FAQ: The Windows Server 2016 and Azure AD Recycle Bins, and Quest® Recovery Solutions

What the Microsoft Recycle Bin can and can't do, and how to get the complete recovery capabilities you need with Quest

INTRODUCTION

Window Server 2008 R2 included a particularly welcome enhancement, the Recycle Bin, which enables quick and easy recovery of some objects recently deleted from Active Directory (AD). To facilitate recovery of objects in cloud-based environments, Microsoft provides the Azure AD Recycle Bin, which offers similar but not identical functionality to its on-premises sibling. These Recycle Bins are extremely valuable in certain situations. If an AD object such as a user account has been mistakenly deleted, for instance, you might be able to quickly and easily restore the object from the AD or Azure AD Recycle Bin.

However, the Microsoft Recycle Bin is not, and was never intended to be, a complete recovery solution. This FAQ explains exactly what each of the two Recycle Bins can do, explores their key limitations, and details the comprehensive recovery capabilities provided by Quest® recovery solutions. It even offers a handy chart that makes it easy to see exactly which functionality you get in each Quest solution, in earlier versions of Windows Server that do not include the Recycle Bin, in later versions with the AD Recycle Bin, and in the Azure AD Recycle Bin.

WHAT IS THE MICROSOFT RECYCLE BIN?

Microsoft introduced the Recycle Bin in Windows Server 2008 R2 to address an important issue: In previous versions of Windows Server such as 2008 or earlier, recovering an Active Directory object that has been deleted is difficult. In short, a deleted object is tombstoned — basic information about the object is retained for a period of time, but most of the attributes are stripped. The object can be reanimated, but most of its attributes will be missing and have to be recovered manually or via scripting.

The Recycle Bin eliminates that manual effort. In Windows Server 2008 R2, 2012 or 2016, when an Active Directory object is deleted, it is placed in the Recycle Bin, where it is maintained for a configurable period of time so it can be restored much more easily, along with its attributes, groups and group membership. To make it easier to search, filter and undelete objects in the Recycle Bin, Windows Server 2012 and 2016 even include a GUI — the Active Directory Administrative Center (ADAC).

The AD Recycle Bin only enables you to restore AD objects that have been deleted. Recovery Manager for Active Directory empowers you to roll back improper or unwanted object changes, such as attribute, group membership or Group Policy modifications.

WHAT ARE THE LIMITATIONS OF THE AD RECYCLE BIN?

There are a number of limitations that are important to know about the Recycle Bin:

- **You might have to upgrade to use it —** In order to use the AD Recycle Bin, it is necessary to upgrade your AD forest to Windows Server 2008 R2 forest functional mode. To upgrade your forest, all domain controllers (DCs) in the forest must first be upgraded to Windows Server 2008 R2 or higher.
- **You have to have enabled it —** The Windows Server Recycle Bin is disabled by default and must be specifically enabled before it can be used.
- **Enabling it is permanent —** Once the Recycle Bin has been enabled, it is not possible to disable it at a later time.
- **You can't delegate recovery tasks —** The ability to restore AD objects from the Recycle Bin cannot be delegated. Only a full administrator can recover deleted objects.
- **Only recently deleted objects can be recovered —** After a configurable period of time, an object in the Recycle Bin is moved from the deleted state to a recycled state, and it can no longer be recovered.
- **Your AD database can get very large —** Retaining all deleted object information can cause significant growth of the Active Directory database.
- **You can't restore modified attributes —** The Recycle Bin is designed for restoring deleted Active Directory objects, not fixing accidental attribute modifications caused by an admin or an HR system.

WHAT IS THE MICROSOFT AZURE AD RECYCLE BIN?

If you use Microsoft Azure AD or Office 365, it is important to understand the differences between the on-premises Recycle Bin and the Azure AD Recycle Bin. If Azure AD or Office 365 users are deleted in Azure AD or Office 365, they are moved to the Recycle Bin, which is stored in the Office 365 portal. But other deleted Azure AD and Office 365 objects, including Azure AD groups and group membership, are not stored in the Recycle Bin.

