:

*Exclude scopes (ranges) are no longer supported. Would you like to remove them?*

#### **Solution:**

This behavior happens because ranges of IP addresses to be excluded from discovery were previously configured for your discovery agent. The Discovery Wizard does not support exclude ranges and cannot proceed until the exclude ranges are deleted. You can either accept the prompt to delete your exclude ranges, or exit the Discovery Wizard and manually delete them from the CA UIM database.

### **Slow Restart of discovery\_server on MySQL**

#### **Symptom:**

When `discovery_server` starts, it executes a script to check and create tables in the database. A bug in MySQL 5.5 causes this script to run slowly. For more information, search the [MySQL Documentation Site](#) for *Changes in MySQL 5.6.13 (2013-07-31)* and *MySQL Bug: Create Table If Not Exists*.

#### **Solution:**

Upgrade MySQL to version 5.6.13 or later.

### **WMI and SSH Discovery Provide More Detailed Host System Information Than SNMP**

#### **Symptom:**

For network devices such as routers and switches, SNMP is the only source for detailed discovery information. For host systems (such as Windows, Unix, or Linux servers) we recommend that you use WMI or SSH discovery in addition to SNMP. While SNMP provides the most complete network interface information for devices and systems, the host system information available from SNMP (for example, processor attributes) is less complete than the information from WMI or SSH discovery. Specifically:

- The **ProcessorDescription** attribute might not provide a meaningful value. Windows and Linux systems should provide meaningful values for this attribute, but Solaris systems might provide a generic value.
- The **ProcessorSpeedInGhz**, **NumberOfPhysicalProcessors**, **NumberOfProcessorCores**, and **NumberOfLogicalProcessors** attributes are not available from SNMP.
- The **MemoryInGB** attribute is set only for devices that implement the HOST-RESOURCES-MIB.
- The **Model** attribute is not set for host systems. This attribute is provided by the ENTITY-MIB, which is typically not implemented by host systems.
- The hardware vendors for Windows and Linux systems are Microsoft and NetSNMP respectively.

#### **Solution:**

Enable the combination of WMI or SSH discovery and SNMP discovery for host systems. This solution provides the most comprehensive set of host and network interface information.

## **Troubleshooting the Service Desk Adapter**

If you have concerns about the correct configuration of the Service Desk Adapter for the CMDB Gateway probe, verify the following:

- Examine the cmdbgwtw log, located in probes/gateway/cmdbgwtw. If the log shows zero (0) entities exported, the Service Desk adapter is not receiving data. Use the CMDB Gateway probe configuration interface to make the necessary changes to export data.
- After the first export, the probes/gateway/cmdbgwtw/sdsync directory contains a file named cmdblImport.log. This log file contains the final output of the last run, which may provide information and may help to troubleshoot configuration issues.
- Examine the probes/gateway/cmdbgwtwCIBulkImportUtility0.log log file. This log file contains complete details of the last run, which may help to troubleshoot issues.

**NOTE**

If the command line program fails, the CMDB Gateway probe does not change the Change Marker. The next export detects any changes that occurred after the last successful run.

## Troubleshooting Alarm Views

The Operator Console (OC) is designed to handle tens of thousands of alarms; returning metrics, severities, historic, and active alarms. However, large numbers of alarms can overwhelm the capacity of OC to return information on a timely basis. Java heap errors, for example, can indicate insufficient memory allocation to handle large numbers of alarms. One or more of the following actions may resolve alarm view performance issues.

- **Increase memory allocated to OC or wasp.**

The topic [Prepare Your Server Hardware](#) contains recommended OC memory allocations for small, medium, and large systems. Increase available memory if your system has grown in complexity to manage increased numbers of alarms. You can also increase the memory available to the wasp probe.

**NOTE**

Adding memory to the application may not overcome memory limitations in other, third-party software that loads and displays alarms in OC.

**Follow these steps:**

- Open the configuration interface for wasp.
  - Under **Java Startup Parameters**, increase the settings for Initial Memory and Maximum Memory.
- **Reduce the retention period for alarms in ems and nas probes to delete historic alarms that are no longer needed.** By default, transaction history for the ems probe is stored for 30 days. You can change the retention settings so that the ems .csv files are purged on a more or less frequent basis.

**Follow these steps:**

- In Admin Console, navigate to the ems node and select the Configure option.
- Change the **Transaction Log Retention (Days)** to the desired number of days.

For more information about configuring the ems probe, see the [ems](#) probe documentation on the Probes Documentation Space. The nas probe contains settings for transaction log management, including transaction history. These can be changed to limit retention of alarm history.

**Follow these steps:**

- In Infrastructure Manager, navigate to the top-level nas node and select the Configure option.
  - Under the Setup tab, select the Transaction Log tab and change the settings for **Keep transaction history**.
- For more information about configuring the nas probe, see the [nas](#) probe documentation on the Probes Documentation Space.
- Read any knowledge-base articles that address your system issue at the [CA Support site](#).

