

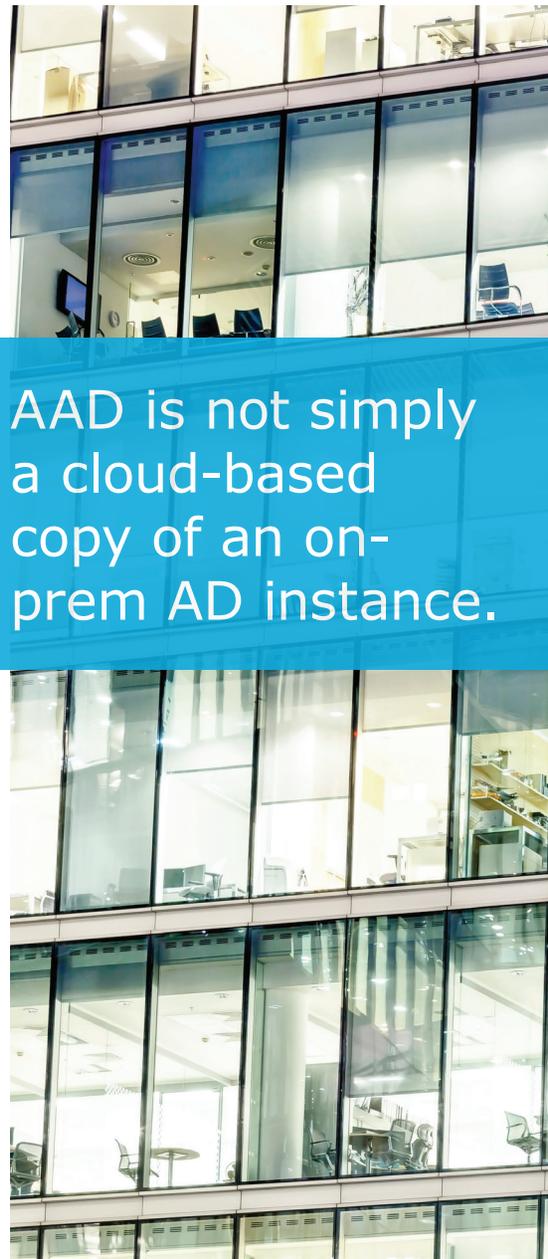
The top five ways to relieve the pain of managing hybrid AD environments

By Todd Peterson
IAM Evangelist, One Identity



Table of Contents

Challenge #1: Two tools too many	4
Pain Remedy 1: One tool to rule them all	4
Challenge #2: Inconsistency kills	6
Pain Remedy 2: Templates are cool	6
Challenge #3: It all starts with provisioning	7
Pain Remedy 3: Provisioning done right ... and done once	9
Challenge #4: A syncing ship	9
Pain Remedy 4: Everything shipshape	9
Challenge #5: Who gives you the right?	10
Pain Remedy 5: The right rights	10
Conclusion	12



AAD is not simply a cloud-based copy of an on-prem AD instance.

Active Directory is everywhere and Azure Active Directory (AAD), its cloud-based cousin, is quickly gaining ground. Currently, nearly ninety percent of organizations worldwide are using Active Directory (AD) for on-premises resources (aka on-prem). That represents 500 million organizations and somewhere around 10 billion daily authentications. In fact, in the world of identity and access management (IAM), AD has become unavoidable and absolutely necessary for on-prem user authentication and authorization. You have to go through AD. It's just how it's done. Now, mix in the cloud – and Azure AD – and your management complexity just skyrocketed – and you could be in for a world of pain, if your on-prem or cloud identity environments are not managed and synched properly.

Currently, there are north of 10 million AAD tenants representing about 700 million accounts and approximately 13 billion daily logons. The majority of these transactions are to access the extremely popular productivity applications available via the Microsoft cloud initiative, such as Office 365, Exchange Online, SharePoint, etc. However, reliance on the Azure platform is growing

for traditional IAM activities, such as multifactor authentication (MFA), federation and single sign-on, and password management. It's important to note that most of these expanded capabilities are only available via Azure Active Directory Premium, which is significantly more expensive than the AAD functionality necessary to use Office 365 (for instance).

In all but the rarest of cases, organizations that adopt cloud-focused AAD do so while still firmly rooted in the on-prem AD world. This poses a huge and unexpected issue - AAD is not simply a cloud-based copy of an on-prem AD instance. It is a wholly separate environment. In other words, in organizations where on-prem AD and Azure AD coexist and are equally critical to success, the organization – and the IT team – must manage a two-part, hybrid AD environment.