WHAT ARE THE LIMITATIONS OF THE AZURE AD RECYCLE BIN?

Additional limitations of the Azure AD Recycle Bin include:

- **You must use multiple interfaces —** The Azure AD Recycle Bin is not found in the Microsoft Azure portal; it is located in the Office 365 portal.
- **You can recover only recently deleted objects —** The Azure AD Recycle Bin will store deleted Azure AD users and Office 365 groups (through PowerShell) for only 30 days. The default is 7 days. This limit can't be increased, and once the users are gone from the Azure AD Recycle Bin, they are gone forever: Microsoft does not back up or offer restores of deleted Azure AD users beyond the 30-day period.
- **Some objects cannot be recovered —** Items that were hard-deleted (meaning these objects bypassed the Recycle Bin altogether) have no native ability to be restored; they are lost forever.
- **You can't restore specific attributes —** There is no way to restore specific attributes that have been modified in a user object.
- **You can't restore in bulk —** There is no way to restore multiple users and attributes at one time from the Azure AD Recycle Bin.
- **It's hard to figure out what you need to restore —** You need to know which user or users were deleted in order to restore them, but there is no Azure AD change log or comparison report to help you determine which users have been changed or deleted.
- **You can't restore objects across tenants —** Microsoft Azure AD does not support cross-tenant backup or restores, which means there is no ability to restore Azure AD objects across multiple Azure or Office 365 tenants.

WHY DO I NEED OTHER TOOLS IF I HAVE THE RECYCLE BIN?

While the Recycle Bin GUI makes it easier to recover a single deleted object in Windows Server 2012 and 2016, and the Azure AD Recycle Bin enables recovery of deleted Azure AD or Office 365 users, Recycle Bin recovery is not a comprehensive solution for the range of AD recovery challenges that enterprise organizations face today, both on premises and in the cloud. For example, you need to be able to restore deleted AD and Azure AD objects quickly and

efficiently — sometimes even after the object has been moved from a deleted state to a recycled state. You also need to be able to granularly restore attribute information, and to be able to restore other kinds of objects, such as Group Policy objects (GPOs). And you need to be able to efficiently restore your entire forest in case of a disaster. The Recycle Bin simply cannot deliver these capabilities.

Recovery Manager for Active Directory, on the other hand, delivers the enterprise backup and recovery functionality you need. And now with the integration with On Demand Recovery for Azure Active Directory, you are protected with a complete hybrid recovery solution to give you peace of mind.

WHAT FUNCTIONALITY DOES RECOVERY MANAGER FOR ACTIVE DIRECTORY OFFER?

Recovery Manager for Active Directory provides superior recovery functionality for on-premises AD environments, including the following key features:

Comparison reporting

One of the most time-consuming aspects of native AD recovery is determining which objects need to be restored: IT administrators must manually compare backups to the current state of AD in order to determine what has changed. Aside from being tedious and error-prone, this process increases recovery time significantly.

Recovery Manager provides a comparison report that automates the comparison process, enabling you to restore deleted AD users and attributes or other objects such as groups or GPOs much faster, thereby reducing the impact of the deletion on the business.

Online granular restore

Restore users, groups and group membership as well as individual attributes (such as account settings) and binary attributes, even when the object itself has not been deleted. This enables you to restore only the required attributes without restarting domain controllers.

Attribute rollback

Accidental object deletion is only one recovery challenge; attribute information can also be overwritten or deleted. In those situations, it is even more difficult to determine what information needs to be restored, and the comparison reports in Recovery Manager are even more critical. Native tools only provide the capability to restore an object that has been deleted; Recovery Manager for Active Directory enables you to roll back improper or unwanted changes.

Restore of GPOs

GPOs store some of their information in AD, but they also store information in configuration files. Because the entire GPO is not stored in the directory, it is not possible to restore GPOs with Windows Server 2008 R2, 2012 or 2016. Recovery Manager for Active Directory enables you to recover any object, including a GPO, in a matter of minutes.

Delegation

You can delegate access to perform restores to trusted staff who are not full administrators.

