

Technical Review

Microsoft Active Directory Disaster? Recover at Least Five Times Faster with Quest Recovery Manager

Date: November 2021 Authors: Jack Poller, Senior Analyst; and Eve Falk, Associate Validation Analyst

Executive Summary

In this ESG Technical Review, ESG validated how Quest Recovery Manager for Active Directory Disaster Recovery Edition (RMADDRE) simplifies, accelerates, and automates backup and recovery of Microsoft Active Directory. We also focused on how using Quest RMADDRE reduces organizational risk in the face of ever-increasing ransomware and other cyberattacks.

What we found. AD is a mission-critical component of the IT infrastructure. When AD fails, either from ransomware, cyberattacks, or catastrophes, the IT environment comes to a grinding halt, which means the entire organization stops working until AD is restored.

Quest RMADDRE automates the manual Active Directory recovery process documented in Microsoft's *Active Directory Forest Recovery Guide*. This onerous, error-prone, and lengthy manual process includes 18 major steps (each with many minor steps) that must be coordinated and synchronized across the entire suite of DCs being recovered. Automating the manual process significantly reduces the opportunity for manual errors.

Quest RMADDRE runs operations in parallel and synchronizes steps as necessary. This significantly accelerates the process and reduces the time to recover from an AD failure. Quest offers a wide variety of backup and recovery options, providing flexibility, speed, efficiency, and risk reduction for both backup and recovery operations.

Using RMADDRE can reduce risk, as the solution can scan backups for malware. In addition, RMADDRE can back up just the Windows components necessary to recover AD to a system with a clean install of Windows Server. This avoids backing up and restoring malware hiding in boot sectors, temporary directories, or system directories, and results in smaller, faster backups.

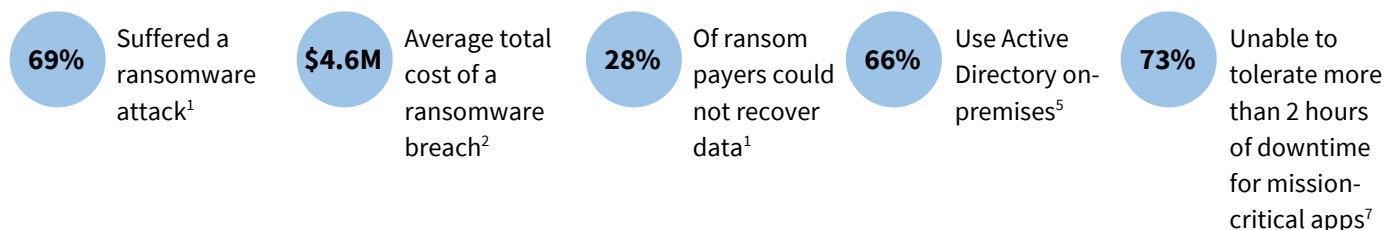
With Quest Recovery Manager, organizations can further accelerate the recovery process by first recovering the bare minimum number of DCs needed for proper operations. Once AD is operational, the teams responsible for recovering business applications, databases, and files can begin their recovery operations while the AD recovery team works in parallel to increase AD forest performance and capacity.

If your organization is looking to reduce risk from ransomware, cyberattacks, or catastrophic failures to AD by automating and simplifying AD backup and recovery, then ESG believes that you should give serious consideration to Quest Recovery Manager for Active Directory Disaster Recovery Edition.

ESG-validated Benefits

- **Performance:** Recovering AD with Quest RMADDRE was at least 5 times faster than the manual process. Large environments with hundreds of DCs may require days to manually recover AD versus just a few hours when using Quest RMADDRE.
- **Automation:** Automating the process drastically reduced the amount of keyboard interaction and concomitant risk of human error.
- **Reduced Risk:** By avoiding backing up non-critical files and directories, and scanning for malware during backup and recovery, Quest RMADDRE reduces the possibility of reintroducing malware during recovery operations.
- **Flexibility:** Recovering to a clean OS install and implementing a two-phase recovery process provides flexibility while simultaneously accelerating time to recovery.

The Challenges



Cyber-criminals are increasing in sophistication, gaining knowledge through experience, developing stealthy attacks targeting existing and new vulnerabilities, and leveraging the supply chain. With increasing sophistication comes increased success: in 2020, 86% of organizations were compromised by successful cyberattacks, up 5.5% from 2019. For many criminals, ransomware has become a favorite tactic, and 69% of organizations have fallen victim to ransomware.¹

With a \$4.62 million average total cost of a ransomware breach.² 57% of organizations gambled on recovering their data by paying the ransom.³ Unfortunately, that was a bad bet for 28% of those organizations that could **not** successfully recover despite ransoming their data.⁴

According to ESG research, 66% of organizations use Active Directory (AD) to manage access to on-premises storage systems⁵ and the ransomware problem is even worse for these organizations. Active Directory is the backbone of an organization's IT infrastructure, acting as the single source of truth for identities and permissions for systems, services, and people. When Active Directory is compromised by malware, or by human error, machine failure, or natural disasters, the organization's entire IT environment comes to a halt. The entire workforce is prevented from logging in, applications cannot run, and all work comes to a dead stop until AD services are restored.

For the 66% of organizations that use AD to manage access to on-premises systems,⁶ AD is a mission-critical application. And, according to ESG research, almost three-quarters (73%) of organizations are unable to tolerate more than two hours of downtime for mission-critical applications.⁷ Thus, it is imperative that organizations ensure that they can back up and quickly recover AD systems and data to protect from lost employee productivity, customer confidence, revenue, and more.

The Solution: Quest Recovery Manager for Active Directory Disaster Recovery Edition

Quest designed Recovery Manager for Active Directory Disaster Recovery Edition to help organizations backup and rapidly recover their AD infrastructure after a ransomware attack or disaster that cripples AD services. Because AD is the single source of truth for identity and access, it needs to be one of the first services recovered after a disaster.