The sprint to the cloud is fraught with complexity, risk, inefficiencies and pitfalls. If not implemented and managed properly, it can cause headaches or worse for your AD administrators and users. This eBook addresses five potentially pain-inducing challenges that most organizations must overcome as they attempt to navigate the potentially turbulent transition to a hybrid AD implementation.

Challenge #1: Two tools too many

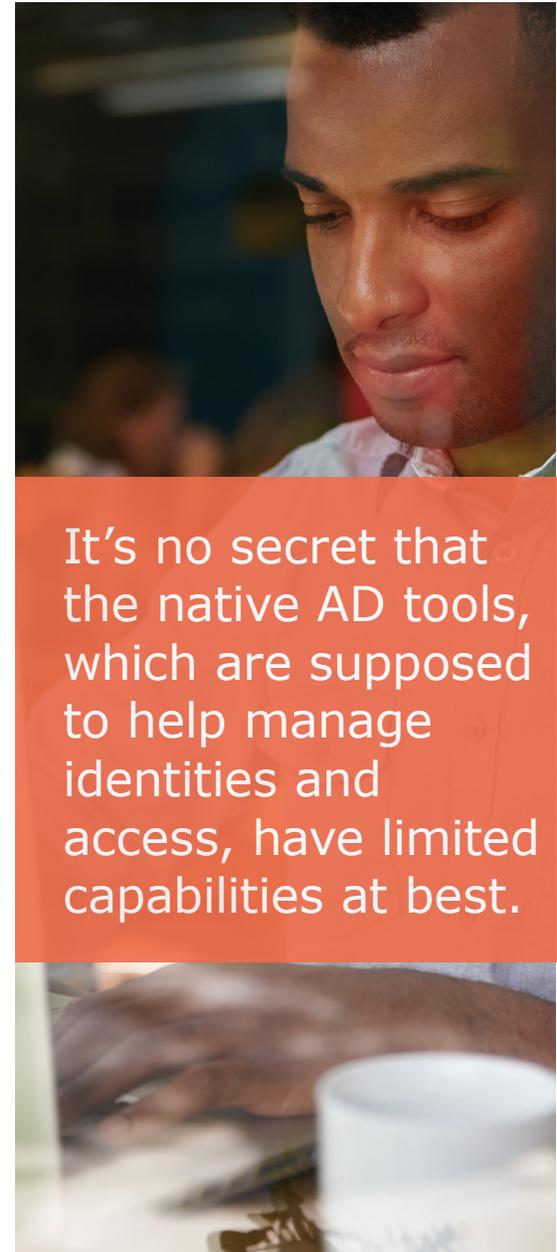
It's no secret that the native AD tools, which are supposed to help manage identities and access, have limited capabilities at best. Even with earnest efforts to improve native Active Directory Users and Computers (ADUC) tool, most organizations choose to adopt a third-party tool to streamline, automate and bring consistency to AD-management tasks. The situation is only exacerbated as organizations adopt Azure Active Directory (AAD). AAD does not use ADUC and requires its own tool for basic administrative tasks.

To execute the same action, such as provisioning a user, in AD and AAD requires the use of separate tools with entirely unrelated interfaces, disparate functionality and divergent training methodologies. Therefore, an already cumbersome task for on-prem AD becomes doubly so when it must be duplicated for AAD. Again, AAD is not simply a cloud-version of AD. So home-grown scripts, PowerShell automation and manual processes cannot be easily applied to AAD.

