



# Does Your Active Directory Disaster Recovery Plan Cover Cyberattacks?

BY GUIDO GRILLENMEIER AND GIL KIRKPATRICK

02	RECOVERING AD FROM CURRENT THREATS
04	WHY PROTECTING ACTIVE DIRECTORY IS SO IMPORTANT
06	HOW THE THREAT LANDSCAPE HAS CHANGED
07	WHY ACTIVE DIRECTORY IS VULNERABLE
11	RECOVERING ACTIVE DIRECTORY

# RECOVERING ACTIVE DIRECTORY FROM CURRENT THREATS

Sixteen years ago, Gil Kirkpatrick (Semperis Chief Architect) and Guido Grillenmeier (Semperis Chief Technologist)—each working for different companies at the time—got together to share their experience and expertise on protecting and recovering Active Directory (AD). The result of this collaboration was the publication in 2005 of the whitepaper “A Definitive Guide to Active Directory Disaster Recovery.” The whitepaper served a critical need in the industry, as most companies had accepted AD as the de facto standard directory service to use for controlling access to their corporate network, applications, and services for their users.

Back then, information about recovering all or part of an AD was scarce, and not many AD practitioners understood the reality of the challenge. The whitepaper explained the mechanics of AD recovery and clarified how necessary it was for companies to prepare themselves to properly recover from various AD problems. It described how to recover from several types of disasters, including inadvertent deletion of AD objects, group policy misconfiguration, and failed AD domain controllers. The document ended with a brief outline of the process to recover an AD environment after a complete meltdown, with the caveat: “However, the likelihood of [needing] a full AD forest recovery is very small.”

That was then, this is now. The cybersecurity landscape has drastically changed. A week doesn't go by without some organization's on-premises Windows network being flattened by a ransomware or wiper attack. For instance, from 2019 and early 2020 (with estimated recovery costs):

- City of New Orleans (\$3M+)
- City of Baltimore (\$18M)
- Norsk Hydro (\$70M)
- Demant (\$80M)

And there are dozens more. The point is that the ability to recover your AD environment entirely from backup is no longer a nice-to-have response to a highly unlikely event. It is a requirement.

