Be Prepared for Ransomware Attacks with Active Directory Disaster Recovery Planning

Ransomware attacks are skyrocketing. Here's how to reduce your organization's risk.

Quest

Introduction

The urgency of the ransomware threat

Devastating ransomware attacks on critical organizations and infrastructure like JBS and the Colonial Pipeline have escalated ransomware awareness to the highest levels. In fact, due to increasing geopolitical tensions, the Cybersecurity and Infrastructure Security Agency (CISA) has issued a "Shields Up" message to every U.S. organization, including federal agencies, urging them to adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets. In particular, CISA recommends that organizations assess their resilience by testing backup procedures to ensure that critical systems and data can be rapidly restored if your organization is impacted by ransomware or a destructive cyberattack.

There is good reason to be alarmed. Consider these statistics:

- **69%** of organizations were compromised by ransomware.
- Just **8%** of those that paid a ransom got all their data back.
- The average downtime due to a ransomware attack is **21 days**.
- The average cost of remediating a single ransomware attack is **$1.85 million**.
- The total cost of ransomware was **$20.8 billion** — just for US healthcare organizations!

If your business suffered a ransomware attack today, would you be prepared?

Components of a comprehensive ransomware strategy

A comprehensive approach to ransomware requires a defense-in-depth strategy that covers all five functions detailed in the NIST Cybersecurity Framework:

- **Identify —** Understand your organization's current cybersecurity posture, including your physical and software assets and related cybersecurity risks; business context and risk tolerance; current cybersecurity policies and controls; and legal and compliance requirements.
- **Protect —** Limit the risk and impact of cybersecurity events by remediating vulnerabilities, training staff, implementing processes to improve information protection, and strengthening governance and administration.
- **Detect —** Sound the alarm faster on suspicious activity with capabilities like real-time auditing, anomaly detection and alerting.
- **Respond —** Take appropriate action quickly, before damage spreads, with strong communication and forensic analysis.
- **Recover —**Reduce the impact of a security incident by restoring normal operations quickly.

While all of these functions are essential, this white paper focuses on the last one, Recover. It will help you craft the strong Active Directory disaster recovery plan you need and get the flexible recovery options required to execute it quickly and effectively.

Calculating the cost of a ransomware attack

Just how important is the Recover function? One way to quantify it is to tally up the cost of a ransomware attack based on how long it takes to restore normal operations.

Here's a very simple calculation. It includes just three factors: lost employee productivity, lost revenue and the direct costs of restoring IT operations.

The "Example" column is based on the following assumptions:

- Average employee compensation is $65,000/year.
- There are 260 work days per year.
- The company's total yearly revenue is $100M.

To find your cost, simply plug in the appropriate figures for your organization.

> **"Business continuity plans are vital, it's obvious when you say it. But seriously, at whatever level of the organization you are, there are things you can do to plan for the worst. No, literally, the worst. No, worse than that, I mean the absolute worst that you can possibly think of. Plan for that because when it all goes bang, you will seriously thank yourself."**
>
> *Gavin Ashton*
> *Former IAM SME for Maersk during NotPetya ransomware attack*

Lost productivity	Example	Your Numbers
Average daily compensation (salary + benefits)	$250	
Days of downtime	21	
Number of employees unable to work because of the disaster	10,000	
Subtotal	**$52,500,000**	
Lost revenue		
Average daily revenue	$384,615	
Days of downtime	21	
Subtotal	$8,076,915	
Cost of restoring IT operations		
Employee overtime or contractor pay to restore operations	$50,000	
Hardware repairs	$25,000	
Subtotal	$75,000	
Total basic cost of incident	**$60,651,915**	

Table 1. Calculating the cost of a single ransomware attack

Remember that this is a very simplified and conservative estimate. Here are just a few of the additional costs you'll need to tack on for a more accurate calculation:

- If the downtime affects a customer-facing website or application, you'll need to add in the expense of the flood of calls to your customer support teams and the lost revenue stream from frustrated customers turning to your competitors.
- If you're subject to compliance regulations, you'll need to add in the costs of fines and additional audits.
- If customer data is exposed — as ransomware operators are now increasingly doing to strong-arm victims into paying the ransom — you might also face legal fees and costs for remediation measures like free credit monitoring.
- If you choose to pay the ransom, you'll need to add that cost in as well.
- Harder to quantify but potentially the biggest cost is the damage to your organization's reputation. In addition to the customers who turn away immediately, you'll lose revenue from all the prospects who will avoid you in the future. Indeed, you may well struggle for years to rebuild your brand.

