Eight concepts that can help you protect and recover from unwanted changes across your Active Directories

8

TRUTHS & TIPS:

PROTECTING AZURE ACTIVE DIRECTORY AND HYBRID AD

WRITTEN BY
BRIEN POSEY,
MICROSOFT MVP

8 TRUTHS AND TIPS:

PROTECTING AZURE ACTIVE DIRECTORY AND HYBRID AD

Be Prepared for Outages

Microsoft introduced Active Directory (AD) in Windows 2000. With decades to mature, and the work that Microsoft has done over the years, Active Directory today is both stable and reliable.

Unfortunately, unwanted changes to Active Directory (on-premises and in hybrid and cloud environments) are a harsh reality for many organizations, especially as threat of malicious actors breaching AD is on the rise. These business-critical services must be protected from costly outages and threats, which can stop users from getting to email, important documents and applications. While Microsoft provides limited tools to recover a deleted account, restoring the associated permissions, groups, roles and applications can be a manual, expensive and error-prone process.

Understanding the eight concepts discussed in this paper should help you better protect your environment and plan for the inevitable recovery event.

8 TRUTHS AND TIPS:

PROTECTING AZURE ACTIVE DIRECTORY AND HYBRID AD

I. Microsoft Won't Restore Your Directory Data

As IT teams strive to avoid Active Directory data loss, it's critically important to understand that Microsoft provides limited directory protection. For on-premises Active Directory environments, the primary protective mechanisms are the Active Directory Recycle Bin and any backups that you create yourself.

Microsoft's cloud-based Active Directory (Azure Active Directory) has similar challenges. There has long been a misconception that Microsoft backs up Azure AD on its customers' behalf because Microsoft offers Azure AD as a service. However, organizations are 100% responsible for backing up their own Azure AD environments. The only significant protective mechanism that Microsoft provides is the Azure AD Recycle Bin. As such, an organization is responsible for protecting its own Active Directory and Azure AD data.

"The only significant protective mechanism that Microsoft provides is the Azure AD Recycle Bin... an organization is responsible for protecting its own Active Directory and Azure AD data."

2. The Active Directory Recycle Bin Only Protects Against Deletions

The Recycle Bin is the go-to mechanism for recovering from Active Directory problems, so it is important to understand both its capabilities and its limitations. The most important thing for administrators to know about the AD and Azure AD Recycle Bins is that although they do offer a degree of protection, they never were intended to take the place of backups.

In many ways, the AD and Azure AD Recycle Bins function similarly to the Recycle Bin that is built into Windows 10. If a user deletes a document from a Windows 10 PC's hard disk, that item is not physically deleted, but rather is placed into the Recycle Bin. This allows the item to be easily recovered if necessary.

With that in mind, consider what would happen if the documents on a user's Windows 10 PC were to become encrypted by ransomware. In such a situation, the Recycle Bin would not provide any means for recovering the now encrypted documents. That's because the Windows 10 Recycle Bin protects only against deletions, not accidental modifications.

The Azure and Azure AD Recycle Bins serve a similar purpose. ***It exists as a tool for protecting organizations when an Active Directory object is accidentally deleted, but it does nothing to protect against unwanted modifications to objects.*** Only backups can give you point-in-time recovery capabilities for Active Directory objects, unless you're using a third-party tool.

3. The Recycle Bin Won't Always Protect You Against Accidental Deletions

As previously noted, the AD and Azure AD Recycle Bins exist as a tool for protecting you against the accidental deletion of directory objects. If an administrator accidentally deletes an Active Directory user for example, it is possible to retrieve the user object from the Recycle Bin. Even so, administrators must avoid becoming completely dependent on the Recycle Bin. The Recycle Bin has a number of inherent limitations, and there is a possibility that an object that needs to be restored may not be exist within the Recycle Bin.

One of the most common reasons for an Active Directory object not being recoverable through the Recycle Bin is that the Recycle Bin is not enabled. Although the Azure AD Recycle Bin is enabled automatically, the Active Directory Recycle Bin must be manually enabled before it can be used. Until an administrator takes the steps necessary to enable the Active Directory Recycle Bin, there is no native protection against the deletion of Active Directory objects.

Another reason why the Recycle Bin may fail to provide the required protection is that items within the Recycle Bin are subject to a retention period. Once this retention period expires, the item is purged and no longer available for recovery. The default retention period for deleted Active Directory objects is 180 days. In the case of the Azure AD however, objects are only retained in the Recycle Bin for 30 days. Administrators are able to decrease the retention period, but it cannot be increased beyond the 30-day limit.

One more reason why an administrator may not be able to use the Recycle Bin to recover a deleted Active Directory object is that an object may be hard deleted. A hard delete either removes a deleted object from the Recycle Bin, or it bypasses the Recycle Bin altogether. In either case, the deleted object is rendered unrecoverable.