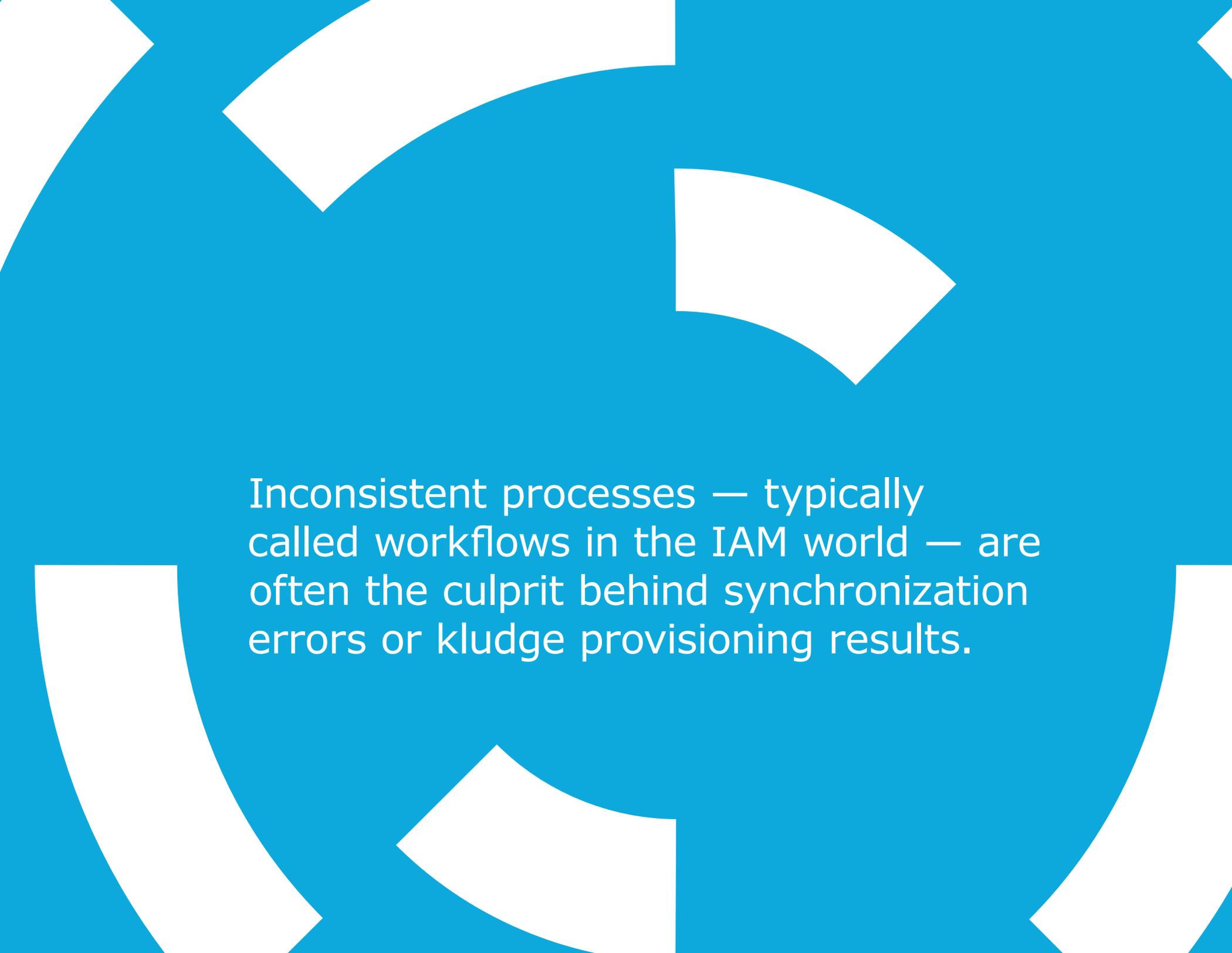
Pain Remedy 1: One tool to rule them all

The ideal solution to the two-tool challenge would be a single tool that overcomes the native shortcoming of ADUC and AAD's administrative interface. That tool exists in One Identity Active Roles. Active Roles provides a layer of automation, consistency, and ease-of-use that makes every administrative task for AD and AAD quick, easy, thorough and accurate. Thousands of organizations rely on Active Roles every day to ensure the efficiency and security the administration of their on-prem AD demands and now those organizations can apply that same rigor and efficiency to AAD.

Active Roles is optimized for both AD and AAD and provides single-action task execution that solves the issues of the hybrid AD environment. Admin-users report significant time savings (often more than 80 percent) through the use of Active Roles. They also report a dramatic increase in security (i.e. less opportunity for user error). In fact, Active Roles provides administrative and workflow templates that ensure administrative tasks in the hybrid AD environment are executed correctly every time.



It's no secret that the native AD tools, which are supposed to help manage identities and access, have limited capabilities at best.



Inconsistent processes — typically called workflows in the IAM world — are often the culprit behind synchronization errors or kludge provisioning results.