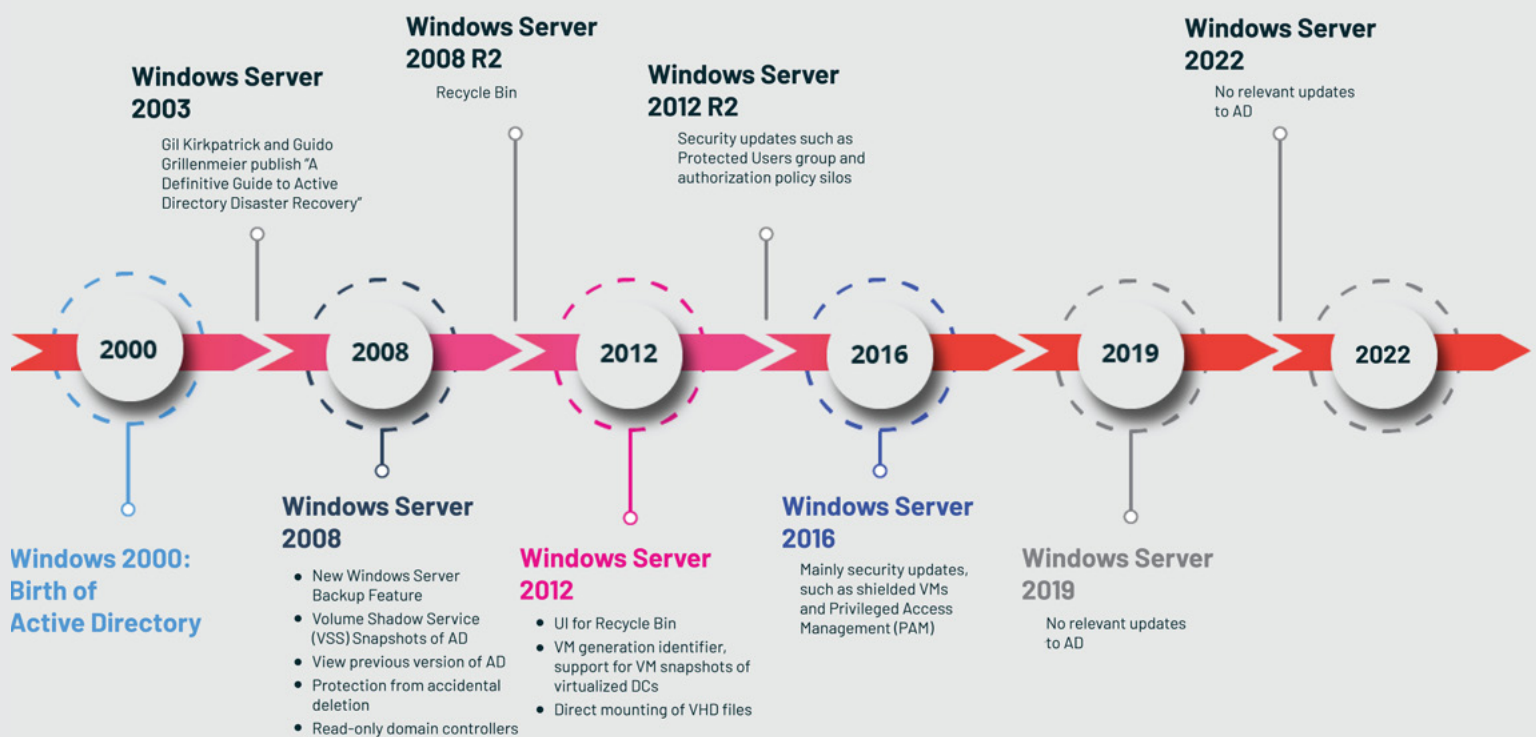
As the threat model has changed dramatically since 2005, so too has the Windows Server Operating System (OS) and its built-in Active Directory service. Microsoft has improved Windows security substantially, added features and capabilities to simplify AD object recovery, and improved the behavior of AD when running in a virtualized environment. But the fundamental problems of recovering an entire Active Directory forest from backup haven't changed. It's still an error-prone, complex process that requires planning and practice for all but the most trivial AD deployments.

It's notable that the two latest Windows Server releases (Windows Server 2019 and 2022) are the first versions of Windows Server with no relevant updates to the AD service itself. Apparently, in Microsoft's view, there are no more issues in AD to fix and no more service improvements required. More to the point, AD disaster recovery is not going to get any easier.

We now need to evaluate a company's recovery capabilities in the context of the new cyberthreats targeting AD today, which we didn't have to worry about in 2005. Sadly, the increase in attacks means that companies urgently need to prepare for fast remediation of attacks against their corporate AD. The improvements Microsoft has made to the core of the AD service over the years might still prove of little help in recovering your AD if you are hit. Is your company ready to quickly recover your own corporate AD in case of a true disaster that wipes out the complete AD service?

*"Companies urgently need to prepare for fast remediation of attacks against their corporate AD."*

# Active Directory backup-related changes over time



***Is your company ready to quickly recover your own corporate AD in case of a true disaster that wipes out the complete AD service?***

# WHY PROTECTING ACTIVE DIRECTORY IS SO IMPORTANT

Active Directory (AD) has been in production for more than 20 years. As it was originally designed, this Microsoft server role provides:

**Authentication:** Authenticates on-premises users logging in to their PCs and the corporate network and remote users logging in to in-house hosted applications or virtual desktops

**Authorization:** Controls which AD-integrated resources—such as file services, printing, Exchange Server, SharePoint Server, and SQL Server—they have permissions to access

**Security and control:** Group Policy can apply policy configurations to every computer, server, and user that is joined to AD

**Directory:** A single location to discover users and resources

**DNS:** AD-integrated DNS to provide network name resolution

**PKI:** Active Directory Certificate Services provides certificates for domain users and computers

The rise of popularity of the Windows Server OS to provide basic file- and print-sharing services—and other back-office services such as email, messaging, and collaboration—helped cement AD as the network directory of choice. Microsoft evolved practically all its popular applications to rely on it, making AD one of the most ubiquitous software services in the enterprise today. Over 90% of organizations worldwide larger than 500 employees use AD.