Microsoft's [Active Directory Forest Recovery Guide](#) "contains best-practice recommendations for recovering an Active Directory forest if forest-wide failure renders all domain controllers (DCs) in the forest incapable of functioning normally." Microsoft designed the guide to serve as a backup and recovery template and encourage organizations to customize the plan to the organization's AD deployment. While originally a standalone 43 page document, Microsoft now publishes the guide as a set of a linked web pages encompassing 18 major steps, each of which involves a complicated set of actions that must be coordinated and synchronized across the entire suite of DCs being recovered.

¹ Source: CyberEdge Group, [2021 Cyberthreat Defense Report](#).

² Source: IBM Security, [Cost of a Data Breach Report 2021](#).

³ Source: CyberEdge Group, [2021 Cyberthreat Defense Report](#).

⁴ Source: CyberEdge Group, [2021 Cyberthreat Defense Report](#).

⁵ Source: ESG Master Survey Results, [Trends in IAM: Cloud-driven Identities](#), December 2020.

⁶ Source: ESG Master Survey Results, [Trends in IAM: Cloud-driven Identities](#), December 2020.

⁷ Source: ESG Research Report, [Real-world SLAs and Availability Requirements](#), October 2020.

Quest Recovery Manager for Active Directory automates, coordinates, and synchronizes the activities documented in Microsoft’s backup and recovery guidance. Organizations using Recovery Manager can customize, automate, simplify, and accelerate the onerous and arduous AD recovery process. Automating the process removes the human element and the potential for error, thereby decreasing organizational risk and ensuring normal operations resume as quickly as possible.

Key features of Quest RMADDRE include:

- **Automation.** Quest Recovery Manager automates the complex recovery process, removing the element of human error. RMADDRE runs operations in parallel and synchronizes tasks when necessary, simplifying and accelerating the recovery process.
- **Flexibility and choice.** RMADDRE offers a wide variety of options, from a Clean OS recovery method to bare metal. Organizations can simply remove a DC from the directory, promote in a replacement, force demote and/or re-promote it at any time. Admins can configure “pauses” at each stage of the recovery to verify or make configuration changes before continuing the process. And RMADDRE ensures that all critical roles and functions are healthy and available before confirming a successful recovery.
- **Increased security.** Recovery to clean OS systems reduces the footprint where undetected malware may be hiding, reducing the possibility of reinfecting AD from backups. Automated malware scanning enables scanning backups just before recovery.
- **Increased efficiency and reliability of AD backups.** Quest has analyzed Microsoft’s native System State backups and removed any elements that are *not* necessary for AD recovery. This reduces the size of the backup set, increasing efficiency and reliability, and prevents backing up malware hiding in system storage.
- **Avoidance of malware reinfection.** RMADDRE can scan for malware during both backup and recovery processes, reducing the possibility of malware reinfection.
- **Phased recovery to shorten recovery time objective (RTO).** Quest Recovery Manager enables organizations to recover their AD in phases. Quickly recovering the most critical domain controllers (DCs) first enables organizations to start recovery of dependent services and quickly enable employee access to key applications. Organizations can increase AD capacity, availability, and reliability by recovering or adding DCs in subsequent phases.
- **Encrypted AD backups.** RMADDRE can encrypt backups to prevent malicious actors from accessing sensitive information such as passwords.
- **Protected AD backups.** Quest Secure Storage is a hardened server that is completely isolated using IPSec rules with checks to confirm backup integrity. Even if an organization suffers a ransomware attack or loses the DCs, tier-1 storage, or the Recovery Manager server, the organization will still be able to recover using the protected backups in Secure Storage.



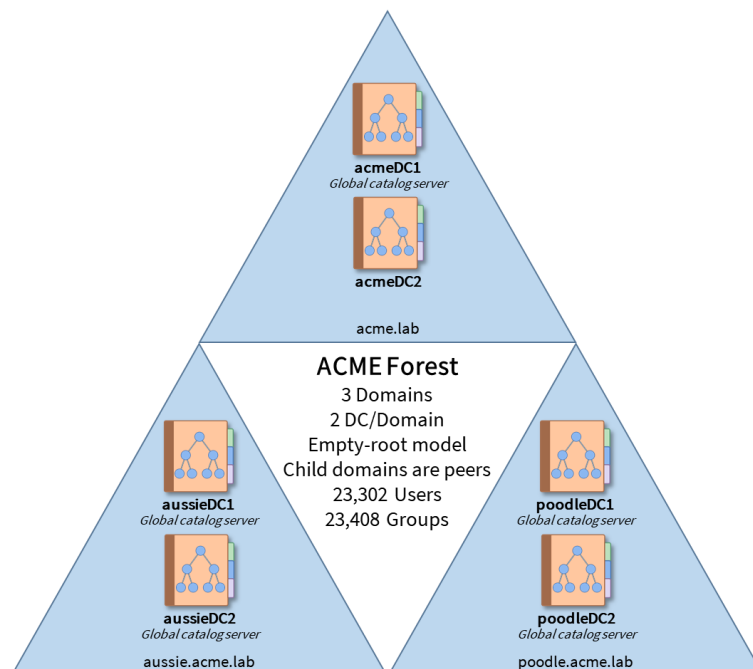
ESG Validated

ESG validated Quest RMADDRE using a remote virtual test bed. The validation was designed to demonstrate how Quest RMADDRE automates, accelerates, and simplifies the onerous, error-prone, and time-consuming task of manually backing up and recovering an Active Directory forest.

The test bed was implemented in a virtual environment, and all DCs were instantiated on virtual machines. The forest included three domains: the root domain acme.lab with two child domains, aussie.acme.lab and poodle.acme.lab. Two DCs were instantiated for each domain. The root domain was essentially empty, containing approximately five users and 50 groups. Each child domain had approximately 10,000 users and 11,500 groups. In total, there were 20,302 users and 23,408 groups in the forest.