## Troubleshooting UIM Server Installation or Upgrade

**Contents:**

## **Unable to Extract the UIM ISO Images**

### **Symptom:**

When I try to unzip or extract the UIM ISO image files, I am unable to do so. I receive the following error:  
The following file already exists

### **Solution:**

The WinZip or WinRAR application is unable to extract the large files and it tries to split them, which causes the above-mentioned error. Therefore, as a workaround, you can use the 7-Zip application to extract the UIM ISO image files. For additional information, see the related [KB Article](#).

## **Getting Error While Opening Dashboard Designer**

### **Symptom:**

I have upgraded from 20.1 to 20.3.2. When I try to open the Dashboard Designer, I receive a message `Not able to get the current user or the roles associated with the user`. I tried a wasp restart, but the problem still remains. This issue is occurring for all the users.

### **Solution:**

UIM 20.3.2 is a patch release, not a major version. The prerequisite for installing 20.3.2 is to have 20.3.0 or 20.3.1. If you have upgraded directly from UIM 20.1 to 20.3.2, you will need to restore the UIM from a backup or uninstall OC and redeploy it from scratch with a supported version.

## **Access Denied for Root User on Linux with MySQL**

### **Symptom:**

When attempting to install UIM Server with a MySQL database, you might see the following error (or its equivalent) after you enter the database server information:

```
ERROR 1045 (28000): Access denied for user 'root'@'<your Nimsoft hostname>' (using
password: YES)
```

This issue occurs either because remote privileges have not been established, or because the password that is identified for remote systems is not consistent with what is set on the database server locally.

### **Solution:**

#### **Follow these steps:**

1. Log in to the MySQL database locally (on the actual server hosting MySQL).
2. To set up access from:

- Any host, execute:

```
mysql> use mysql;
mysql> UPDATE user SET password=PASSWORD("<your password>") where User = 'root';
mysql> GRANT ALL PRIVILEGES ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql> GRANT TRIGGER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql> GRANT SUPER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql> FLUSH PRIVILEGES;
```

- A particular host, execute these commands, replacing HostX with the name of your host:

```
mysql> use mysql;
mysql> UPDATE user SET password=PASSWORD("<your password>") where User = 'root' AND Host = 'HostX';
mysql> GRANT ALL PRIVILEGES ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql> GRANT TRIGGER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
```



```
mysql> GRANT SUPER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql> FLUSH PRIVILEGES;
```

### **Invalid IP Error When Installing a Windows Robot, Hub, and Distribution Server**

When installing a Windows robot, hub, and distribution server, you might see an Invalid IP Error. This error is harmless and can safely be ignored. Click **OK** and continue.

### **Login Error When Using Windows Authentication with Microsoft SQL Server**

#### **Symptom:**

In deployments that use Microsoft SQL Server with Windows authentication, you might see this error when you attempt to log in to Admin Console:

*Unable to Sign In. Check the user name and password you entered are correct and try signing in again.*

#### **Cause:**

This error occurs when the service\_host probe cannot find the path to the SQL Server JDBC driver (sqljdbc\_auth.dll). The log file (C:\Program Files (x86)\Nimsoft\probes\service\service\_host\service\_host.log), has entries that contain the following:

```
WARNING: Failed to load the sqljdbc_auth.dll
SEVERE: Login Error 2: Cannot create PoolableConnectionFactory. (This driver is not
configured for integrated authentication.)
```

#### **Solution:**

Add the path to the SQL Server JDBC driver to the service\_host configuration.

1. Open the service\_host Raw Configure utility:
  - *Admin Console:* Click the service\_host drop-down list and select **Raw Configure**.
  - *Infrastructure Manager:* Right-click the service\_host probe and select **Configure**.
2. In the utility, click the **setup** folder, select the **CATALINA\_OPTS** key, then click **Edit Key**.
3. Append the following to the key value (ensure that you leave a blank space between command line options):
 

```
-Djava.library.path="..../..../lib"
```
4. Click **OK** to save the new key value, then click **OK** to save the configuration. The service\_host probe automatically deactivates, then activates and applies the new configuration.

### **Ruby Scripts for QoS Enrichment No Longer Work After Upgrading**

#### **Symptom:**

- After upgrading to CA UIM 8.4 or later, my Ruby scripts for QoS enrichment no longer work.
- I see the following error message in the qos\_processor log file:

```
Failed to invoke monitor modifier 'enrichment': org.jruby.embed.EvalFailedException: (LoadError) no such
file to load -- scripts/rest_client
```

#### **Solution:**

The qos\_processor was updated to use JRuby 1.7.22. If you are using the **require** method to load files, do one of the following:

- Supply the absolute path to the file.
- Use the **require\_relative** method instead.

For more information, see the [JRuby documentation](#).

