Plugging the Gaps Azure AD Connect Leaves in Your Cloud Disaster Recovery Strategy

Your cloud-only objects and attributes aren't covered by your on-premises backup and recovery plan.

INTRODUCTION

If your organization has a hybrid Active Directory (AD) environment, or is considering moving to one, you're not alone. Microsoft says that 75 percent of customers with at least 500 users have an AD environment that is hybrid: Their on-premises AD remains the primary source of authentication and authorization, and they synchronize that on-premises AD to Azure AD using Azure AD Connect[1]. On-premises credentials authenticate users to cloud applications and the on-premises backup and recovery solution protects everything. What's not to love?

But there is one very large fly in the ointment: Your on-premises solution won't actually back up and recover everything. The fact is, it's practically impossible to run Office 365 or Azure without creating some cloud-only objects. Since the Azure AD Connect synchronization is in most cases one-way, from on-premises AD to Azure AD, those cloud-only objects are not covered by your on-premises backup and recovery tools. Moreover, the native option – undeleting cloud objects from the Recycle Bin – is sorely limited. As a result, you're left with a critical gap in your enterprise data recovery strategy.

This white paper explores this problem and offers a solution. We'll review how a hybrid AD environment works, explain the types and purposes of cloud-only objects and attributes, and discuss the limitations of native tools for recovering them. Then we'll explain how you can get the comprehensive backup, recovery and disaster recovery you need for your hybrid AD environment with Quest® solutions.

1 Simons, Alex, "Best way to connect to Office 365 and Azure AD (latest data) + Azure AD Connect Momentum," Microsoft Enterprise Mobility + Security Blog, January 2016, https://cloudblogs.microsoft.com/enterprisemobility/2016/01/05/best-way-to-connect-to-office-365-and-azure-ad-latest-data-azure-ad-connect-momentum/

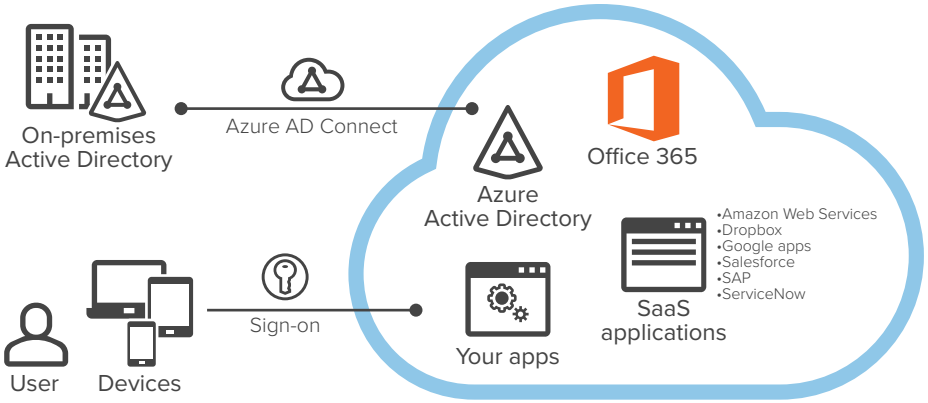

Figure 1. Many organizations link their on-premises Active Directory environment to the Microsoft Azure cloud using Azure AD Connect.

When we ask our customers how many cloud-only objects and attributes they have, they frequently tell us that they don't know.

THE ANATOMY OF A HYBRID ACTIVE DIRECTORY ENVIRONMENT

In most organizations with a hybrid AD environment, the on-premises AD is the primary source of authentication and authorization, and on-premises AD is synchronized to Azure AD using Azure AD Connect. On-premises credentials authenticate users to Office 365, custom cloud applications, and common SaaS apps like Dropbox, Google apps and Amazon Web Services (AWS), as illustrated in Figure 1.