It's really no surprise that 40% of enterprises say that a single hour of downtime costs $1 million to over $5 million. In a worst-case scenario, losses can exceed millions of dollars per minute.

The key to a speedy recovery from ransomware: a phased approach with active directory at the center

Active Directory is critical to virtually all IT operations.

Remember the infamous NotPetya attack in 2017? Within hours, this malware brought companies around the world to a standstill, including shipping giant Maersk. While Maersk had backups of many mission-critical servers, no one at the company could locate a single backup of a domain controller (DC) — in other words, a backup of Active Directory. As a result, the company was dead in the water.

> **According to Gartner, you can 'accelerate recovery from attacks by adding a dedicated tool for backup and recovery of Microsoft Active Directory'.**
>
> *Gartner, Inc., "How to Protect Backup Systems From Ransomware Attacks," Nik Simpson, September 21, 2021.*

Active Directory (AD) is the keystone to effective disaster recovery because it's the primary mechanism for authenticating users and enabling access to data and applications. As long as AD is down, employees can't access the tools and information they need to do their jobs, and the business simply cannot function.

For Maersk, the effects of the AD downtime were profound. It wasn't just that employees couldn't log in and do their jobs; the company had to reroute ships, was unable to dock or unload cargo ships in dozens of ports, and could not process new orders. In the end, Maersk was saved only by a stroke of luck: One DC at a remote office had been offline during the attack, and the company was able to painstakingly shuttle that precious machine to its headquarters to enable the AD recovery process.

Clearly, luck is not a strategy. To minimize their risk of devastating financial losses from destructive cyberattacks like ransomware, organizations need a robust backup and disaster recovery plan with Active Directory recovery at its core. As one Gartner analyst succinctly put it: "The restore process from many well-documented ransomware attacks has been hindered by not having an intact Active Directory restore process." In addition, Gartner also stated that you can "accelerate recovery from attacks by adding a dedicated tool for backup and recovery of Microsoft Active Directory."[2]

A phased approach to AD disaster recovery helps shorten RTO objectives.

The Maersk story not only highlights the critical role of AD in disaster recovery, it also illustrates the fastest path to restoring operations. All the IT team needed was to get a single DC online, even if not on the most ideal hardware, to get the rest of the disaster recovery process going. Using the last intact DC, carefully air-lifted out of the remote office, they were able to restore one DC onto a Surface Pro 4.2, and the business began to get back on its feet.

1 Gartner, Inc., "How to Recover From a Ransomware Attack Using Modern Backup Infrastructure," Fintan Quinn, June 4, 2021.
2 Gartner, Inc., "How to Protect Backup Systems From Ransomware Attacks," Nik Simpson, September 21, 2021.attack

> **"The restore process from many well-documented ransomware attacks has been hindered by not having an intact Active Directory restore process."**
>
> *Source: Gartner, Inc., "How to Recover From a Ransomware Attack Using Modern Backup Infrastructure," Fintan Quinn, June 4, 2021.*

A phased approach to AD recovery is the Microsoft recommended best practice for AD forest recovery, and it is the quickest way to get your business on its feet again after a ransomware attack. At a high level, the strategy is to identify at least one DC in each domain to prioritize in a recovery scenario. Get those DCs back online quickly, and then turn your attention to the less critical DCs:

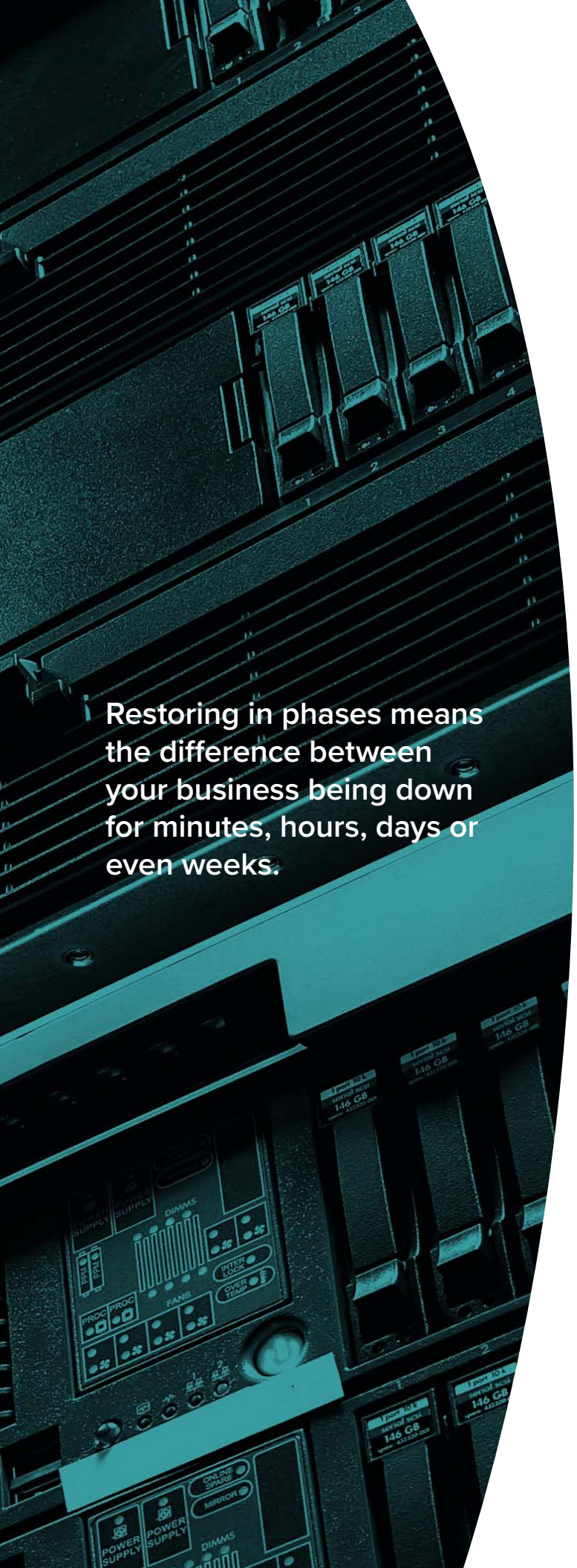
- Phase 1: Perform initial recovery. Perform restore of one or several domain controllers in each domain.
- Phase 2: Redeploy remaining DCs. Restore remaining domain controllers through promotion.

Restoring in phases means the difference between your business being down for minutes, hours, days or even weeks.

For example, using the Quest AD disaster recovery solution, you can restore a DC in less than one hour, enabling critical operations to resume while you complete the rest of the recovery.

Diving into the details

Let's review exactly what's involved in a phased approach to AD disaster recovery.



Prerequisite: Good backups

As the Maersk story dramatically illustrates, disaster recovery depends on having a solid backup of Active Directory. There are actually three types of backups to know about:

- **Active Directory backups —** Active Directory backups are the foundation for Active Directory recovery, whether you need to restore a single object, attribute or DC, or you need full-on disaster recovery of an entire forest. AD backups involve a variety of components from Active Directory domain controllers, including the NTDS directory, SYSVOL (which contains Group Policy and logon scripts) and aspects of the registry that have to do with AD.