Following the Microsoft AD Forest Recovery Guide, ESG took the following steps for both manual backup and recovery and Quest RMADDRE automated backup and recovery:

1. Back up each DC in the forest.
2. Simulate a disaster by destroying all VMs in the forest.
3. Simulate a recovery by creating new VMs.
4. Recover three DCs, one for each domain, from backup to bare metal VMs.
5. For Quest RMADDRE, recover three DCs, one for each domain, from backup to clean OS VMs.
6. For Quest RMADDRE, perform a second phase of recovery, installing AD from media to new Windows Servers VMs.



Manual Backup of the AD Forest

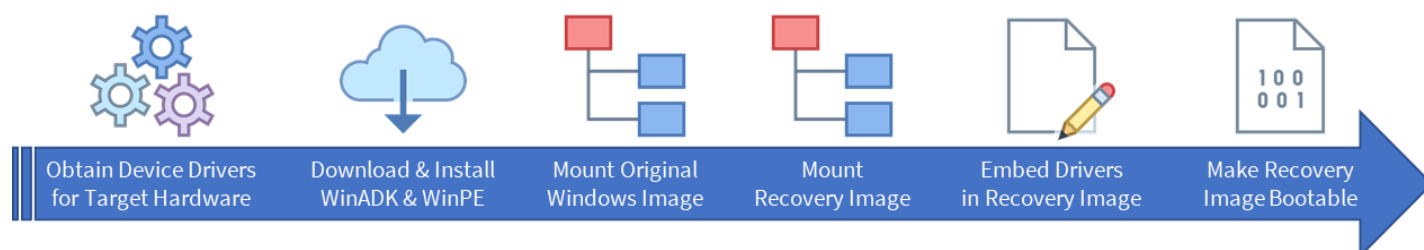
ESG created a customized version of the Microsoft Recovery Guide that included the specific actions, command lines, and utilities we would need to back up and recover this environment. To recover the forest, we needed complete backups of one DC from each domain in the forest.

ESG began by backing up the primary DCs of the three domains: acmeDC1, aussieDC1, and poodleDC1. First, we installed the Windows Server backup feature on each DC. Next, we forced AD replication to ensure that every DC was synchronized with its partner DCs. Then, we started the backup using both the command line and the Windows Backup Once Wizard.

Windows Backup is an OS-level backup and makes a complete copy of the OS installation, including the entire contents of the disk drives. We stored the backups on another Windows Server, and each DC took 25 minutes to complete the process. We noted that in a real-world environment, organizations must ensure that their backups are accessible during the recovery process.

Creating a Custom WinRE Image

When recovering to a bare metal server, the target server needs to be booted from the Windows installation media to access the *Repair your computer* option. However, the Windows installation media most likely does not contain the correct device drivers, language packs, custom utilities, windows updates, and other software necessary for the target computer. Thus, as part of the recovery process, administrators need to build a customized Windows recovery environment (WinRE) that can be used to boot the target server. This multi-step [process](#) required us to obtain device drivers for the target server, download and install WinADK and WinPE, and then execute a series of command lines to build a customized WinRE image.

Figure 1. Create a Custom Windows Server Recovery Image

Source: Enterprise Strategy Group

Because our test bed target servers were identical VMs, we only had to perform this 60-minute process once. In a production environment, administrators need to build a separate WinRE image for each target server with different hardware.

Why This Matters

When hit with catastrophic failures, it is likely that the organization will have to acquire new hardware to host the recovered DCs, and thus will need to create a Windows recovery environment image for each system. Even when using existing systems, the best practice is to create WinRE images as part of the recovery process to ensure all drivers and software are correct and up to date.

While necessary, creating custom WinRE images is onerous, slow, prone to errors, and lengthens the already long manual recovery effort.

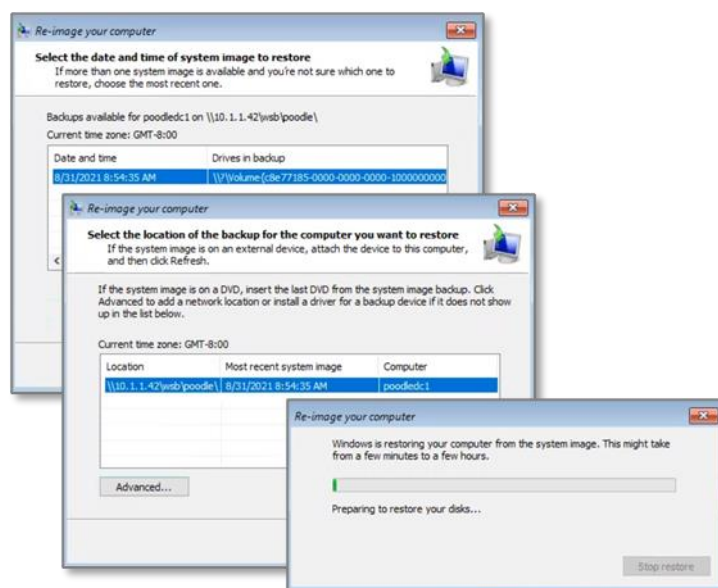
Manual Recovery of the AD Forest

Manual recovery of the AD forest is a four-step process. In the first step, we created customized Windows recovery environment images. Next, we booted the target servers and restored the systems from the backups. In the third step, we reconfigured AD, and in the fourth step, we verified AD replication and that all DCs were correctly synchronized.

We simulated a catastrophic failure by destroying the six VMs running the six DCs in the AD forest.

Next, we started the second step of recovery by instantiating three new VMs to be the replacement server hardware. We booted these VMs using the customized WinRE image we created after the backup process.

When booting from the WinRE image into recovery mode, networking is disabled. However, we needed to enable networking to access the backup images. Using the repair your computer option, we started a command shell, started and configured networking, and then verified we could access the backup server. Next, we started the Windows system image recovery processes and restored each DC image from backups. Configuring the environment and starting the image recovery required 10 minutes of direct interaction and an additional 25 minutes waiting for the restoration process to complete.