Challenge #2: Inconsistency kills

When forced to rely on manual processes, busy organizations struggling with managing the intricacies of a hybrid AD environment often find themselves doing the best they can, and fall into bad habits of 'just get it done' with little thought on how it should be done. It's understandable: We have impatient users demanding immediate results; tools that make it difficult to do things consistently in one environment, much less two; separate and unrelated native tools with limited capabilities; and too much reliance on tribal knowledge and 'that's how it's always been done.'

This inconsistent processes — typically called workflows in the IAM world — are often the culprit behind synchronization errors or kludge provisioning results. Typical areas of inconsistency for the hybrid AD environment include:

- Aligning group membership with job role in both AD and AAD
- Gaining appropriate line-of-business approvals for provisioning actions
- Assigning correct permissions to individual admins (least-privilege model)
- Designing easily repeatable processes for particular tasks

As AAD is not simply a cloud copy of AD, consistency does not mean you cut and paste an on-prem AD workflow into the cloud (such as PowerShell-scripted workflow). However, it does mean ensuring that your workflows address the unique needs of both AD and AAD.

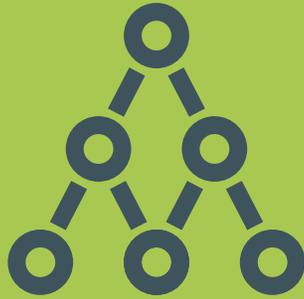
Pain Remedy 2: Templates are cool

Active Roles 7.1 includes pre-defined workflow templates for AD and ADD (individually and for hybrid environments) that are based on the experience and innovation of thousands of organizations that use Active Roles to automate, streamline

and secure the administration of their hybrid AD environments.

These templates include everything from provisioning actions in the directories, seeking approval from the appropriate line-of-business (LOB) managers, making additions to groups, DL membership assignment in Exchange/Exchange Online and virtually every imaginable scenario. In fact, Active Roles 7.1 includes out-of-the-box access templates for Office 365 and Exchange Online.

In addition, Active Roles includes customizable templates and workflows to address the unique needs of any organization. While many organization may start down the path of automation with scripting, most end up finding that the ease-of-use and intuitiveness of Active Roles make it the preferred tool in their AD management strategy. Its depth of coverage – including the hybrid AD environment – and legacy of helping organizations overcome the toughest AD/AAD challenges make Active Roles the industry-leading platform for automation.



Native tools
don't cut it
when it comes
to provisioning.

Challenge #3: It all starts with provisioning

Much of the AD/AAD-management burden is from user provisioning. This involves setting up accounts in the directory, placing people in the correct groups, and making sure they have access the proper accounts and access to all the necessary applications – such as Exchange, Exchange Online, SharePoint, SharePoint Online, Office 365 – and myriad other cloud-based applications that are available via AAD. But setting up the accounts is one thing, turning them off (or de-provisioning) is another and perhaps the more important. After all, the risk associated with a terminated employee retaining access is extremely high – but easily avoidable with the right tools.

As discussed earlier, native tools simply don't cut it when it comes to provisioning. Setting up on-prem access requires use of ADUC for AD, a different interface and process for Exchange, another for Skype for Business, and the list goes on-and-on. That doesn't even bring into account the additional tools required to set up

the same individual in AAD and all its associated cloud services.

There's a number of challenges with provisioning/re-provisioning/de-provisioning in the hybrid AD environment, namely:

- The use of multiple native tools introduces significant room for human error and inconsistency.
- The amount of time it takes to "fully" provision a user in the hybrid environment means that users may experience long periods of inactivity and non-productivity waiting for access to be granted.
- Delays in de-provisioning (or re-provisioning) introduce risk as inappropriate access may be retained long after it should be terminated.
- The authoritative data source (typically an HR system) is difficult to enable for AD, not to mention AAD resulting in large amounts of human intervention required to do the most basic provisioning/re-provisioning/de-provisioning action.



- Synchronization between AD and AAD cannot be relied on if the original AD data is flawed – a direct result of provisioning errors.

The bottom line is: If you can't get provisioning right, you can't proceed with any confidence in the security or efficacy of your hybrid AD environment.

Pain Remedy 3: Provisioning done right ... and done once

So how do you get provisioning right? To start with, eliminating as much potential for human error is key. This is done through a single tool that provides thorough provisioning (and de-provisioning) coverage for both AD and AAD. Active Roles is one such tool. Through the use of template workflows and automation, Active Roles streamlines the hybrid AD provisioning process to a single action – including AD, AAD, Exchange, Exchange Online, SharePoint, SharePoint Online, Skype for Business and so on.