## **Pluggable Database Not Open Error During UIM Server Installation**

### **Symptom:**

I am trying to install UIM Server. On the **Database Configuration** dialog, when I try to connect to the Oracle database, I receive the following error:

```
java.sql.SQLException: ORA-01219: database or pluggable database not open: queries allowed on fixed tables or views only
```

### **Solution:**

After you install the Oracle database, by default, all the pluggable databases are in the closed state. CA UIM displays the above-mentioned error if the pluggable database is not open. To open the pluggable database, connect to the Oracle database with the `sys` user and run the following command:

```
SQL> ALTER PLUGGABLE DATABASE ALL OPEN;
```

## **Oracle Database Already Exists Error During UIM Server Installation**

### **Symptom:**

I am trying to install UIM Server. On the **Database Configuration** dialog, when I try to connect to the Oracle database, I receive the following error:

```
Database named 'CA_UIM' already exists. Modify creation mode to 'Use Existing Database' or enter a different database name.
```

### **Solution:**

During the UIM Server installation, if you click the **Test** button on the **Database Configuration** dialog, Oracle creates a schema and tablespace with the specified information. If you cancel the installation for some reason, the created schema and tablespace are not deleted. Therefore, you cannot use the same name again. If you try to use the same name, you get the above-mentioned error.

You can use the following script if you want to drop the user and associated tablespace:

```
create or replace procedure drop_user(inUser varchar2) IS
 v_count INT :=0 ;
begin
 declare cursor c_user is select s.sid, s.serial#
 from v$$session s, v$$process p
 where s.username = '||upper(inUser)||'
 and p.addr (+) = s.paddr;
 r_user c_user%ROWTYPE;
 begin
 SELECT COUNT (1) INTO v_count FROM dba_users WHERE username =upper(inUser);
 dbms_output.put_line('user '||upper(inUser)||'exist '||v_count);
 IF v_count != 0
 then
 open c_user;
 loop
 fetch c_user into r_user;
 exit when c_user%NOTFOUND;
 execute IMMEDIATE 'ALTER SYSTEM KILL SESSION '||r_user.sid||','||
r_user.serial#||'''';
```

```

 end loop;
 close c_user;
 execute IMMEDIATE 'drop user ' || inUser||' cascade';
 execute immediate 'DROP TABLESPACE ' || inUser||' INCLUDING CONTENTS AND
DATAFILES';
 end if;
 end;
 end;

```

Script to call the stored procedure:

```

declare
begin
drop_user('user_name');
end;
/

```

### **Service Name Error While Installing UIM Server**

#### **Symptom:**

I am trying to install UIM Server. On the **Database Configuration** dialog, after I provide the Oracle-related information and try to verify the information, I get the following error:

```

Failed to connect to database server with provided field values. Recheck fields for
accuracy.

```

```

Listener refused the connection with the following error:
ORA-12514, TNS:listener does not currently know of service requested in connect
descriptor

```

#### **Solution:**

If the service name provided in the UIM Server installation is not correct, the above-mentioned error is displayed. To address this issue:

- Ensure that the service name is correct in the tnsnames.ora file located at \$ORACLE\_HOME/network/admin/
- Ensure that the host name is correct in the listener.ora and tnsnames.ora files located at \$ORACLE\_HOME/network/admin/

### **Listener Down Error While Installing UIM Server**

#### **Symptom:**

I am trying to install UIM Server. On the **Database Configuration** dialog, after I provide the Oracle-related information and try to verify the information, I get the following error:

```

Failed to connect to database server with provided field values. Recheck fields for
accuracy.

```

```

The Network Adapter could not establish connection

```

#### **Solution:**

CA UIM displays the above-mentioned error if the listener is down on the computer where Oracle is installed. To address this issue:

- Ensure that the listener is started.
- Ensure that the host name is correct in the listener file located at \$ORACLE\_HOME/network/admin/

To stop and start the listener, use the following commands at the command prompt:

- lsnrctl stop listener
- lsnrctl start listener
- lsnrctl status listener

### **mon\_config\_service Failed to Activate After Upgrading to CA UIM 9.0.2 with MySQL5.5**

#### **Symptom:**

I upgraded CA UIM 8.47 to CA UIM 9.0.2 using MySQL 5.5 on CentOS7. However, the mon\_config\_service probe remained inactive. How can I address this issue?

#### **Solution:**

CA UIM 8.47 supports MySQL 5.5; whereas, CA UIM 9.0.2 does not support this MySQL version. Therefore, we recommend that before you upgrade to 9.0.2, ensure that you use the correct MySQL version that 9.0.2 supports. For more information about supported database versions, see [Compatibility Matrix](#).

However, consider a scenario where you first upgrade 8.47 (with MySQL 5.5) to 9.0.2. You then upgrade the MySQL version to the version that 9.0.2 supports. In this case, you need to follow these steps to activate MCS:

1. Use the following query to view the details:  

```
select * from ssrv2schemamigration
```
2. Verify the output.  
 For the version 9.0.2.00 entry, the success status must be 0 .
3. If the status is 0 , delete the entry from the ssrv2schemamigration table where version='9.0.2.00' by using the following query.  

```
delete from ssrv2schemamigration where version='9.0.2.00'
```
4. Deactivate and activate MCS.  
 MCS is displayed with the active status.