In the test bed, we had remote access to the system consoles via the virtualization environment and started to monitor the restoration processes for all three DCs in parallel. In a production environment, typically with geographically dispersed DCs,

admins would need to have direct access to the consoles and coordinate the multiple administrators and activities, and remote access may be degraded because AD has failed. This increases the difficulty and probability for errors in an already difficult and error-prone process.

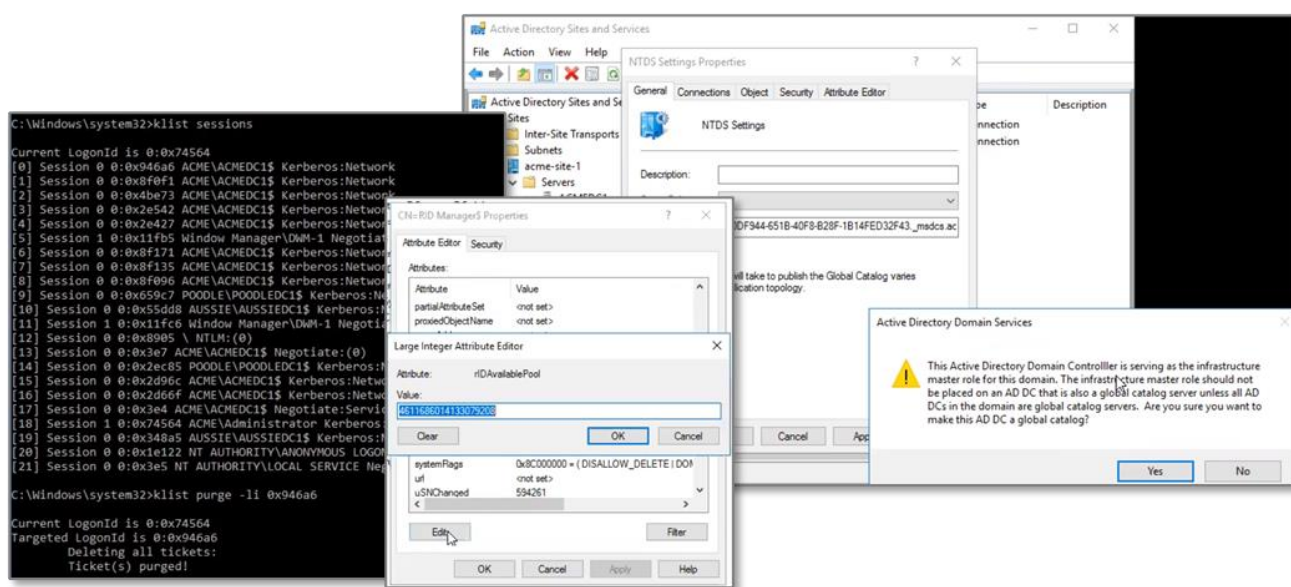
The third step, reconfiguring AD, cannot be started until at least one DC per domain has been restored and rebooted and has network connectivity. In a production environment, the DCs being recovered should remain isolated from the production network so that a corrupt DC that may still be running cannot communicate with those DCs being recovered. Thus, administrators must manually configure networking, routing, and DNS to provide the requisite network connectivity.

The process for the third step includes:⁸

1. Verify network connectivity and DNS.
2. Reset the DC computer account passwords.
3. Raise the RID pool, invalidating any published RIDs.
4. Seize FSMO roles for the root domain.
5. Seize FSMO roles for all other domains.
6. Clean up the metadata of other DCs.
7. Reset the KRBTGT account password.
8. Reset internal Trust passwords.
9. Validate SYSVOL share is available.
10. Add the Global Catalog.

We had to complete each step in the process on all DCs in the forest before proceeding to the next step. Each step included a complex sequence of actions, some of which were initiated via the command line, others via the GUI, with some requiring both command line and GUI-based tools (see Figure 2).

Figure 2. Reconfiguring AD Post-restoration



Source: Enterprise Strategy Group

Next, we proceeded to the final step of recovering AD by verifying AD replication for each of the DCs. Despite having a detailed, customized guide that included each specific action and command line, we found the process of reconfiguring AD post-restoration to be difficult, error-prone, time-consuming, and frustrating. We invested 30 minutes to reconfigure AD and an additional 30 minutes to verify that AD was replicating properly, and only then could we declare that we had successfully manually recovered the AD forest.

⁸ Refer to Microsoft's [Active Directory Forest Recovery Guide](#) for detailed instructions.

Why This Matters

When AD fails, the entire IT environment stops. For most companies, this means all activity stops until admins restore AD services.

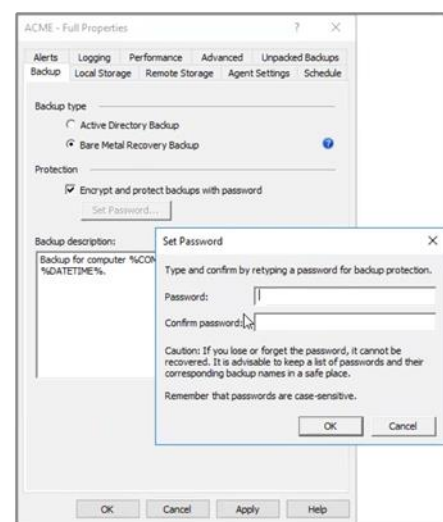
We found the manual AD disaster recovery process to be long, onerous, slow, and prone to errors. Disaster recovery of production environments is exacerbated by the need to recover AD as quickly as possible and the visibility of the failure to the entire company, especially company executives. This puts even more pressure on the admins involved in the disaster recovery process, which inevitably leads to even more human errors, both when entering command lines and in following the process.

Quest RMADDRE Automated Backup

ESG used Quest Recovery Manager to duplicate the manual test bed AD backup and recovery. As with the manual backup and recovery, we began by backing up the primary DCs of the three domains: acmeDC1, aussieDC1, and poodleDC1. We configured Quest RMADDRE, specifying the three DCs and the location for the backups.