  It should be noted that AD backups are not the same as System State backups, which back up the entire operating system, not just the Active Directory pieces. In fact, System State backups have expanded over the years to include a huge number of files that aren't really related to System State, such as the Internet Information Services (IIS) Metabase, device drivers, DLL cache folder and Volume Shadow Copy Service (VSS) components. Many of these files are not necessary for recovering Active Directory, but they do increase the risk that you'll inadvertently back up (and then restore) an infected file. For more information about why System State backups can be as much a liability as an asset, please see the white paper, "The Varied History of System State Backups and Why You Don't Need Them for AD Recovery."

- **Azure AD backups —** Accidents and malicious activity don't happen just on premises. Therefore, in hybrid AD environments, a complete IT disaster recovery plan must include a backup strategy for cloud-only objects and attributes, which are not adequately protected by native Microsoft tools nor covered by any on-premises AD backup solution.

  For example, suppose you are using Azure AD Conditional Access policies to require an extra form of authentication if a user from outside the corporate network attempts to access a sensitive

Quest

application and to block access entirely from certain IP addresses — but then you discover that the authentication controls you want are no longer in place for that application. To fix the problem, you need to understand the root issue. Is the application no longer associated with the proper Conditional Access policy? Has the policy changed? Has the security group that controls who the Conditional Access policy applies to changed? However, the Recycle Bin offers no benefit here, since it is for deleted objects only; improper modifications to objects are not stored in the Recycle Bin and therefore cannot be recovered from it. To ensure you can restore any object that might be improperly changed, you'll need complete, current documentation of the configuration of all your Azure AD objects — which is virtually impossible to create and maintain using manual methods.

- **Bare metal recovery (BMR) backups —** Bare metal recovery enables you to restore your Active Directory forest to different hardware instances. This is particularly valuable in case of physical corruption of domain controllers, domain data or services due to a ransomware attack. If you have the authority to back up and restore your entire AD server, you can restore your Active Directory forest to different hardware instances using your BMR backup combined with the standard AD backup.

  Of course, you also need to ensure that your backups are intact and usable. Microsoft recommends following the 3-2-1 rule: Keep three backups of your data on two different storage types, and keep at least one backup offsite.

Phase 1: Restore one DC in each domain (preferably using clean OS recovery).

The first step is to get your organization up and limping, if not fully running. That means restoring one DC in each domain. Your options depend on what tools you have. The preferred method for ransomware recovery is clean operating system (OS) recovery, but it's available only if you've invested in an enterprise AD disaster recovery solution like Recovery Manager Disaster Recovery Edition from Quest.

Why is clean OS recovery superior to BMR in case of a ransomware attack? The main reason is that BMR restores entire volumes (disk partitions), which includes files that are not part of AD, such as the boot sector, the program files directory, and the Windows and WinSXS directories. This leaves a LOT of places where malware can hide, leaving the organization at risk of still being infected after the recovery operation (see Figure 1). Clean OS recovery, on the other hand, restores only AD components, which drastically reduces the places where malware can hide (see Figure 2).

There are two other factors to consider when choosing a recovery strategy, though. The first is that restoring a BMR backup is difficult. Although the target machine doesn't need an operating system, it does need the same physical disk layout and those disks must be at least as large as the original DC so the same partitions can be laid down just as they were on the original computer. The second is whether you need the additional data stored in the BMR backup. For example, if domain controllers are being used for non-AD-related services (like hosting DNS zones that are not AD-integrated, running a Certificate Authority, or running file and print services), BMR can be the best option.

Restore to clean OS is the preferred method of recovery from ransomware because BMR leaves a LOT of places where malware can hide.