WHAT THE AZURE AD CONNECT SYNCHRONIZATION MISSES

For most customers, however, the synchronization goes in one direction only: from on-premises AD to Azure AD. Objects and attributes that are created in the cloud are not usually synchronized back to the on-premises AD. That means they are not covered by on-premises backup and recovery solutions. In fact, when organizations do enable the write-back feature for two-way synchronization, they risk leaving even more objects in their Azure AD uncovered by their backup and recovery plan.

When we ask our customers how many cloud-only objects and attributes they have, they frequently tell us that they don't know. Here, then, are the most common types of cloud-only items that are invisible to on-premises backup and recovery, and the challenges involved with restoring them in the cloud using native tools.

Cloud-only attributes

While most Azure AD objects are synchronized from on-premises AD, they often have certain additional attributes that exist only in the cloud. These include:

- **Office 365 license type —** Every Azure AD user has an Office 365 license type that determines the features to which the user is entitled.
- **Extension attributes —** Azure AD also allows you to create new attributes for users, groups and certain other objects. For example, financial services companies build trading applications in Azure and create an extension attribute that controls access to them.

If a user object with one or more cloud-only attributes is deleted, you could recover the on-premises AD user object and use Azure AD Connect to synchronize it back up to Azure AD, but the cloud-only attributes would be gone and the user would lose access. For example, if a user is restored without the license type attribute, they would be unable to access any Office 365 applications. And you'll need to hurry to get the attribute restored before another user claims the license!

So instead of using Azure AD Connect, you have to restore the user object from the Azure AD Recycle Bin. Sounds easy enough, right? Well, keep in mind the following limitations:

- It's hard to figure out what you need to restore. There is no native change log or comparison report to help you determine which Azure AD objects have been changed or deleted, so how could you figure out exactly what you need to restore?
- You can recover only recently deleted objects. The Azure AD Recycle Bin keeps deleted objects for a maximum of 30 days. If it has been longer than that since the user was deleted, you're out of luck.
- Some objects cannot be recovered at all. A hard-deleted object bypasses the Recycle Bin, so you can't restore it using native tools no matter how recently it was deleted.
- You can't restore in bulk without PowerShell. An outside attacker, an errant script or a malicious insider can easily cause a massive number of incorrect changes or deletions in your Azure AD. But there is no native way to restore multiple users at one time without using PowerShell.

Moreover, sometimes the object itself isn't deleted; rather, the object's Office 365 license type or extension attribute is improperly changed or deleted. In those cases, you're really out of luck. Since cloud-only attributes are never recorded in your on-premises AD, neither Azure AD Connect nor native tools will help you restore them.

Finally, there is no way to restore specific attributes that have been modified in a user object.

Office 365 groups

Users often create Office 365 groups to establish sets of people they want to collaborate with and a collection of resources for those people to share, such as a mailbox and calendar in Exchange Online, team sites in SharePoint Online and notebooks in OneNote.

If one of these cloud-only groups is deleted by mistake, affected users will want it back quickly. You can't restore the group using Azure AD Connect, since it never existed in your on-premises AD. The Azure AD Recycle Bin stores deleted groups for 30 days, but restoring Office 365 groups is a complicated process. You can use PowerShell or the Exchange admin center to restore the groups, but you can't restore individual attributes or groups.

Similarly, if a malicious user clears the membership and deletes the group, you can restore the group to its membership only at the moment of deletion, with no way to get the membership back natively. You would need to know which users were deleted, but again, there is no Azure AD change log or comparison report to help you determine which Azure AD objects have been changed or deleted.

Azure AD groups and group membership

Organizations also create Azure AD groups to manage access to resources efficiently and in keeping with best practices. Unfortunately, if an Azure AD group or its membership is deleted, you'll have to recreate it from scratch. Azure AD groups and group membership are not moved to the Recycle Bin when they are deleted; therefore, they cannot be recovered with native tools.