We chose to perform a bare metal recovery backup. This is similar to Windows' built-in backup facility, which makes a copy of each disk in the server. Additionally, Quest RMADDRE can increase backup security by encrypting the backup, preventing malicious actors from accessing sensitive data like passwords.

Admins can further increase backup security by storing the backup in Quest's Secure Storage, a hardened server designed to protect items in its vault from corruption due to ransomware attacks or other malicious activities. Secure Storage enables admins to recover AD despite ransomware or losses due to catastrophic failures of the DCs, tier-1 storage, or the Recovery Manager server.



Quest RMADDRE Automated Recovery to Bare Metal

Quest RMADDRE automated recovery of the AD forest to bare metal servers is a three-step process: configure Recovery Manager, verify the configuration (including booting the target servers), and start the recovery process.

First, we simulated a catastrophic failure by destroying the six VMs running the six DCs in the AD forest. Then we instantiated three new VMs to be the replacement server hardware.

Using Recovery Manager, we invoked the AD forest Recovery console, which started a wizard to guide us through configuring Recovery Manager. First, we selected the backup, and the wizard retrieved the forest topology from the backup. Next, we saved the configuration in a password-protected file. This feature enables organizations to preconfigure a recovery project, incorporating key access credentials, to accelerate the forest recovery process.

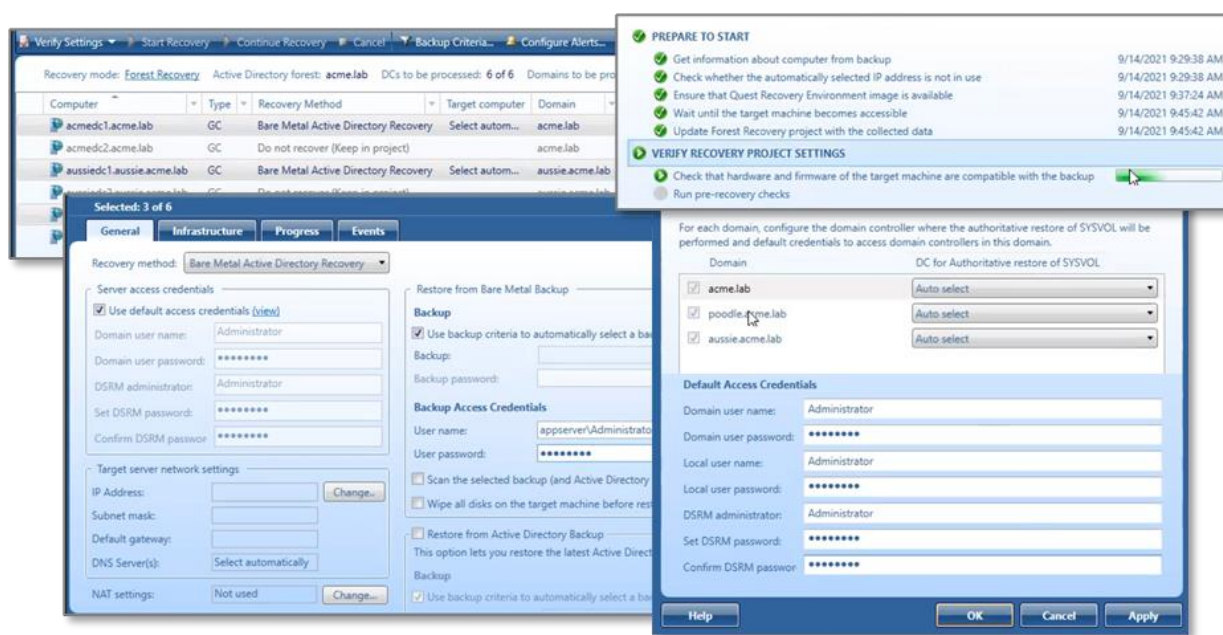
The Forest Recovery Console displayed a list of all Domain Controllers in the forest. As with the manual recovery, we were recovering just the three primary DCs, so we selected the secondary DCs and switched the recovery method from **Bare Metal Active Directory Recovery** to **Do not recover (Keep in project)** as shown in Figure 3. We supplied credentials for accessing the backup server and for each DC's domain user, local user, and DSRM administrator. We could also reset key credentials if they were no longer known or compromised. Quest included an option to wipe all disks on the target machine before restoration and to scan the selected backup for malware during the restoration process.

We started the second step, verification, by clicking **Verify Settings**. Recovery Manager completed numerous verification steps to ensure we could restore the AD forest. As part of the verification process, Recovery Manager automatically created a customized WinRE image specific to each DC.

We booted the new target server VMs using the customized WinRE images, which included the Quest Bare Metal Recovery Console agent. This agent runs at boot time to both automatically configure networking using the original servers' IP addresses and act as a remote access agent, receiving and executing commands from the Recovery Manager Forest Recovery Console. Thus, once we booted the servers, we had no other direct interaction with the server consoles.