## **Troubleshooting Additional Scenarios**

This article includes additional troubleshooting scenarios.

### **Windows Blue Screen (BSOD) During Reboot**

#### **Symptom:**

Upon rebooting a system, during or immediately after the reboot process, a Windows crash event is occurring. For example, some users were observing this issue with robot 7.97hf4.

When a robot restarts, it tries to shut down all the probes that are running. If they do not shut down within 10 seconds, the controller issues a 'kill' command based on the PID. At this time, the controller also records the PIDs of these processes, and when it restarts, it checks if these PIDs are still active. If so, it kills those processes before starting up the probes again.

Sometimes during a reboot, one or more probes can take longer to shut down and the reboot interrupts this process. Therefore, after the reboot, a new process has taken a PID that was previously owned by a probe, and the controller terminates this process. If this is a system critical process, it will cause a BSOD.

**Solution:****NOTE**

This issue is now fixed in UIM 20.3.3. Therefore, you do not perform this workaround if you are using UIM 20.3.3.

This can be worked around with some configuration settings on the robot. However, adding these settings may cause robot restarts to take longer than usual.

These keys should be added to the robot.cfg in the main <controller> section.

- use\_force\_stop = 0 to prevent the robot forcing stopping probe processes. It will loop waiting for probes to shut down naturally instead.
- stop\_existing\_processes = 0 to prevent the robot killing processes from a previous run of controller if it believes they exist.

Working in tandem, these should mitigate cases where the controller could terminate processes it does not own.

**Getalarms Giving Error for Account User with Alarm Filter ACL****Symptom:**

I am logged in as an account user with an ACL with alarm filters. Now, when I try to get alarms using webservices\_rest or uimapi, I am getting the HTTP Status 500 error. The http://rest/alarms endpoint does not retrieve any alarms (SERVER ERROR) if the ACL assigned to the user contains an alarm filter.

**Solution:**

This issue is occurring because of the missing .jar files.

1. Download the following .jar files from the [KB Article](#):
  - flex-messaging-common-4.7.1.jar
  - flex-messaging-core-4.7.1.jar
2. Stop the wasp probe.
3. Connect to the OC server and copy the .jar files to the following folders:
  - Nimsoft\_install\_Dir\probes\service\wasp\webapps\uiimapi\WEB-INF\lib
  - Nimsoft\_install\_Dir\probes\service\wasp\webapps\rest\WEB-INF\lib
4. Start the OC wasp.
5. Test whether the issue is resolved.

This issue affects both webservices\_rest and uimapi. The workaround is applicable for both of them.

**Duplicate IDs if Master Image Updated with a Working Robot****Symptom:**

I have a master image that is used to provision systems when users request them. I need to monitor them with a robot. However, if I update the master image with a working robot, I end up having duplicate development IDs. How can I resolve this issue?

**Solution:**

You can address this issue by using one of the following solutions depending on your environment:

- **Cloud Robot Installation**  
Update the master image with a Cloud robot installation. Using this method, you can monitor new systems as they are deployed. Cloud installation leaves the installed robot in a latent state. The robot starts after a configurable number of host restarts.

- You must identify the count to find the correct number for the master image so that the robot goes live on the final provisioning.
- This solution also needs to include a request.cfg file that would then activate to add the probes and configurations needed to monitor that device.
- **Robot Installation on Master Image**  
Install a robot on the master image with all the probes and configurations.
  - Set the master image for the robot to start manually and be inactive.
  - Set up a script that gets executed when the system is provisioned. This clears the niscache folder, starts the robot service, and sets it to be automatic from that point onward.

#### Considerations:

- With the robot cloud installation, all robots must report to the same hub. Currently, this cannot be set manually. You can create a script.
- With the script that starts the robot, you can update the robot.cfg file with different hub information.

#### Sample Rate for QOS\_POWER\_STATE Metric is 0

##### Symptom:

In my environment, the QoS interval for the QOS\_POWER\_STATE metric is 5 minutes. The expectation is that the sample rate in the s\_qos\_data table must be 300; whereas, it is 0.

##### Solution:

To resolve this issue, run the appropriate script in your database environment. The scripts are attached to this page and are as follows:

- [oracle\\_update\\_qos\\_type.sql](#)
- [mysql\\_update\\_qos\\_type.sql](#)
- [sqlserver\\_update\\_qos\\_type.sql](#)

(For Microsoft SQL Server) You can run the script as follows:

1. Copy and paste the content of the sqlserver\_update\_qos\_type.sql script file in the query editor you are using for updating the database.
2. Update the database name in the first line of the script with the database in which it is going to be executed.
3. Execute the script.
4. The spn\_update\_qos\_addcolumn stored procedure will be created.
5. Run the newly created stored procedure as follows:  
exec spn\_update\_qos\_addcolumn

(For Oracle and MySQL) You can run the appropriate script as follows:

1. Copy and paste the content of the mysql\_update\_qos\_type.sql script file (for MySQL) and oracle\_update\_qos\_type.sql (for Oracle) in the query editor you are using for updating the database.
2. Log in as a schema owner (for Oracle) or database owner (for MySQL).
3. Execute the script.
4. The spn\_update\_qos\_addcolumn and spn\_de\_update\_qosp stored procedures will be created on completion of the execution.
5. Validate the stored procedures before calling them.
6. Run the newly created stored procedures as follows:  
For MySQL: call spn\_de\_update\_qosp  
For Oracle: exec spn\_de\_update\_qosp

## **Unable to Download from the Web Archive on Windows 2016**

### **Symptom:**

I am unable to download distsrv 5.30 from the archive. I am getting the following error:

```
Internet Archive Error
Forbidden
Release ID: 3925
Local file:
C:\Users\ADMINI~1\AppData\Local\Temp\2\ReleaseID-3925.zip
```

### **Solution:**

This issue occurs because of a security setting in a browser. To address this issue, add `http://*.nimsoft.com` as a trusted site to your browser. For example, for Internet Explorer, follow these steps:

1. Open Internet Explorer.
2. Open the **Internet Options** dialog.
3. Click **Security, Trusted Sites, Sites**.
4. Enter `http://*.nimsoft.com` and click **Add**.
5. Click **Close** to close the dialog.
6. Click **OK**.

You can now download the items without any issue.

## **MySQL Service Stops Inadvertently After Installing CA UIM**

### **Symptom:**

After I install CA UIM, I have observed that the MySQL service has stopped inadvertently.

### **Solution:**

To address this issue, after you install MySQL, follow these steps:

1. Stop the MySQL service.
2. Specify the below configuration parameters in the `my.cnf` file:
  - `lower_case_table_names=1`
  - `local_infile=ON`
  - `table_definition_cache=2000`
  - `log_bin_trust_function_creators=ON` (if `log_bin` is enabled)
  - `binlog_format=mixed` (if `log_bin` is enabled)
  - `max_connections = 1000`
  - `innodb_file_per_table=0`
  - `innodb_buffer_pool_size=800M`
3. Start the MySQL service.

## **Maximum Number of Sessions Exceeded in Oracle**

### **Symptom:**

In my CA UIM environment, the maximum number of sessions has exceeded in Oracle. How can I address this issue?

### **Solution:**

If multiple CA UIM installers point to the same Oracle database, the maximum number of sessions can exceed in Oracle. You can follow these steps to resolve this issue:

1. View the actual number of sessions to the Oracle instance:
 

```
SQL> show parameter sessions;
SQL> show parameter processes;
```
2. Change the sessions and processes parameters in spfile for all the SIDs:
 

```
SQL> alter system set processes=1500 scope=spfile sid='*';
SQL> alter system set sessions=1500 scope=spfile sid='*';
```
3. Shut down and start the Oracle instance so that the changes are saved:
 

```
SQL> shutdown immediate
SQL> startup
```
4. Open all the pluggable databases after restarting the oracle instance:
 

```
SQL> alter pluggable database all open;
```
5. View the effected values:
 

```
SQL> show parameter sessions;
SQL> show parameter processes;
```

### **Unable to Reach controller (Linux robot Communication Error)**

#### **Symptom:**

In my Linux environment, I am receiving Linux robot communication error, where the controller is unreachable.

#### **Solution:**

Some Linux environments have trouble auto-detecting the local IP. This causes problems with probes listening for incoming connections.

To address this issue, manually set the specific host name and IP address in the robot.cfg file under the `/opt/nimsoft` directory. Leave all the defaults except the following three lines:

```
robotname = ?set this to the computer hostname (shortname)
robotip = set this to the local/internal IP address of the machine
first_probe_port = 48003
```

Also, note that the local firewall may play a role in this case. Typically, you must open the ports 48000-48100 on any robot, allowing connections from all other computers on the local network.

### **Unable to Write to the Log File**

#### **Symptom:**

I am receiving the following error for my probe:

```
CA UIM Alert : Failed to re-open log file 5 times. Logging is deactivated. Error:
Permission denied
```

#### **Solution:**

This issue of unable to write to the log file usually occurs because of an anti-virus or some other permissions issue. Ensure that your anti-virus is not preventing the logs from being written. We recommend that you exclude the entire UIM folder from the anti-virus scanning. This alert can occur in multiple probes. Therefore, excluding the entire UIM folder from anti-virus scanning is recommended.

### **Clearing niscache on an Individual robot**

#### **Symptom:**



I want to understand how can I clear niscache contents of an individual robot using IM?

**Solution:**

1. Access Infrastructure Manager.
2. Navigate to the robot, select the controller probe, and press Ctrl-P.  
The probe utility dialog opens.
3. Click the **Options** icon.
4. Select the **Expert Mode** option, and click **OK**.
5. In Probe Commandset, select `_nis_cache_clean`, and click the arrow (green) to send the command request.
6. In Probe Commandset, select `_reset_device_id_and_restart`, and click the arrow (green) to send the command request.  
The niscache is now clean and the robot is restarting.