But it doesn't stop there. Active Roles also draws from authoritative data sources, such as an HR system, to initiate and execute end-to-end provisioning and de-provisioning across the entire hybrid AD environment. When things happen automatically and according to the rules you established, incidents of human error, oversight or malice are virtually eliminated.

Challenge #4: A syncing ship

Azure AD includes a capability called Azure AD Connect, which synchronizes users, groups, attributes, and passwords from the on-prem AD to AAD. This single capability has driven the widespread adoption of Office 365 – the smooth migration of Office users to the cloud version, often without user realization. It enables users to login once to access on-prem and cloud-based resources seamlessly and easily.

Of course this smooth migration is much easier said than done. Typically, security for the cloud-based access is based on permissions and memberships established in the on-prem AD world. So, any errors, risk factors or security holes that exist in the on-prem AD – perhaps caused by limitations of the native tools – will replicate to the Azure AD environment.

Let me give an example: Let's say that you have a group in AD called Finance and a User X was added to the group as a necessity when User A was on leave and needed coverage. However, when the User A came back from leave, the User X was never removed from the group. This could happen for a number

of reasons, such as AD administrative staff was too busy – or forgot - to de-provision the access when it was no longer needed; possibly, the manager of Finance didn't realize the risk of this over-provisioning action; or the native tools just made it too difficult or time-consuming to do. Whatever the reason, when AD is synched with AAD, the same inappropriate rights associated with this user are now also present in AAD. If there are Finance resources available on SharePoint Online, OneDrive or any of the hundreds of applications that could potentially be enabled via AAD, this user has permission (or at least rights) to access and manipulate this sensitive data.

It's a big risk. Consider the implications of inadvertent errors from your on-prem AD being replicated out to AAD and all the resources to which AAD connects your users.

Pain Remedy 4: Everything shipshape

The solution is simple – if there are no errors in AD, they cannot be replicated to AAD. So how do you ensure that your on-prem AD is shipshape? Since the source of most errors is the human factor, removing as much opportunity for error is key to a clean and safe AD – and thus a clean and safe AAD.

Active Roles provides the automation and built-in workflows necessary to ensure that users are granted appropriate rights and placed in the correct groups, along with all the approvals, audit trails, and checks-and-balances required to reduce risk. If it's easy (or automatic) to grant people correct rights and consequently revoke rights when necessary, it's easy to keep AD clean. Active Roles can even communicate with an authoritative data source (such as an HR system) to automatically initiate actions on AD and AAD accounts. So in the case of our example, when User A returned from leave, Active Roles would automatically reinstate those rights and revoke the rights of User X.

With Active Roles central to your AD-management strategy, the potential for errors – and replicating them in AAD – is significantly reduced.

Challenge #5: Who gives you the right?

The glaring security gap in native AD/AAD management tools is the lack of privileged account management. With these tools, an administrator account

is required to do any action – such as provisioning a user, placing people in groups, resetting a password, installing updates, backing up the directory, deploying a new domain controller or any other necessary admin actions. The problem is that this account is tied to the directory and not an individual. That means a number of people share the credential and that everyone uses the same administrator login info. Plus, this one login has access to everything. So, it doesn't matter if the action is to simply reset a user's password or to deploy a new domain controller – everyone with that login has the same rights.

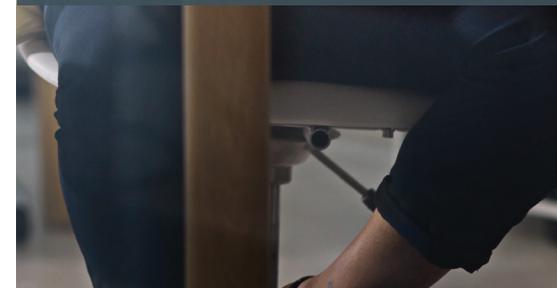
This situation is fraught with risk due to a complete lack of individual accountability for the admin account. On top of that, the on-prem AD admin account does not apply to AAD (and vice versa), and the permissions are still all-or-nothing, which now opens up your cloud environment to risk.

Pain Remedy 5: The right rights

The correct way to issue admin rights in a hybrid AD environment is to grant privileged users only enough permission to do their job – nothing more, nothing less. This is a concept called least-privilege access. Active Roles 7.1 provides a least-privilege



This situation is fraught with risk due to a complete lack of individual accountability for the admin account.