Azure AD B2B and B2C accounts

Azure AD offers two special kinds of user accounts to help you support your external customers and partners: business-to-business (B2B) and business-to-consumer (B2C) accounts. Organizations often have thousands or even millions of these accounts. By design, however, B2B and B2C accounts are not Microsoft Azure Enterprise accounts, and therefore they are not part of the Azure AD Connect synchronization. These accounts have different purposes:

- Organizations use B2B accounts to authenticate users from partner organizations. For example, suppose the U.S. branch of a multi-national organization has moved to a hybrid AD environment, but its Canadian counterpart has not yet adopted Azure AD. To enable the Canadian employees to access the company's cloud applications and documents, the U.S. organization creates Azure B2B accounts for them.
- B2C accounts enable you to invite users of your mobile and web apps into your Azure AD using any supported social identity with direct federation, such as

A hard-deleted object bypasses the Recycle Bin, so you can't restore it using native tools no matter how recently it was deleted.

their Facebook, Microsoft or Google+ account. B2C accounts are already extremely popular in a wide range of verticals, including finance, healthcare, insurance and retail. For instance, a company may allow customers to use their LinkedIn credentials to log on to its Azure AD. The company creates a B2C account for customers that enables them to access particular applications and data.

If a B2B or B2C account is deleted, that user won't be able to log on and access the resources and data they need. You can't recover the account using your on-premises solution, since it never existed in your on-prem AD. Instead, you have to restore it from the Azure AD Recycle Bin, subject to the same limitations discussed earlier.

If a B2B or B2C account is deleted, that user won't be able to log on and access the resources and data they need. You can't recover the account using your on-premises solution, since it never existed in your on-prem AD. Instead, you have to restore it from the Azure AD Recycle Bin, subject to the same limitations discussed earlier.

Other cloud-only user accounts

In addition to synchronizing user objects from an on-premises AD using Azure AD Connect, some organizations create Azure AD accounts using either an external directory, such as a virtual directory, or their identity management solution. Or they create cloud-only user objects that help employees connect to SaaS applications like Concur and Salesforce through Azure AD. On-premises backup and recovery will not cover those user accounts and their properties.

Objects synchronized from sources other than on-premises AD

Some applications, especially those created in house, do not work with AD natively, either by design or by function. They write directly to Azure AD outside of its native synchronization process. Examples include software for multifactor authentication that writes into Azure AD to enable user access, and applications that write data to an extended Azure AD environment to validate users.

Without synchronization from Azure AD, these objects fall outside of the coverage of on-premises backup and recovery.

TENANT-TO-TENANT MIGRATION

Another little-considered use case often arises during tenant-to-tenant migration; for example, because of organization and role changes during a consolidation, merger, acquisition or divestiture. Some companies look to Azure AD as part of their backup and recovery strategy.

Consider a company undergoing a consolidation. It has dozens of tenants and must move users among tenants because of changes in employee roles and reporting structure. But it also sees the wisdom in allowing for contingencies during the consolidation, such as the need to restore some users to their former level of application access or to offer multiple temporary levels of access to certain users. Or consider a company undergoing divestiture of an entire line of business and spinning out a tenant with hundreds or thousands of user accounts. It would be prudent, good practice to retain a final backup of the accounts.

Some companies have dozens or even hundreds Azure AD tenants for their various business units, managed by different administrative teams. If they rely on Azure AD as a failsafe during migrations and something goes wrong during their tenant-to-tenant migration or consolidation, they will find that native tools are not well suited to the task of disaster recovery.

ENTERPRISE-QUALITY BACKUP AND RECOVERY FOR HYBRID ENVIRONMENTS

Having reliable backup and recovery for both on-premises AD and Azure AD is critical for security, compliance and business continuity. As we've seen, having a solid on-premises solution is necessary but not sufficient, because it is practically impossible to run Office 365 or Azure without creating some cloud-only users, groups and attributes. The Azure AD Recycle Bin is a convenient way to restore certain recently deleted objects, but it was never intended to be an enterprise backup and recovery solution.

With solutions from Quest, you can protect your entire hybrid environment. Recovery Manager for Active Directory now integrates with Quest On Demand Recovery to deliver a complete, hybrid recovery solution that gives you peace of mind.