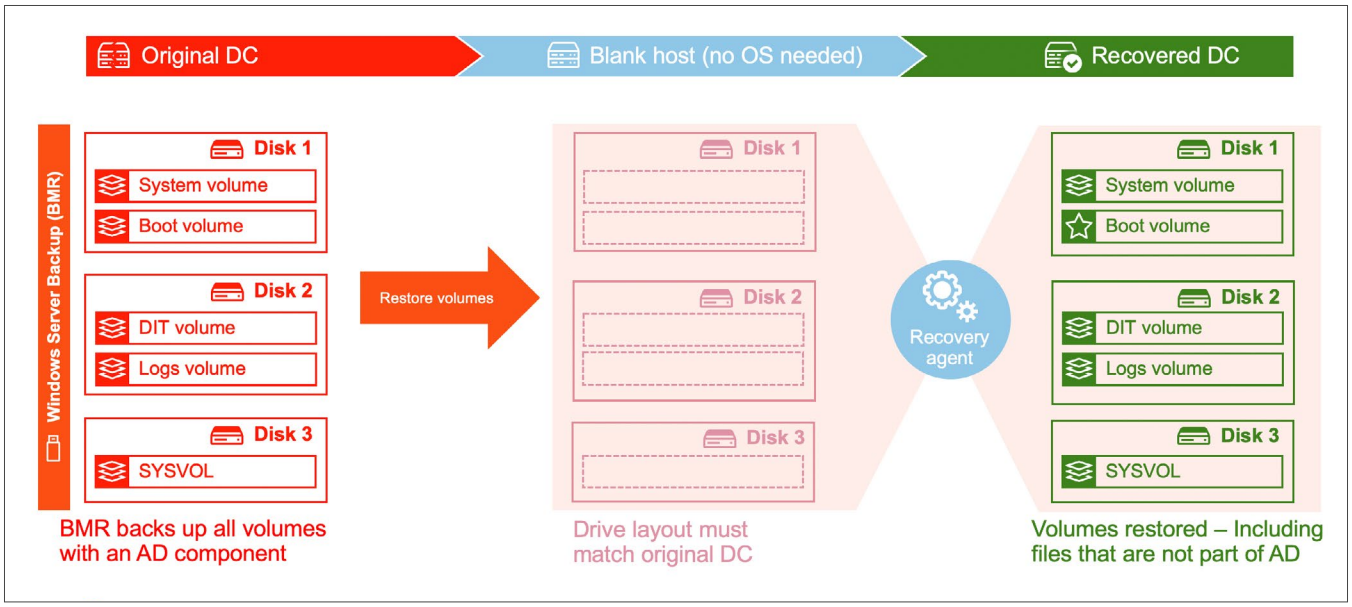


Figure 1. Bare metal recovery leaves a lot of places for malware to hide.