**data\_engine Memory Usage Not Coming Down**

**Symptom:**

In my environment, I observe that the memory usage of the `data_engine` probe keeps on increasing. It does not come down even after one or two days.

**Solution:**

To resolve this issue, configure the `data_engine` probe with the following configuration parameters based on your requirements:

- `hub_bulk_size`  
This parameter specifies the number of QoS messages that are sent at one time between the primary hub and `data_engine`. Enter the appropriate value depending on the number of incoming QoS messages in the primary hub.
- `thread_count_insert`  
This parameter helps increase the `data_engine` performance. When `thread_count_insert` is greater than one, multi-threading is enabled and the configured number of threads are allocated to commit data to the database server. We recommend that you set this parameter value to the number of CPU cores at the primary hub.

**Communication Error When Double-Clicking a Probe**

**Symptom:**

When I double-click a probe, I receive the following communication error:

```
Unable to reach controller, node: </Domain/Hub/Robot/Probe> error message: communication error
```

**Solution:**

Use the telnet utility on the host where IM is running to test the connectivity to the controller port on robot. For example, telnet 192.168.2.4 48000

If the telnet succeeds, verify the messages section in IM for a timeout related to getting the probe configuration. If a timeout message exists, increase the **Probe Request, Timeout Value** in IM from the **Options** menu. Set the value to a slightly higher value, and retest the failing operation. Repeat, if necessary.

If the telnet fails, verify whether a firewall exists between the robot and the computer where IM is running and/or a firewall on the robot host.

If any NAT is involved; that is, the registered robot IP is not reachable directly but only through an NAT interface, add the following parameters to your robot.cfg file for the robot where you are unable to reach the probes:

```
robotip_alias = <NAT IP through which robot can be reached>
robotip = <Robot local IP address>
```

An example is as follows:

```
robotip = 192.168.2.4 <= Local IP of the robot host
robotip_alias = 172.16.1.4 <= NAT IP of robot host
```

## **Facing Issues with baseline\_engine**

### **Symptom:**

I am facing the following issue with the baseline\_engine probe:

- The baseline\_engine.QOS\_MESSAGE queue has a large number of unprocessed items and appears to have stopped processing.
- Memory for the baseline\_engine probe shows to be at 100% of Xmx.
- Processor usage shows to be equal to 1 core CPU availability.
- Restarting the probe allows it to process messages for a few minutes before coming to a halt again.

### **Solution:**

This probe uses the log4j system for probe logging. A known issue exists with this SDK where it has been discovered that if the thread that handles logging is unable to keep up with the amount of information being logged, it blocks other threads that do the real work of the probe.

#### **NOTE**

This problem can affect other Java-based probes that use the log4j SDK for logging (such as the discovery\_server probe).

To address this issue, follow these steps:

1. Navigate to the nimsoft\probes\SLM\baseline\_engine directory.
2. Edit the log4j2.xml file.
3. Modify the AppenderRef lines to have ref="console" as shown below:

```
<Loggers>
<Root level="info" additivity="false">
<AppenderRef ref="console"/>
</Root>
<Logger name="PERFORMANCE" level="off" additivity="false">
<AppenderRef ref="console"/>
</Logger>
<Logger name="MESSAGELIMIT" level="off" additivity="false">
<AppenderRef ref="console"/>
</Logger>
<Logger name="com.ca.analytics.dmc.receive" level="info" additivity="false">
<AppenderRef ref="console"/>
</Logger>
<Logger name="org.quartz" level="warn" additivity="false">
<AppenderRef ref="console"/>
</Logger>
<Logger name="always" level="trace" additivity="false">
<AppenderRef ref="console"/>
</Logger>
<Logger name="org.springframework" level="warn" additivity="false">
<AppenderRef ref="console"/>
```

```

</Logger>
<Logger name="com.nimsoft.threshold.cmd" level="error" additivity="false">
<AppenderRef ref="console"/>
</Logger>
<Logger name="com.nimsoft.derivedmetrics.performancstats" level="warn"
 additivity="false">
<AppenderRef ref="console"/>
</Logger>
<Logger name="com.nimsoft.derivedmetrics.scriptlink" level="warn" additivity="false">
<AppenderRef ref="console"/>
</Logger>
</Loggers>

```

For more information about this issue, see the related [Knowledge Base Article](#).

## **Troubleshooting CVE-2018-13820 and CVE-2018-13819 Vulnerabilities Fix**

### **ems Not Working After Upgrade**

**Symptom:** I upgraded my current CA UIM environment using the upgrade patch. However, the ems probe is not working.

**Solution:** If ems is not working after the upgrade, follow these steps:

1. Deactivate the ems probe.
2. Navigate to the location where ems is installed ( `<uim_home>\probes\service\ems` ).
3. Remove or rename the db folder.
4. Activate the ems probe.  
The probe now starts working.