Faster restores

You can restore objects faster without having to restore the system state data or take the DC offline.

Restore of recycled objects

With Recovery Manager for Active Directory, you can also restore recycled objects.

Forest recovery

Most organizations have a critical dependence on AD and cannot afford any downtime. To ensure total protection, you need to be able to quickly restore AD in the event of corrupted schema extensions or physical disaster. But the features in Windows Server 2008 R2 and higher are focused on object-level recovery only.

To deliver the comprehensive protection you need, Quest offers Recovery Manager for Active Directory Forest Edition. This edition of the solution enables organizations to address all of their disaster recovery challenges, including domain and forest recovery.

Recovery Manager for Active Directory Forest Edition enables organizations to address all of their disaster recovery challenges, including domain and forest recovery.

On Demand Recovery for Azure Active Directory enables you to view and restore all changes, both on premises or in the cloud, from a single console.

Perhaps the most valuable feature of Recovery Manager for Active Directory Forest Edition is its ability to automate the creation of a virtual forest test lab with production data to test disaster scenarios and safely perform testing prior to making changes in the production domain or forest.

Recovery Manager for Active Directory Forest Edition enables organizations to address all of their disaster recovery challenges, including domain and forest recovery.

WHAT FUNCTIONALITY DOES ON DEMAND RECOVERY FOR AZURE ACTIVE DIRECTORY OFFER?

Quest also provides superior recovery functionality for your Azure AD environment. On Demand Recovery for Azure Active Directory includes the following key features:

Hybrid AD and Azure AD recovery dashboard

With Quest On Demand Recovery for Azure AD, you get a single recovery dashboard to differentiate hybrid and cloud-only objects, run difference reports between production and real-time backups, and restore all changes, whether on premises or in Azure AD.

Secure Azure AD and Office 365 backups

You can back up Azure AD and Office 365 users, attributes, groups and group membership, easily and securely. Plus, you can choose the backup retention period that best meets your company's compliance needs, so you never have to worry about not getting back what you need.

Azure AD and Office 365 bulk restores

On Demand Recovery for Azure Active Directory enables you to restore multiple users, groups (including nested groups) and group membership at the same time — with no PowerShell scripting needed. You'll be able to recover objects far faster than before (in minutes rather than hours) without having to access multiple admin interfaces in Office 365 or Azure AD.

Difference reporting

You can search or compare specific attributes from multiple sources that were modified and roll back only those changes rather than restore the entire object. You can also report on all changes made across Azure AD and highlight differences between backups and the live environment, and perform restores directly from the reporting interface.

Recovery of hard-deleted objects

On Demand Recovery for Azure Active Directory can recreate hard-deleted objects that have bypassed the Recycle Bin and Azure AD groups, which never make it to the Recycle Bin to start with. Now, you can easily restore anything that has been deleted, either accidentally or maliciously.

On Demand Recovery for Azure Active Directory enables you to view and restore all changes, both on premises or in the cloud, from a single console.