4. Not All Object Types Are Protected

Another critically important thing to know about the Recycle Bins is that not all objects are protected. As previously mentioned, the Active Directory Recycle Bin protects any deleted Active Directory objects, so long as the Recycle Bin is enabled.

In contrast, the Azure AD Recycle Bin was primarily designed to protect user objects. It will also protect Office 365 groups (which are sometimes called unified groups). It does not however, offer any protection for security groups or Exchange Server distribution groups.

5. Azure AD Connect Indiscriminately Synchronizes Active Directory Objects

Another thing that you need to know if your goal is to avoid Active Directory data loss is that Azure AD Connect synchronizes all Active Directory changes. This means both desirable and undesirable changes will be synched to the Azure Active Directory.

Suppose for a moment that an administrator was to make an accidental modification to an on-premises Active Directory object. Azure AD Connect has no way of knowing whether that modification was good or bad. As such, the change will be replicated to Azure AD in either case.

Similarly, if an administrator deletes an on-premises Active Directory object, Azure AD Connect will take it upon itself to also delete the corresponding user object from Azure AD in an effort to keep the two directories in sync with one another.

6. On-Premises Restorations May Create New Objects in the Cloud

One of the keys to avoiding Active Directory data loss is to understand how Azure AD Connect works. Azure AD Connect does not actually copy Active Directory items from an on-premises Active Directory environment to Azure AD, but rather it creates corresponding objects. If an administrator were to create a new user object, for example, Azure AD Connect wouldn't simply copy that object to the cloud, but would instead send an instruction that would cause Azure AD to create a new object that is similar to the one that was created on-premises. While this distinction might at first seem trivial, Azure AD Connect's synchronization architecture can cause data loss in certain circumstances.

Suppose for a moment that an administrator was to create a new user object within an on-premises Active Directory domain. Azure AD Connect would synchronize the new user object to Azure AD as expected. If the administrator later decided to delete the newly created account, the user object would be removed from the local Active Directory and placed into the Active Directory Recycle Bin (assuming that it is enabled). Azure AD Connect would detect the deletion and instruct Azure AD to remove the corresponding user object.

What happens if that the administrator decided that the user object should not have been deleted after all and restores the object from the Active Directory Recycle Bin? Azure AD Connect will realize that a change has occurred and synchronize the user object to Azure AD. Because Azure AD Connect does not actually copy objects between directories, however, the user object that is created in Azure AD is newly created. This new user object has a different GUID than the user object that previously existed in Azure AD, meaning that it is an entirely different user object.

This is problematic because of the way that user objects are managed in hybrid environments. Some user object attributes, such as proxy addresses, have to be managed at the local Active Directory domain level. Other attributes, such as Office 365 licenses, have to be managed in the cloud and are written directly to the user object within Azure AD. So, in a situation like the one described earlier where an on-premises user object was deleted and then restored, the corresponding Azure AD object is also deleted and recreated rather than being restored. This means that any Active Directory attributes that had been created or modified directly within Azure AD are now gone. When the user logs into their account, they will likely discover that although they are able to log in, there are certain things that do not work correctly. The user might for example, be unable to access their mailbox, or they might have lost access to a SharePoint team site.

"So, in a situation...where an on-premises user object was deleted and then restored, the corresponding Azure AD object is also deleted and recreated rather than being restored. This means that any Active Directory attributes that had been created or modified directly within Azure AD are now gone. "

8 TRUTHS AND TIPS:
PROTECTING AZURE ACTIVE DIRECTORY AND HYBRID AD

7. Legacy Tools Don't Work

To avoid Active Directory data loss, it's best to steer clear of using legacy tools in hybrid environments. There are a variety of legacy Active Directory management and recovery tools on the market, and while these tools may work very well in on-premises Active Directory environments, Azure AD is architecturally different from Active Directory. As such, a tool that has been designed for on-premises use probably isn't going to be as effective (if it even works at all) in an Azure AD environment.

Another option that has become popular over the last couple of years is to use a cloud-based (SaaS) solution to protect the Active Directory. Such solutions commonly synchronize an organization's Active Directory objects to the cloud provider's service. That way, administrators can use the cloud-based data to restore AD objects or to roll back changes if necessary.

Although this approach will allow you to protect your Active Directory data, it is very important that you consider the following whether a SaaS solution is able to adequately protect the Azure AD environment and what security implications you may encounter.

When you allow a cloud provider to back up your Active Directory objects, you are essentially trusting that provider with the full contents of your Active Directory. The provider may have access to user objects, group memberships, and maybe even passwords. You then have to question what the provider will do with your most sensitive data.

- *Are they outsourcing their data storage to another cloud provider?*
- *Will the data be stored in a datacenter in a foreign country, possibly causing compliance issues for your organization?*
- *Will the provider make your data available to your partners?*

These are all important questions that need to be definitively answered.