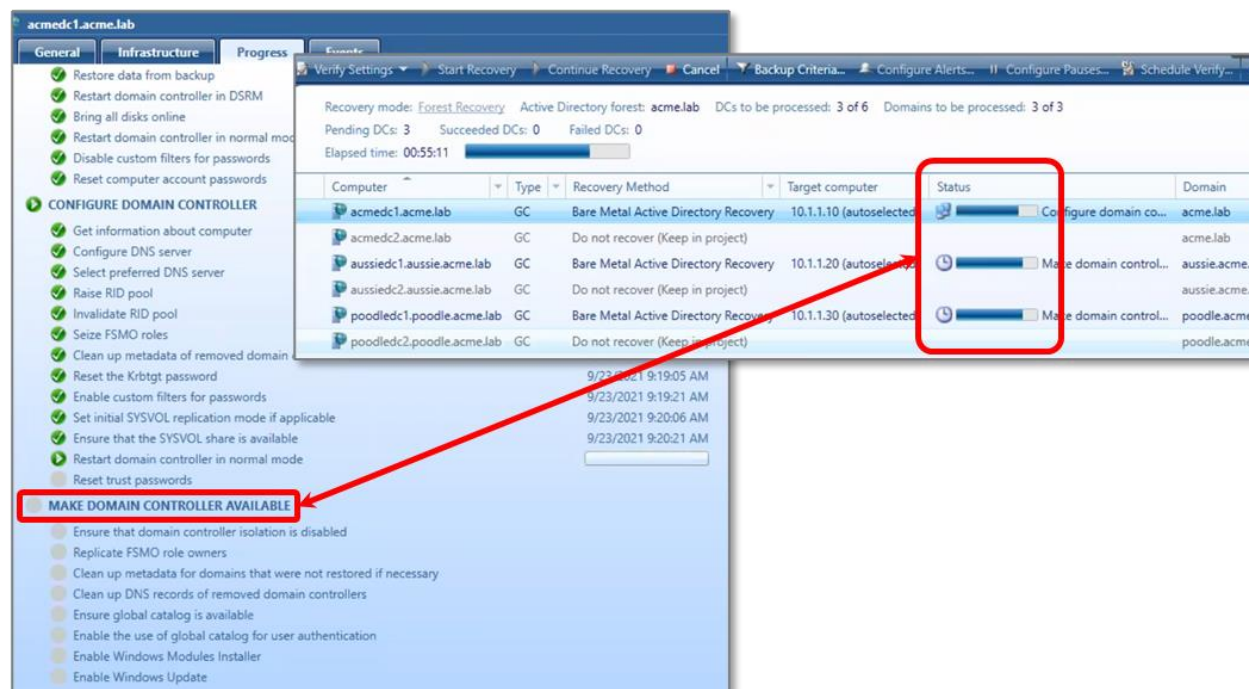
The verification process waited until all target machines were booted and accessible and then executed an additional series of pre-recovery checks and ensured the hardware and firmware of the target machines were compatible with the backup. In total, the verification process took 10 minutes plus the actual time it took to boot the servers.

Figure 3. Configuring RMADDRE to Recover AD Forest to Bare Metal Servers



Source: Enterprise Strategy Group

We started the last step of recovery by clicking on **Start Recovery**, and RMADDRE began the recovery process. As shown in Figure 4, RMADDRE displayed the recovery process. There are multiple points in the process where all servers have to be synchronized before continuing, and RMADDRE displayed a clock to indicate servers were ready and waiting.

Figure 4. RMADDRE Recovery Process with Sync Points

Source: Enterprise Strategy Group

The recovery process for all three bare metal servers completed in 61 minutes. During the entire recovery process, we only monitored the system activity.

Quest RMADDRE Backup and Recovery to Clean OS

We used Recovery Manager to make an Active Directory backup, which makes a copy of just the components necessary to recover AD to a system with a clean install of Windows Server: the AD database itself (ntds.dit file), the AD database log files, SYSVOL (group policy, logon scripts), and necessary parts of the Windows Registry. Unlike bare metal recovery backups or System State backups, Recovery Manager AD backups do not back up the boot sector (which could be compromised by a root-kit virus) or the entire Windows directory (including Windows/temp and Windows/winSxS, which were utilized by the Kaseya supply chain/ransomware attacks in July 2021).

Thus, Recovery manager AD backups are smaller and faster. And Quest can compress AD backups. We noted that for our environment, Quest compressed the backups to approximately 25% of their actual size.

We destroyed the AD forest and booted three pre-staged systems with clean installations of Windows Server.

We used Recovery Manager to create a new recovery project, specifying **Restore Active Directory on Clean OS** for each of the three primary DCs. We provided the IP address for each server and requisite credentials and then verified the project settings. The verification completed in eight minutes, and during the process, Recovery Manager installed the agent on the target systems.

We selected **Start Recovery** and waited 31 minutes for the recovery process to complete.

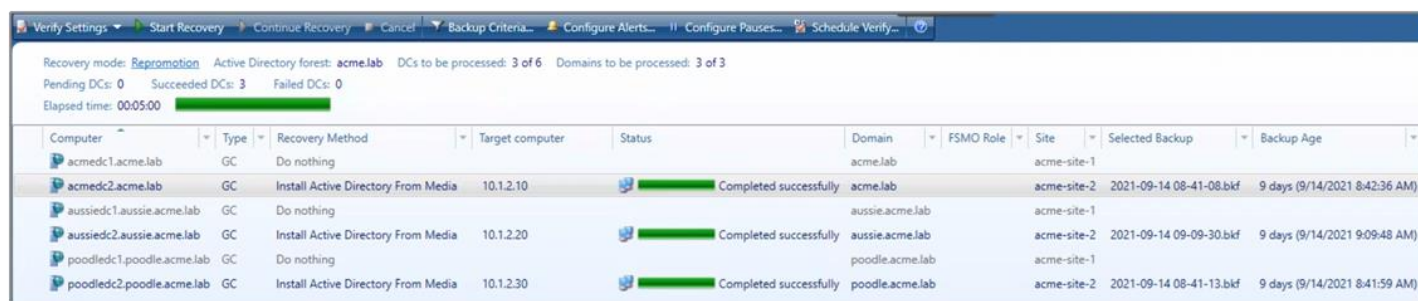
Two-phased AD Forest Recovery

Quest RMADDRE enables organizations to accelerate the recovery of the infrastructure by splitting the forest recovery process into two phases. In the first phase, admins recover the number of DCs needed to support the business' primary operations. Once the first phase is complete, the teams responsible for recovering business applications, databases, and

files can begin their recovery operations while the AD recovery team works in parallel on the second phase of AD forest recovery: increasing the AD forest performance and capacity by promoting groups of Windows Servers to take the place of secondary, remote, or ancillary DCs that were not recovered in the first phase. Admins can run the second phase multiple times to add performance and capacity over time.