FEATURE COMPARISON

	Recovery Manager for Active Directory and Forest Edition	On Demand Recovery for Azure Active Directory	Windows Server 2003, 2008 (no AD Recycle Bin)	AD Recycle Bin (Windows Server 2008 R2, 2012 and 2016)	Microsoft Azure AD Recycle Bin
Environment changes					
Requires permanently enabling the AD Recycle Bin	No	N/A	Yes	Yes	N/A
Requires upgrade to forest functional mode	No	N/A	Yes	Yes	N/A
Undelete features					
GUI for viewing deleted objects	Yes	Yes	No	Yes	Yes (the Office 365 portal)
Undelete deleted objects	Yes	Yes	Partially (attribute values lost)	Yes	Yes
Hierarchical view of deleted objects	Yes	Yes	No	No	No
Delegation of undelete tasks	Yes	No	No	No	No
Identify deleted objects, including hierarchy	Yes (comparison report)	Yes (comparison report)	No	No	No
Undelete containers with child objects	Yes	Yes	No (requires other tools to see hierarchy)	No (requires other tools to see hierarchy)	No
Average time to identify object and undelete it	< 10 minutes	<5 minutes	> 30 minutes	> 10 minutes	>5 minutes
Restore features					
Restore a single user object from backup	Yes	Yes	No UI	No UI	No, only from Recycle Bin
Restore Azure AD groups and group membership	N/A	Yes	N/A	N/A	No
Restore Office 365 groups and group membership	N/A	Yes	N/A	N/A	Yes (using PowerShell)
Granular (attribute-level) restore of one or more objects from backup	Yes	Yes	No	No	No
Restore containers with all child objects	Yes	Yes	No UI	No UI	No
Average time to identify object and undelete it	< 10 minutes	<5 minutes	> 30 minutes	> 30 minutes	>5 minutes
Restore one or more GPOs	Yes	N/A	No UI; all links will be lost	Yes, but all links will be lost	N/A
Restore indefinitely	Yes	Yes	No	No	No; only for 30 days
Restore with PowerShell API	Yes	Yes	No	No	Some restore functions are available
Restore across multiple cloud tenants (databases)	N/A	Yes	N/A	N/A	No
Restore full DC in offline mode	Yes	N/A	Yes	Yes	N/A

	Recovery Manager for Active Directory and Forest Edition	On Demand Recovery for Azure Active Directory	Windows Server 2003, 2008 (no AD Recycle Bin)	AD Recycle Bin (Windows Server 2008 R2, 2012 and 2016)	Microsoft Azure AD Recycle Bin
Monitoring and analysis features					
Identify which objects have been changed or deleted between backups	Yes	Yes	No	No	No
Detect password change for a user object	Yes	Yes	No	No	No
Find the exact event of an object's modification or deletion	Yes	Yes	No	No	No
Monitor backup process	Yes, from RMAD or SCOM	Yes	No	No	No
Backup features					
Back up automatically on schedule	Yes	Yes, hourly	Yes	Yes	No backup ability
Centralize administration of backup and recovery	Yes	Yes	No	No	No backup ability
Back up AD state at specific point in time	Yes	Yes	Yes	Yes	No backup ability
Protect backups with passwords	Yes	Yes	No	No	No backup ability
Other features					
Restore functionality can be used from native UI	Yes (Active Directory Users and Computers [ADUC])	N/A	N/A	N/A	N/A
Restore objects deleted from Recycle Bin	Yes	Yes	N/A	Via PowerShell	No
GUI for AD Lightweight Directory Services (LDS) backup and granular recovery	Yes	N/A	No	No	N/A
Forest recovery features					
Automate domain and forest recovery	Yes	N/A	No	No	N/A
Create virtual environment with production data	Yes	N/A	No	No	N/A

CONCLUSION

The AD Recycle Bin is a handy tool for restoring accidentally deleted objects in some situations, and a vast improvement over tombstoning. Similarly, the Azure AD Recycle Bin enables recovery of deleted Azure AD or Office 365 users, provided certain conditions are met.

But neither Recycle Bin should be mistaken for an enterprise recovery solution. Active Directory, whether on premises or in the cloud, is vital to your business, so you need to be able to quickly restore far more than single objects that were recently deleted. You also need to be able to granularly restore object attributes or even your entire AD forest; extend the recovery window to meet your business needs; proactively identify objects that were changed or deleted between backups; restore Azure AD and Office 365 groups and group membership; and much more.

The Recycle Bin is handy, but it should not be mistaken for an enterprise recovery solution. Get the comprehensive functionality you need with Quest backup and recovery solutions.

To learn more or download your free trial, please visit our website:

- **Recovery Manager for Active Directory —** quest.com/products/recovery-manager-for-active-directory
- **Recovery Manager for Active Directory Forest Edition —** quest.com/products/recovery-manager-for-active-directory-forest-edition
- **On Demand Recovery for Azure Active Directory —** quest.com/products/on-demand-recovery-for-azure-active-directory

The Recycle Bin is handy, but it should not be mistaken for an enterprise recovery solution. Get the comprehensive functionality you need with Quest backup and recovery solutions.

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