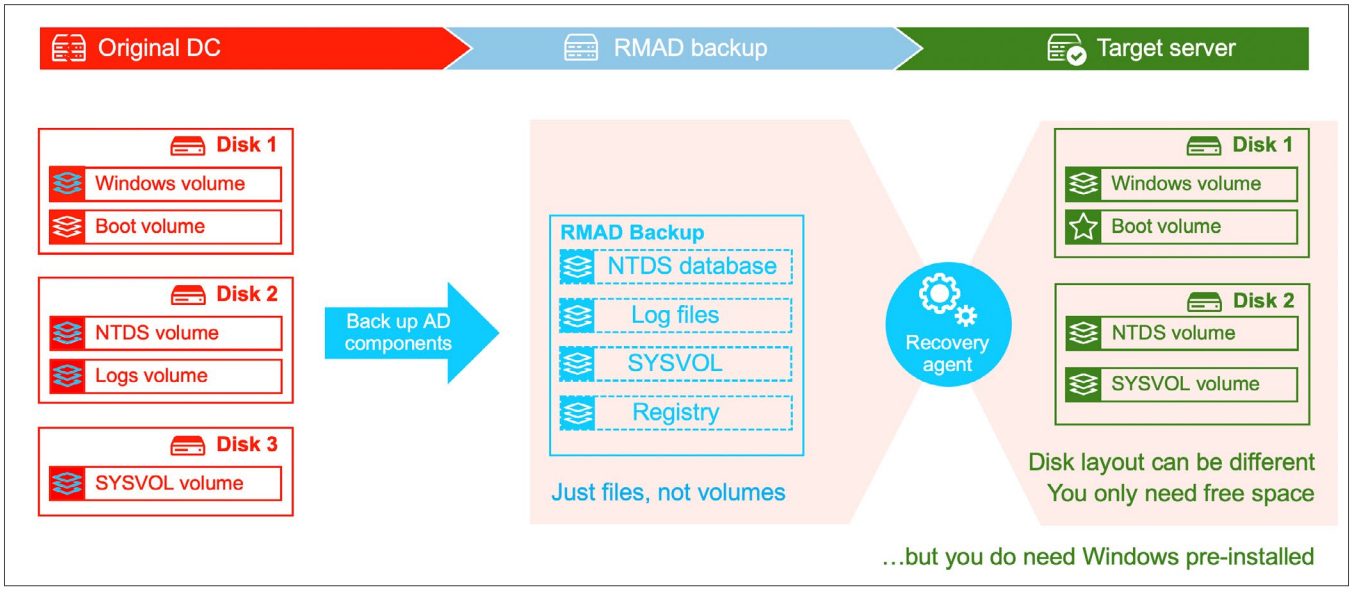


Figure 2. Clean OS recovery (a feature of some third-party solutions) is the preferred option for AD recovery in case of a ransomware attack.

Phase 2: Promote the rest of your DCs (preferably using IFM).

Exactly how should you go about promoting the rest of your DCs? While there are several methods, including replication, the best option by far is install from media (IFM). Microsoft recommends IFM because it is an efficient way to reinstall AD on a domain controller; in fact, it speeds the process considerably by cutting traffic across your network in half. If you were to use replication rather than IFM, the process could easily take 12–36 hours, depending on where your DCs are located.

Using native tools, IFM is a tedious manual process that you have to perform on each DC, one by one, by going to each DC and executing the PowerShell commands to install from media in order to promote the domain controller. A third-party solution can dramatically speed Phase 2 of the recovery and get your organization back up and running much sooner.

Quest

Install from media (IFM) enables you to promote the rest of your domain controllers much faster than other methods.

Choosing the right tools to put your plan into action

Many organizations have a false sense of security around their resilience to destructive ransomware events. Neither native tools nor traditional data protection products are a substitute for an enterprise-grade AD backup and disaster recovery solution, especially in a ransomware scenario. We've touched on a few of the reasons, but it's worth a more thorough review.

Limitations of native tools and manual processes

We've already seen that native tools do not offer the option of using the clean OS recovery method to reduce the risk of ransomware reinfection, and promoting DCs using IFM is slow and tedious. But there are additional drawbacks to native backup and recovery, including the following.

The forest recovery process is long and complicated.

With native tools and manual processes, AD forest recovery is a difficult, time-consuming and error-prone process. In fact, Microsoft's "Active Directory Forest Recovery Guide" document outlines some 40 high-level steps, including:

- Isolate the DCs that you are recovering from the ones you are not recovering or have not yet recovered.
- Reset computer, Kerberos and trust relationship passwords.
- Raise the RID pool by 100k and invalidate current RIDs on each DC before you allow it to be used.
- Rebuild your Global Catalogs.

These steps must be performed on each DC you plan to recover, correctly and in the proper sequence, and the process must be coordinated across the forest. In addition, many of the steps aren't operations that AD administrators are familiar with; they are tedious, often command-line based steps, so it's very easy to make mistakes and have to start over.