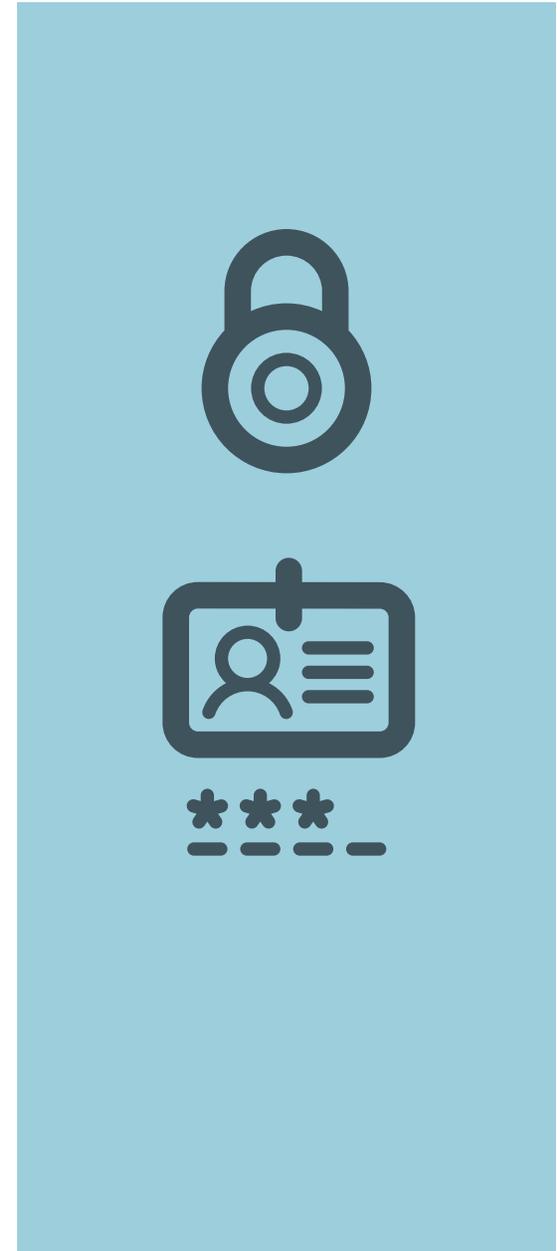
layer of security for AD and AAD by which you can manage what individual admins are allowed to do and what they are not allowed to do. It removes the potential for individuals to inadvertently or maliciously take actions beyond their role and responsibility.

With Active Roles 7.1, you have a single tool that enables you to define administrative roles across AD, AAD, Office 365, Exchange, and so on. The admin tasked with resetting passwords can only reset passwords (maybe you want them to handle both AD and AAD environments); the provisioning admin(s) can't access or manipulate logs; and the software-install person is insulated from doing day-to-day user administration tasks. Active Roles 7.1 acts as an additional layer of control and security around the hybrid AD environments.

But wait there's more... Our hybrid capabilities don't stop with the cloud

In addition to solving the five challenges mentioned above, Active Roles 7.1 also delivers:

- Auditing with change history and user activity reporting for both AD and AAD
- Application-license management to optimize SaaS expense control
- Integration with leading AD management tools for auditing, migration, Group Policy management and change auditing
- Extensive scripting and customization capabilities
- Integration with enterprise IAM functionality including:
 - Enterprise provisioning and governance
 - AD bridging
 - Password vaulting
 - User and LOB self-service
 - Multifactor authentication
 - Secure remote access
 - Risk-based adaptive security



Conclusion

With the rapid rise of Azure Active Directory, the vast majority of organizations will maintain on-prem AD while also growing their cloud deployment. This hybrid AD environment presents unique challenges that can be extremely painful to manage with native tools or manual processes. One Identity's Active Roles 7.1 is the ideal solution to avoid or relieve the pain of the hybrid challenges described above, as well as close security holes, reduce risk, and – above all – drive consistency and efficiencies in any hybrid AD environment.

About One Identity

The One Identity family of identity and access management (IAM) solutions offers IAM for the real world, including business-centric, modular and integrated, and future-ready solutions for identity governance, access management and privileged management.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.

© 2016 Quest Software Inc. ALL RIGHTS RESERVED. This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.