### **Probe Not Communicating with data\_engine**

After the upgrade, if an impacted probe is not communicating with data\_engine, verify that the same .pem file that is generated on data\_engine is also present on the robot. Also, the robot.cfg is configured accordingly.

## **Troubleshooting Dependency Removal on EOL Microsoft VC++ Redistributables**

### **New MS VC++ Redistributable Not Installing When Deploying New Robot Using ADE**

If you use the automated\_deployment\_engine (ADE) probe to deploy the new robot (available in this release) onto your Windows computers, the robot will be deployed successfully but the new "Microsoft Visual C++ Redistributable for Visual Studio 2017" might not be installed.

To address this issue, we recommend that you follow the information in the article [Update for Universal C Runtime in Windows \(KB2999226\)](#) before you try to install the new robot using ADE.

### **CABI JasperReports Server Not Responding**

**Symptom:** The CABI JasperReports Server in my environment stops responding inadvertently. The environment details are as follows:

- UIM 20.3
- CABI JasperReports Server 7.1.1

**Solution:** If you are observing the following behavior, the suggested resolution might help you resolve the issue:

- Regular unresponsiveness of the JasperReports Server, leading to the CABI content becoming unavailable in OC.
- The JasperReports Sever log file may display the following errors before the JRS shutdown command is triggered: (path: CA Business Intelligence\apache-tomcat\webapps\jasperserver-pro\WEB-INF\logs\jasperserver.log)
 

```
Caused by: javax.servlet.ServletException: java.lang.IllegalStateException: Cannot create a session after
the response has been committed
 at org.apache.jsp.WEB_002dINF.jsp.modules.about.about_jsp._jspService (about_jsp.java:320)
 at org.apache.jasper.runtime.HttpJspBase.service (HttpJspBase.java:71)

ERROR EhCacheImpl,localhost-startStop-2:556 - -- JasperServer: EhCacheImpl shutdown called. This normal
shutdown operation.
ERROR EhCacheImpl,localhost-startStop-2:559 - -- JasperServer: EhCacheImpl calling cleanerTimer.cancel().
This normal shutdown operation.
ERROR GenericExceptionHandler,https-jsse-nio-8443-exec-5:51 - Unexpected error occurs
java.lang.NullPointerException
```

To resolve the issue, set both JRE\_HOME and JAVA\_HOME server variables to point to JRE provided with Broadcom's CABI JasperReports Server installation: /opt/CA/SharedComponents/CABI/jre.

### **Monitored Technologies Dashboard Not Working with cabi\_external**

**Symptom:** My environment contains UIM 20.3 instance with cabi\_external 4.20 and JasperServer 7.1.1. The cabi\_external deployment is successful and all CABI dashboards are working except for Monitored Technologies. I am receiving the error An unexplained error has occurred and the operation failed.

**Solution:** This issue is seen when uim\_core\_dashboards\_pack 2.46 is deployed on the cabi\_external robot. The uim\_core\_dashboards\_pack 2.46 package is deployed by default because it is included with UIM 20.3. However, it should only be deployed with the bundled cabi installs (cabi 4.30). Therefore, to resolve this issue, download uim\_core\_dashboards\_pack 2.45 from the UIM archive and deploy the package to the cabi\_external robot.

#### **NOTE**

UIM 20.3.3 has removed dependency on CA Business Intelligence (CABI) for rendering the native OC screens: Home page, Group view page, Device view page, and Monitoring Technologies (probes) view page. Custom and Out-of-the-Box dashboards and reports are still rendered by using CABI; that is, they have a dependency on CABI. However, the native OC screens are no longer dependent on CABI (Jaspersoft) and are rendered by using HTML5. For more information about the native OC screens using HTML5, see the [Configuring and Viewing Monitoring Data](#) article or the "Removing CABI Dependency (Native Operator Console)" section in the [UIM 20.3.3](#) article.

### **Some Secondary Hubs Not Updating Robot to 9.31**

**Symptom:** While upgrading, some secondary hubs were not updating robot to the 9.31 version giving a dependency. However, distsrv 9.31 was already installed first.

**Solution:** As a workaround, install "NimBUS Infrastructure.exe" directly on the hub, and then it will upgrade.

### **Memory Issue After Upgrading CABI**

**Symptom:** After I upgraded CABI, I observed that the Java process memory was going up and was becoming unresponsive.

**Solution:** Verify that the PATH environment variables are not pointing to the older Java version. Ensure that your Java path in the PATH environment variable is updated with the new version path for it to start working.

