Recovery Manager for Active Directory Disaster Recovery Edition

Back up Active Directory and quickly recover AD from any disaster.

With 69 percent of companies suffering a ransomware attack in 2020, and an average downtime of 21 days, it's clear that ransomware is a major risk to every organization. You need to ensure you can get your business back up and running as quickly and securely as possible. With Quest® Recovery Manager for Active Directory Disaster Recovery Edition, you can prepare for and quickly recover AD from any mistakes, corruption or cyberattacks.

Following a ransomware attack, you must restore AD first before anything else. According to Gartner, "The restore process from many well-documented ransomware attacks has been hindered by not having an intact Active Directory restore process."[1]

With Recovery Manager for Active Directory Disaster Recovery Edition, you can easily back up Active Directory, and you'll have multiple recovery options to fit the needs of your business continuity plan. It's like an insurance policy for your AD that you just can't afford not to have.

Quest delivers unmatched flexibility and options, and complete AD backup and recovery at the attribute and object level, directory level and operating system level across the entire forest.

STREAMLINED AD RECOVERY FROM RANSOMWARE

Reliable AD backups

Back up exactly what you need to recover AD. By omitting extraneous and risky components like boot files and the IIS Metabase, Recovery Manager reduces backup bloat, makes the backup process more efficient and minimizes the places where malware can hide.

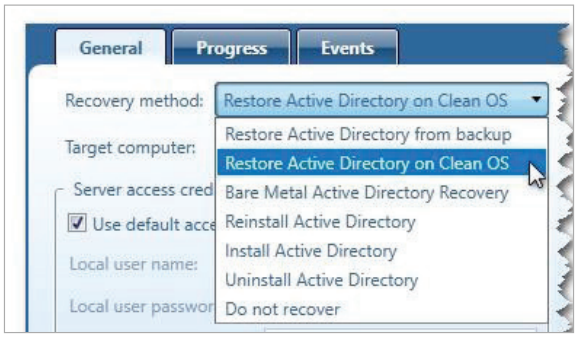
Phased recovery to shorten RTO

After you back up Active Directory, you can shorten recovery time objectives with a phased AD recovery approach. Quickly restore key DCs, enabling sign-in and business-critical functions as soon as possible. Then dramatically accelerate recovery of remaining DCs with automated repromotion methods.

Flexible AD recovery options

Choose the Active Directory disaster recovery method that works best in a given situation, whether that's phased recovery, restoring to a clean OS to minimize the risk of malware reinfection or bare metal recovery. You can restore AD to a clean OS on any machine, whether it's a physical machine, on-prem virtual machine or a cloud-hosted VM.

1 Gartner, Inc., "How to Recover From a Ransomware Attack Using Modern Backup Infrastructure," Fintan Quinn, June 4, 2021.



Flexible recovery methods include restoring AD to a clean OS and a Microsoft-compliant bare metal recovery.

> "Being able to restore an AD forest in hours instead days is priceless. Now I can sleep peacefully."
>
> *IT Manager, Telefónica España*

BENEFITS:

- Handle any AD disaster or recovery scenario, from attribute changes to SYSVOL corruption to full AD forest disasters.
- Automate the entire AD forest recovery process, including the 40+ steps outlined in Microsoft's AD forest recovery best practices.
- Choose the best method for your situation, whether that's phased recovery, restoring AD to a clean OS or bare metal recovery.
- Eliminate the risk of malware re-infection throughout your AD recovery, scanning for malware and minimizing its hiding places.
- Protect your backups from malware to withstand the next ransomware attack.
- Rely on a technology partner that has specialized in AD recovery as long as AD has been around and has helped thousands of customers, including 50% of the Fortune 100.

> "There aren't too many tools that are competitive with Recovery Manager, but we compared one other product. The Quest solution was more complete and met more of our needs; the other tool didn't have nearly as many features."
>
> *Johan Lindahl, IT Infrastructure Specialist, Skandia*

Clean OS recovery to the cloud

During an attack, you need to restore to a new machine you can trust. Quickly and easily create Microsoft Azure resources including virtual machines during a forest recovery. This enables you to recover AD to a readily available, secure and cost-effective machine that you can trust is clean from malware.

Malware detection

Eliminate the risk of malware re-infection throughout your AD disaster recovery process. Implement the added safety of regularly checking files for viruses after the backup file is created, during storage when updates are added and before a restore is started with integrated Microsoft's Defender capabilities.

Secure storage

Protect AD backups from malware infection with Secure Storage, a hardened server that is isolated according to IPSec rules with regular checks to confirm backup integrity. Even if you lose your DCs, Tier 1 storage and even your Recovery Manager server, you still have the Secure Storage backup that is hardened and secure to withstand the ransomware attack.

Operating system recovery

Quickly restore your domain controller's operating system without depending on others. Recovery Manager for Active Directory Disaster Recovery Edition gives AD admins more control of the recovery process, saving time and resources by eliminating dependencies on cross-departmental teams.

Virtual test lab

After you back up Active Directory, you can demonstrate and validate your AD disaster recovery plan by building a separate virtual forest test lab with production data to test disaster scenarios and safely test prior to making changes in the production. Automatically generate detailed, time-stamped reports of the recovery process including before/after state of the organization and actions applied to domain controllers.

ADDITIONAL CAPABILITIES

- **Online granular restore —** Restore individual attributes, such as account settings, group memberships 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.
- **Comparison reporting —** Highlight changes made since the last backup by comparing the online state of AD with its backup or by comparing multiple backups. Accelerate recovery by quickly pinpointing deleted or changed objects or attributes. And with Change Auditor you can easily identify who made the changes.
- **AD management and health validation —** Inspect AD for warning signs of possible issues before they become disasters by checking DC accessibility, replication, trusts and user authentication.
- **Recovery console fault tolerance —** With Recovery Manager for Active Directory Disaster Recovery Edition, you can share persistent configuration data between several instances of your recovery consoles so that you can quickly resume the last restore operation in case it was unexpectedly interrupted.
- **Recovery roadmap —** After you back up Active Directory, you can generate a detailed recovery process report, including an overview of every stage of the recovery, to gain a better understanding and more control over the project.
- **Hybrid AD and Azure AD recovery —** A solid on-premises AD recovery plan alone isn't sufficient since so many organizations are making greater use of cloud-only objects such as Azure AD groups, Azure B2B/B2C accounts, conditional access policies and more. With On Demand Recovery, you can quickly and securely back up and recover Azure AD.

ABOUT QUEST

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

DataSheet-MPM-RMAD-DRE-US-LR-68371