Another reason why it is important to avoid these types of tools and services is that many of them are based around third-party synchronization engines. Microsoft fully supports using Azure AD Connect to synchronize your on-premises Active Directory environment to Azure AD. However, Microsoft does not directly support running Azure AD Connect alongside a third-party synchronization engine. While parallel directory synchronizations should theoretically work without issue, object restorations and other maintenance activities could potentially confuse the synchronization engines leading to data loss or corruption.

8. Pay Attention to Your Azure AD Connect Sync Rules

Finally, be sure to periodically revisit AD Connect sync rules. These rules determine which objects are synchronized to Azure AD. It is relatively common for organizations to make changes to their Active Directory structure without updating their sync rules to accommodate those changes.

Take, for example, an organization synchronizing user objects to Azure AD. Later, the administrator creates a separate folder and moves some of the user objects into that folder, but forgets to update the sync rules to allow that folder to be synchronized to Azure AD. Although the recently moved user objects will continue to exist on premises, Azure AD will think that the user objects have been deleted, and will therefore remove the corresponding Azure AD user objects.

8 TRUTHS AND TIPS:

PROTECTING AZURE ACTIVE DIRECTORY AND HYBRID AD

Protect Your Critical Data

User errors are a reality, and the threat of malicious actors breaching AD is on the rise, yet no native tooling exists to tracks changes, store previous values or enable administrators to restore to a previous point in time. Understanding the eight concepts discussed in this paper should help you better understand the challenge of relying on native tools to protect your environment in case of the inevitable recovery event.

LOOKING FOR A SOLUTION?

Cayosoft Guardian recovers and protects Azure Active Directory and hybrid AD data. With Guardian monitoring all directory changes, administrators can quickly see, understand and rollback mistakes or malicious changes across their entire hybrid AD environment. When rollback is needed, Guardian provides an automated recovery without the need for time-consuming operations and incomplete backup files.

Learn more at www.cayosoft.com/recovery

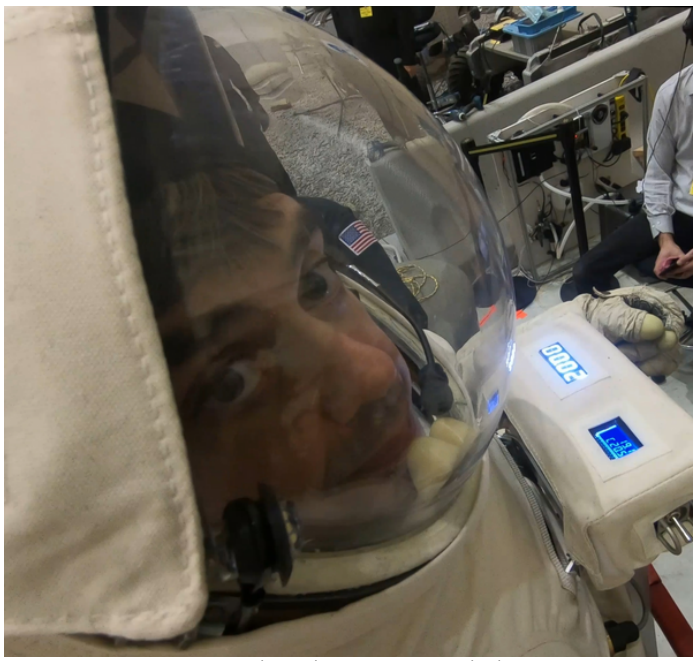
8 TRUTHS AND TIPS:

PROTECTING AZURE ACTIVE DIRECTORY AND HYBRID AD

About the Author

Brien Posey is a freelance technology author, speaker, and 18-time Microsoft MVP. Prior to going freelance, Posey was CIO for a national chain of hospitals and healthcare facilities. He also served as lead network engineer for the United States Department of Defense at Fort Knox and has worked as a network administrator for some of the largest insurance companies in America.

In addition to his ongoing work in IT, Posey has spent the last several years training as a commercial scientist-astronaut candidate in preparation for a mission to study polar mesospheric clouds from space.



Brien rocking his astronaut helmet

8 TRUTHS AND TIPS:

PROTECTING AZURE ACTIVE DIRECTORY AND HYBRID AD

About Cayosoft

Cayosoft helps organizations manage and protect their hybrid Microsoft infrastructures. Applying deep expertise in IT operations and with a focus on delivering practical new functionality, Cayosoft helps customers worldwide streamline adoption of a modern cloud infrastructure and simplify their journey from on-premises, to hybrid and to the cloud, including Office 365, Exchange Online, Azure Active Directory, SharePoint and Teams. Unlike legacy tools developed for on-premises environments , Cayosoft solutions are built from the start with hybrid, cloud and mobile users in mind.