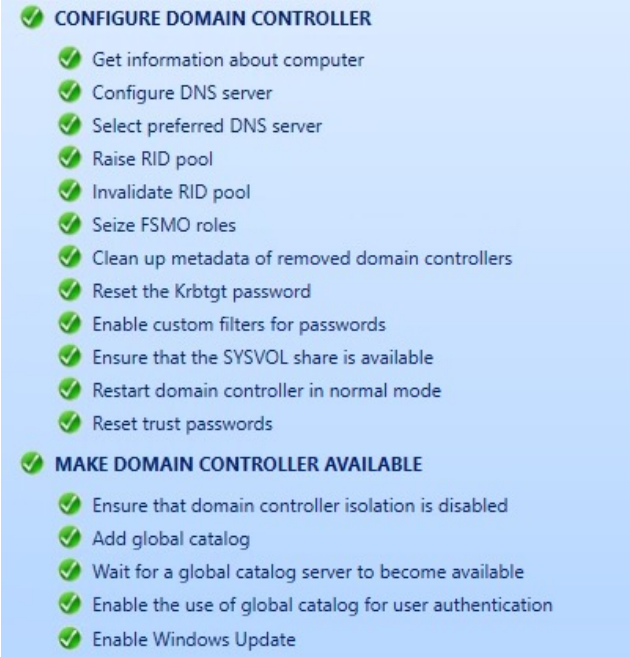


Figure 3. Some of the steps involved in restoring a DC manually

VM snapshots are not adequate AD backups.

Many organizations have virtualized at least some of the servers. One way to back up those servers is to use hypervisor snapshots — images of the virtual machine (VM) at a given point in time. However, relying on snapshots for your AD disaster recovery strategy is unwise for multiple reasons.

The most important is that using snapshots for forest recovery will almost always result in data consistency problems that are difficult to resolve. Since the data on DCs is constantly being updated and the replication process takes time, snapshots of different DCs almost always contain inconsistent information. In particular, restoring from snapshots almost always results in lingering objects — objects that are present on one DC but that were fully deleted from other DCs.

Quest

Identifying, troubleshooting and cleaning up lingering objects can be very difficult.

In addition, like BMR backups, snapshots can include malware, which gets restored with everything else on the DC. Plus, if you store your VM snapshots in the default location, they're an obvious target for ransomware encryption, which can render them useless.

There's also a logistical issue. Usually, control over VM snapshots resides with the virtualization operations team, which complicates the AD team's job during the recovery operation. Moreover, the virtualization team might not even know that the AD team the snapshots are an essential part of the organization's disaster recovery strategy, so they might not protect them appropriately.

Cloud-only objects and attributes are not adequately protected.

Finally, we mentioned the importance of Azure AD backups in hybrid environments, but it's worth mentioning some additional reasons why cloud-only objects and attributes are not adequately protected by native Microsoft tools. These include the following:

- Some objects cannot be recovered at all, including Azure AD groups, group membership and hard-deleted users.
- Only recently deleted objects can be recovered (within last 30 days).
- Some attributes cannot be recovered, such as MFA settings and Conditional Access policies.
- Restore in bulk cannot be done without a PowerShell script.
- There is no Azure AD change log or comparison report to help you determine what needs to be restored.

This list is far from comprehensive; for more details, read the white paper, "What You Don't Know about Office 365 and Azure AD."

Limitations of traditional data protection solutions

Recognizing the limitations of native tools, many organizations have invested in backup tools or other data protection solutions. These products can be sufficient in some recovery scenarios, such as when the operating system needs to be recovered, and some solutions can even perform a bare metal restore of servers.

However, most data protection tools simply do not suffice for Active Directory disaster recovery. As noted earlier, in a forest recovery, you must coordinate the configuration effort across multiple DCs. Failure to do so can run the risk of USN rollback, RID bubbles, RID re-use, lingering objects in the Global Catalog and other issues that can cause serious issues with Active Directory functionality. But most traditional data protection solutions simply focus on getting individual DCs to a "healthy" state — and leave all the coordination work to you.

In addition, while some of data protection solutions support IFM, you still have to promote each DC one at a time. That's not exactly a recipe for getting your business fully back on its feet quickly! Finally, on-premises AD backup solutions do not cover cloud-only objects and properties.

Quest recovery manager for active directory disaster recovery edition

Recovery Manager Disaster Recovery Edition streamlines recovery from ransomware. First of all, it offers reliable backups of exactly what you need to recover AD. By omitting extraneous and risky components like boot files and the IIS Metabase, the solution reduces backup bloat, makes the backup process more efficient and minimizes the places where malware can hide. Moreover, Recovery Manager offers Secure Storage — a hardened server that is isolated according to IPSec rules. Even if you lose your domain controllers, your Tier 1 storage and even your Recovery Manager server, you still have the Recovery Manager Secure Storage backup that is so hardened and secure that it withstands the ransomware attack.