As shown in Figure 5, in our environment we promoted three Windows Servers to secondary DCs in just five minutes.

Figure 5. Phase Two: Install AD from Media



Computer	Type	Recovery Method	Target computer	Status	Domain	FSMO Role	Site	Selected Backup	Backup Age
acmedc1.acme.lab	GC	Do nothing			acme.lab		acme-site-1		
acmedc2.acme.lab	GC	Install Active Directory From Media	10.1.2.10	Completed successfully	acme.lab		acme-site-2	2021-09-14 08-41-08.bkf	9 days (9/14/2021 8:42:36 AM)
aussiedc1.aussie.acme.lab	GC	Do nothing			aussie.acme.lab		acme-site-1		
aussiedc2.aussie.acme.lab	GC	Install Active Directory From Media	10.1.2.20	Completed successfully	aussie.acme.lab		acme-site-2	2021-09-14 09-09-30.bkf	9 days (9/14/2021 9:09:48 AM)
poodledc1.poodle.acme.lab	GC	Do nothing			poodle.acme.lab		acme-site-1		
poodledc2.poodle.acme.lab	GC	Install Active Directory From Media	10.1.2.30	Completed successfully	poodle.acme.lab		acme-site-2	2021-09-14 08-41-13.bkf	9 days (9/14/2021 8:41:59 AM)

Source: Enterprise Strategy Group

Time and Risk Reduction Analysis

Using Quest RMADDRE to automate the onerous, error-prone, and long manual process of recovering an Active Directory forest can help an organization quickly and efficiently resume operations after a ransomware, cyberattack, or disaster takes down AD.

The manual recovery process requires often continuous administrator input and interaction and puts an added burden on persistently under-skilled IT departments. According to ESG research, just 7% of organizations indicated that they did not have a problematic shortage of IT skills. Twenty four percent report a shortage of data protection skills, and almost half (48%) report a shortage of cybersecurity skills.⁹ Thus, many organizations are at increased risk of attack and may not have the skills or personnel to protect and recover AD from attacks or other infrastructure failures.

Despite having a comprehensive and customized guide documenting every step, including all command line options, we made numerous errors during our manual recovery efforts. From having to retype command lines after making typos to having to redo multiple steps when we missed a step or performed steps out of order, we made these errors even though we were operating in a demo environment without time pressures or the weight of knowing that the AD failure was preventing everyone in the company from doing their jobs.

Quest RMADDRE simplified and accelerated the process. Once we configured and validated the recovery environment, we selected **Start Recovery**, and simply waited for the process to complete. Quest RMADDRE automation removed the opportunity for human errors, synchronized activities across all DCs, and verified the AD forest was properly recovered.

Using Quest RMADDRE, we further accelerated the process by recovering to clean OS install systems with the added benefit of preventing potential reinfection that comes with restoring malware hidden in system volumes.

Figure 6 graphically represents the manual recovery process outlined in the Microsoft recovery guide, along with the use of Quest RMADDRE to recover to bare metal and to recover to clean OS.

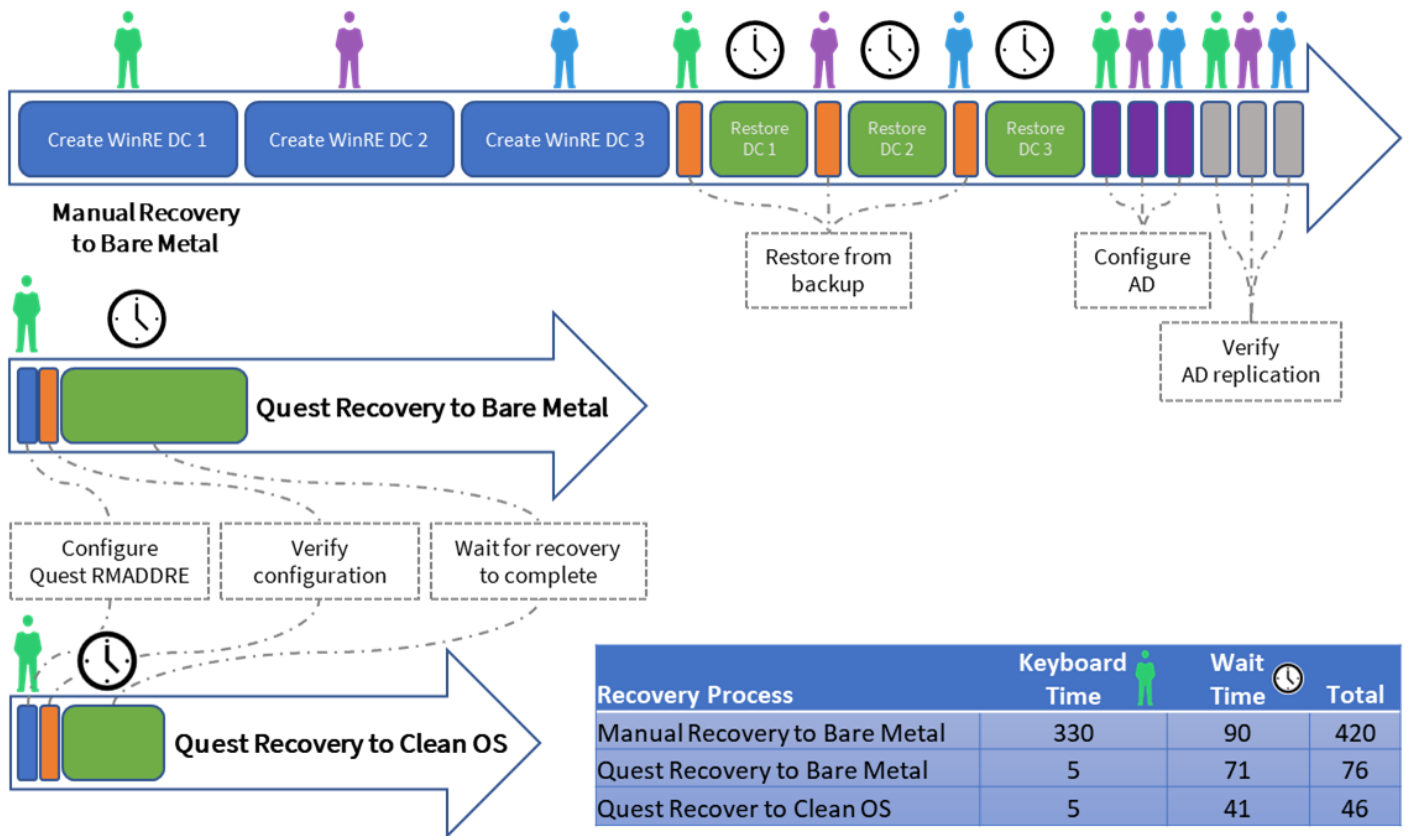
For manual recovery to bare metal servers, we extrapolated from the test environment to a real-world environment, where we would have to create a custom WinRE for each of the three DCs, then sequentially restore each DC, configure AD, and