Recovery Manager for AD helps more than 1,600 organizations protect against inadvertent or malicious modifications to Active Directory data. Without taking Active Directory offline, it also covers any on-premises objects that you have

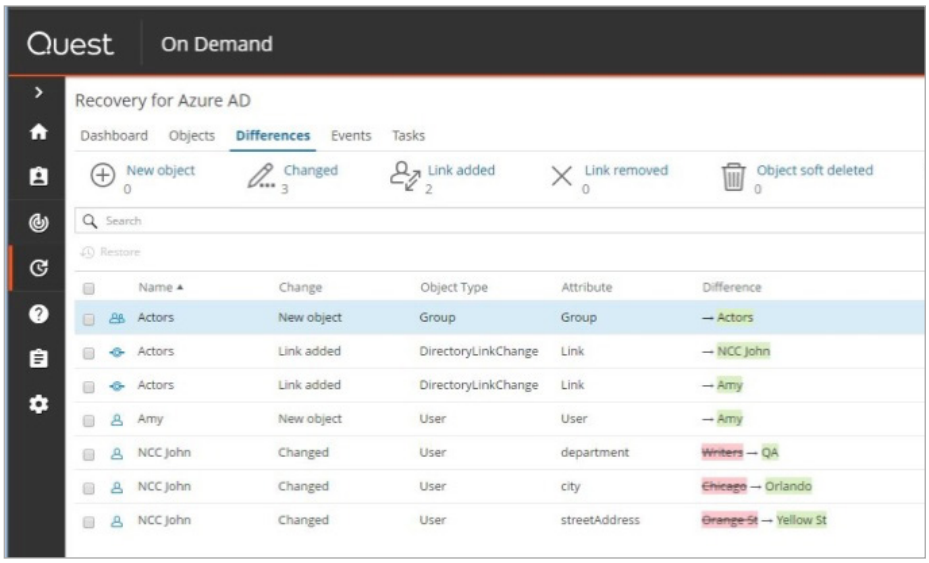

Figure 2. Difference reporting between backups and live Azure AD makes it easy to see what's changed, and select and restore exactly the changes you want.

synchronized to the cloud with Azure AD Connect. You can automate backups, pinpoint changes by comparing the current configuration of Active Directory to a backup and quickly recover entire sections of either the directory, selected objects or individual attributes.

Quest On Demand Recovery takes care of the rest, including objects not synchronized by Azure AD Connect.

By pairing these two solutions, you get a single recovery dashboard for both hybrid and cloud-only objects, with details that native tools do not provide, such as object type. You can run difference reports to determine what you need to recover, and restore any changes, whether on premises or in Azure AD, right from the report (see Figure 2).

With Quest On Demand Recovery, you can monitor the progress of objects being synchronized with Azure AD Connect. You can identify cloud-only objects or attributes that are not synchronized and avoid incomplete recovery of objects.

CONCLUSION

Many organizations depend on Azure AD Connect for synchronization from on-premises AD to Azure AD. But that kind of one-way synchronization exposes a coverage gap in their disaster recovery strategy because it leaves cloud-only objects and attributes out of the reach of on-premises backup and recovery tools.

With the hybrid genie out of the bottle, companies are making greater use of cloud-only attributes, Office 365 groups, Azure AD groups, B2B/B2C accounts and other features of the hybrid AD environment to improve user experience. As that use grows, plugging gaps in their cloud disaster recovery strategy takes on increasing urgency.

The integration of Quest Recovery Manager for AD with Quest On Demand can provide a single recovery dashboard and help plug those gaps. Organizations can use the Quest solution to differentiate hybrid and cloud-only objects, run difference reports between production and real-time backups, and restore changes on premises and in Azure AD.

With Quest On Demand Recovery, you can monitor the progress of objects being synchronized with Azure AD Connect. You can identify cloud-only objects or attributes that are not synchronized and avoid incomplete recovery of objects.

Quest

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

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 website (www.quest.com) for regional and international office information.