### **CABI Installation Is Successful But User Synchronization Failed**

**Symptom:** My CABI installation is successful, but the user synchronization is failing. I see the following error in the cabi.log file:

```

Dec 15 20:17:41:548 [main, cabi] Resetting rest user 'CABI_REST_USER'
Dec 15 20:17:44:035 [main, cabi] Deleting rest user CABI_REST_USER
Dec 15 20:17:46:508 [main, cabi] deleteJasperUser(): userDeleteUrl:
http://10.xx.xxx.xxx:80/cabijs/rest_v2/users/CABI_REST_USER
Dec 15 20:17:50:454 [main, cabi] JasperUserUtility:login(): URL attempted:http://10.xx.xxx.xx:80/cabijs/
login.html
Dec 15 20:17:50:454 [main, cabi] JasperUserUtility:login(): Response code :403
Dec 15 20:17:50:454 [main, cabi] JasperUserUtility:login(): Got an unauthorized response, I should fall back
to superuser login
Dec 15 20:17:51:742 [0176] Controller: Probe 'cabi' (command = <startup java>) returns no-restart code (42)

```

**Solution:** Review the following steps:

1. Connect to the database using any SQL client and check the number of rows in the CM\_AUTHENTICATION table by using the SELECT \* FROM CM\_AUTHENTICATION query.
2. Ideally, it should have only one record. If there are multiple records, take a backup of this table and remove all the older records except the latest ones.
3. Restart the CABI robot.

### **CABI Installation Failing**

**Symptom:** Installation of CABI 4.3 was failing on Windows Server 2016 when the robot service was run using the non-administrator user. The cabi.log shows the following error:

```

Initialization using the property file is unsuccessful. java.lang.RuntimeException: Failed to create the
keystore D:\Nimsoft\config\jrsks
Caused by: java.io.FileNotFoundException: D:\Nimsoft\config\jrsks (Access is denied)

```

**Solution:** Review the following steps:

1. Deploy CABI 4.2 to a robot.
2. Once the deployment is completed, it shows up the "local" keyword reference error. Then, on the CABI robot, navigate to "../probes/service/wasp/webapps/cabijs/WEB-INF/applicationContext-virtualdatasource.xml" and change the keyword from "local" to "bean".
3. Navigate to the OC robot's "../probes/service/wasp/lib/services" folder, copy the "groovy-all-2.4.7.jar" file and place it in the CABI robot's "../probes/service/wasp/webapps/cabijs/WEB-INF/lib" folder. And, remove the existing "groovy-all-2.4.5.jar" file from this location and restart the CABI robot.
4. After the CABI robot restart, you can access CABI through its URL.
5. Deploy the CABI 4.3 probe to the CABI robot.

### **Unable to Edit Created Schedules in CABI**

**Symptom:** I am unable to edit the created schedules in CABI 4.3.

**Solution:** Follow the step 2 in the [KB Article](#).

### **Unable to Run Scheduled Reports**

**Symptom:** I am unable to run the scheduled reports and send the related emails to the intended recipients. I see the following error message in the jasperserver.log file:

```

2020-11-19T10:24:34,406 ERROR ErrorLogger,quartzScheduler_QuartzSchedulerThread:2407 - An error occurred while
scanning for the next triggers to fire. org.quartz.JobPersistenceException: Couldn't acquire next trigger:
[TibcoSoftware][SQLServer JDBC Driver][SQLServer]Invalid column name 'SCHED_TIME'. [See nested exception:
java.sql.SQLException: [TibcoSoftware][SQLServer JDBC Driver][SQLServer]Invalid column name
'SCHED_TIME'.]

```

**Solution:** Follow the step 1 in the [KB Article](#).

## Troubleshooting Monitoring Configuration Service (MCS)

This article provides information about how you can troubleshoot various MCS-related issues.

### MCS processes Group Profile Not Deploying

#### **Symptom:**

I have deployed a processes MCS profile to one of my OC groups. The profile at a group level shows as deployed. However, when I select the device, I do not see any processes profile deployed locally.

#### **Solution:**

This issue can happen if you have inadvertently activated the option "For-Each Deployment" without specifying any matching expression. Activate this option only if you need the profile to be deployed on the subset of target devices inside the destination group. In that case, select that the matching expression should be for the selected Value. If you need the profile to be deployed on ALL target devices, do not use the "For-Each Deployment" option.

### Group Profile Failing on a Few Devices

#### **Symptom:**

After I create a group profile, I check the deployment status of the profile. The status shows that the profile is deployed successfully on certain devices, is yet to deploy on some devices, and has failed to deploy on a few devices. How can I find the reason for the failed deployment?

#### **Solution:**

You can use these queries and try to troubleshoot the issue:

- Use the following query to find out the number of devices on which the profile deployment has failed:  

```
select * from ssrv2profile where ancestorprofile=<group profile id> where status = 'error'
```
- Check the ssrv2audittrail table to understand the reason for the failure.
  - Find the cs\_id and profile ID from the above query.
  - Use the following query for the reason:  

```
select * from ssrv2audittrail where objectid=<profileid>
```

The result specifies the reason for the failure. Some possible reasons are probe deployment deferred, profile deployment deferred. For such reasons, check the robot status. It is possible that there is a communication error or the robot is down.
- Use the following query to get the device information:  

```
select * from cm_device where cs_id=<device cs_id>
```

---

## Documentation Legal Notice

---

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