⁹ Source: ESG Research Report, [2021 Technology Spending Intentions Survey](#), January 2021.

verify replication. This process required 330 minutes of typing at the keyboard and monitoring activity, and 90 minutes waiting for data to be copied from the backup server, for a total of 420 minutes (seven hours).

When using Quest RMADDRE to recover to bare metal or clean OS install servers, we first configured RMADDRE, verified the configuration, and then waited for the process to complete. RMADDRE recovery to bare metal required five minutes of keyboard time and 71 minutes of waiting for a total of 76 minutes (1.25 hours). RMADDRE recovery to clean OS required 5 minutes of keyboard time and 41 minutes of waiting for a total of 46 minutes (0.75 hours).

Figure 6. Time and Effort to Recover AD Forest



Source: Enterprise Strategy Group



Why This Matters

Regardless of whether ransomware, hardware, human error, or a natural disaster is the proximate cause of failure, recovering AD as quickly as possible is the prime directive for IT. Because when AD fails, the entire organization fails.

ESG validated that Quest Recovery Manager for Active Directory Disaster Recovery Edition automated, accelerated, and simplified the AD recovery process. Using Quest, configuring and recovering an AD forest to bare metal servers required just 5 minutes of keyboard time at the beginning of the process, and completed in just 1.25 hours. Overall, using Quest eliminated most of the 5.5 hours of manual interactive keyboard time scattered across the 7 hours of recovery time. Using Quest RMADDRE was more than five times faster than manually recovering AD, and organizations can further accelerate the process by using Quest's ability to recover to a clean OS install.

Organizations can extrapolate from these results estimates of the time and effort required to recover their AD environments. When manually recovering AD, admins must restore at least one DC per domain from backup before attempting to configure and recover AD. Larger environments with more DCs require more time, more people, and more coordination across data centers and time zones. The same is true for the AD configuration and verification process. More DCs introduce more time, more coordination and synchronization, and more possibility for human error. It is reasonable to assume that each additional DC in the environment adds at least an equal amount of time to the recovery process.

As Quest RMADDRE automatically runs operations in parallel and automatically synchronizes each operation across all DCs, the recovery time is not highly dependent on the number of DCs in the environment. This is borne out in the real world, where Quest has documented multiple instances where RMADDRE reduced recovery time from days to a few hours.

The Bigger Truth

According to ESG research, 82% of organizations claim that cyber-risk has increased over the past two years due to factors like an increase in cyber-threats, greater integration of technology within the business, and a growing attack surface.¹⁰ Cyber-risk, human errors, hardware failures, and natural disasters, among other factors, ensure that no organization is safe from catastrophic AD disasters. Organizations must recover from AD failures as soon as possible so as not to lose time, money, or reputation.

Quest designed Recovery Manager for Active Directory Disaster Recovery Edition to help organizations quickly recover from an AD disaster. The solution automates and verifies the process and provides flexibility, enabling organizations to recover to bare metal servers or clean OS install servers. Quest also enables admins to recover in two phases: first, recovering at least one DC per domain; second, recovering or adding DCs from installation media. The two-phase recovery ensures organizations can resume operations as soon as possible and then add DCs for increased capacity and resiliency.

ESG validated that:

- Quest RMADDRE automated and accelerated the manual recovery process recommended by Microsoft and documented in Microsoft's *Active Directory Forest Recovery Guide*. This onerous process consists of 18 major steps, each of which involves a complicated set of actions that must be coordinated and synchronized across the entire suite of DCs being recovered.
- Quest RMADDRE significantly reduced the opportunity for human error. We configured and verified the recovery configuration before proceeding, and Quest RMADDRE reduced the amount of keyboard interaction from hours scattered throughout the manual process to just minutes at the start of the process.

¹⁰ Source: ESG Research Report, [Cybersecurity in the C-Suite and Boardroom](#), February 2021.

- Quest RMADDRE significantly reduced the time to recover an AD forest. Overall, Quest RMADDRE was more than five times faster than the manual process to recover the test bench AD forest to bare metal servers. ESG believes that each additional DC in the forest increases the manual recovery time and effort. The time to recover using Quest RMADDRE, which runs operations in parallel, will not be greatly affected by the number of DCs. Large environments with hundreds of DCs may require days to manually recover AD versus just a few hours when using Quest RMADDRE.
- The ability to implement a two-phase recovery process and to recover to clean OS install systems provided additional flexibility, reduced the possibility of reintroducing malware during the recovery process, and accelerated the process.

The results that are presented in this document are based on validation in a controlled environment. Due to the many variables in each production data center, it is important to perform planning and testing in your own environment to validate the viability and efficacy of any solution.

If your organization is looking to reduce risk from ransomware, cyberattacks, or catastrophic failures to AD by automating and simplifying AD backup and recovery, then ESG believes that you should give serious consideration to Quest Recovery Manager for Active Directory Disaster Recovery Edition.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.