When ransomware strikes, Recovery Manager automates the entire AD recovery process, including the 40+ steps outlined in Microsoft's AD forest recovery document. For example, it provides:

- Automatic rebooting of every DC into DSRM
- Automatic isolation of all DCs during recovery
- Automatic password resets
- Automatic seizing of FSMO roles from DCs that fail to recover
- Automatic re-assignment of Global Catalogs should the last GC in a site fail to recover
- Automatic detection of lingering Global Catalog objects
- Automatic cleanup of metadata after recovery is complete

You get flexible recovery options, so you can choose the method that works best in a given situation, whether that's phased recovery, restore to a clean OS or bare metal recovery. Moreover, you can restore to a clean OS on any machine: a physical machine, an on-prem virtual machine or a cloud-hosted VM. Recovery Manager even includes automated malware detection that minimizes the risk of reintroducing infected files to recovered DCs. 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 production.

In addition, Recovery Manager dramatically accelerates Phase 2 of the disaster recovery process by providing automated bulk IFM: In a single click, you can execute the IFM process on all of the DCs you selected, with no error-prone manual processes or time-consuming visits to each DC. The backup used for the restore process can be held on any backup media (tape, CD or DVD) or on a shared network resource, giving you maximum flexibility and control.

A global manufacturer that suffered a ransomware attack was able to restore basic operations in less than 2 hours using Recovery Manager.

Example: Recovery Manager speeds recovery after ransomware attack

Ransomware struck a global manufacture, impacting 17 domain controllers across multiple continents. The attack also scrambled AD passwords nearly all user accounts, including service accounts.

Using Recovery Manager for Active Directory Disaster Recovery Edition, the IT team was able to restore operations quickly: The most critical DC was back up and running in about one hour. A second DC was recovered in just 12 minutes, followed by three more DCs across two continents in just 36 minutes. With the company firmly back on its feet, recovery of the remaining DCs was planned for later phases.

As the project manager put it, “There’s no way that they would have recovered… so quickly if they did not have the Quest tool!”

Additional disaster recovery best practices

A strong ransomware recovery strategy and proper tools are core elements of a disaster recovery plan. To ensure your strategy is comprehensive, also be sure to follow these best practices:

- Define your recovery time objectives (RTOs) and recovery point objectives (RPOs). RPO will determine how often you back up and replicate your AD, and RTO will help you prioritize which DCs to restore first to get your most critical business processes running as quickly as possible.
- Have separate emergency communications mechanisms that don’t rely on AD. This will help ensure that business, IT and recovery functions can communicate with one another.
- Identify the escalation path and key decision-makers at each critical point in the disaster recovery process. Know how to contact required personnel anywhere, anytime.
- Test the plan with people who didn’t develop the plan. Assumptions about what people understand can stall recovery or send it in the wrong direction.

- Practice the plan at least twice a year. As the calculation of the cost of downtime earlier in this white paper vividly illustrates, seconds count; the best way to shave off seconds is to practice processes until they become automatic.
- Update the plan regularly to account for changes in systems, compliance requirements, the recovery team and more.

Conclusion

Ransomware is a clear and present risk to every organization today. You need to ensure you can get your business back up and running as quickly as possible, which usually means performing a phased recovery.

Recovery Manager for Active Directory Disaster Recovery Edition delivers unmatched stability, flexibility and options. You get a rock-solid solution for backing up Active Directory and flexible recovery options, including clean OS recovery to minimize the risk of malware reinfection. Moreover, you can restore AD to a clean OS on any machine, regardless of its location or type (physical, virtual or cloud-hosted).

In short, when the next disaster strikes, you get to be the hero rather than the scapegoat. To learn more, please visit https://www.quest.com/products/recovery-manager-for-active-directory-disaster-recovery-edition/.

Ensure you can get your business back up and running quickly after a ransomware attack with Recovery Manager.

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. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now.

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.