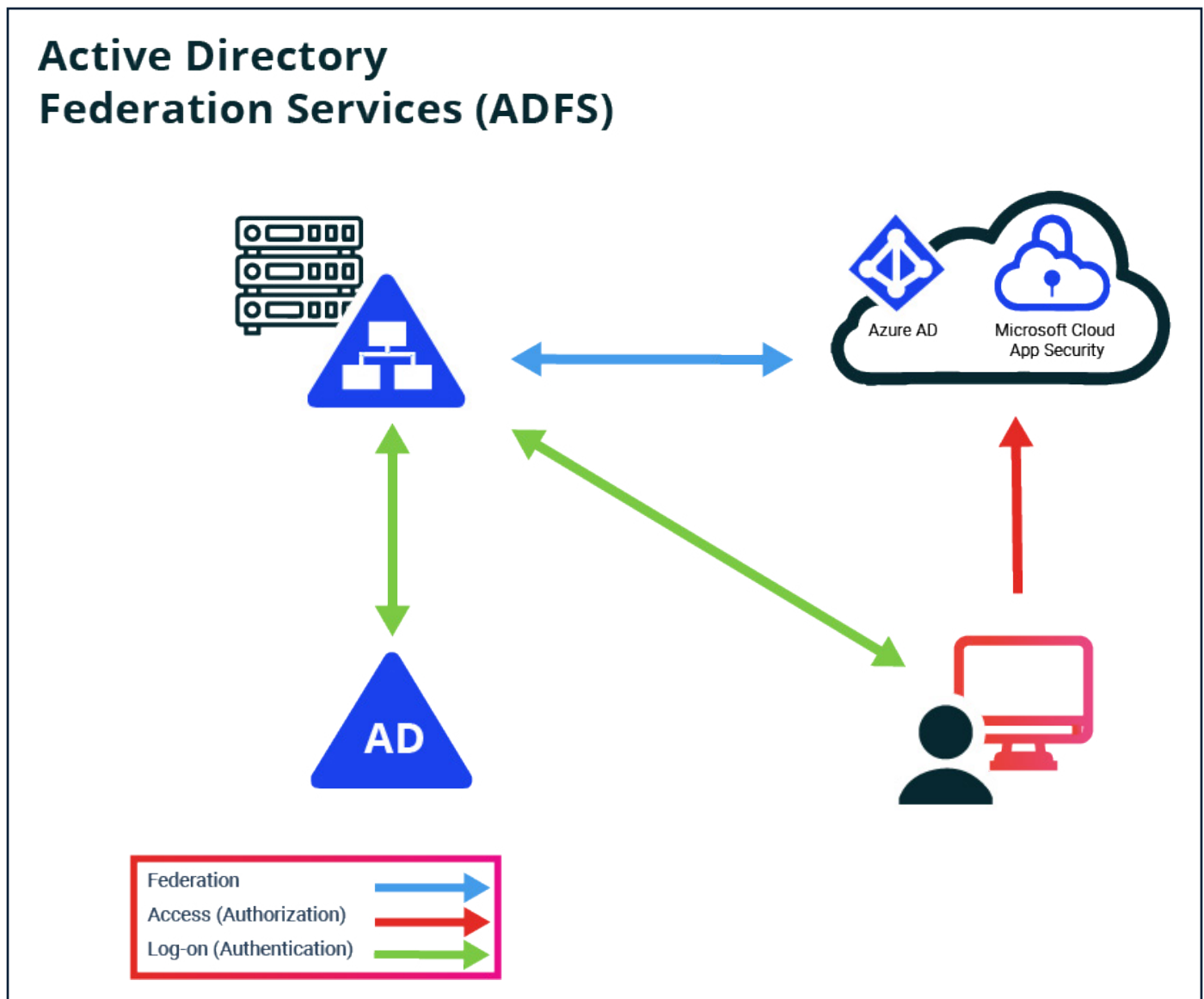
The rise of cloud computing has not changed this reliance. In fact, cloud computing has increased AD's importance to the enterprise. There are two factors behind AD's importance to the cloud.

First, the cloud computing model doesn't depend on trusted networks in the way traditional on-premises computing does because, unlike traditional corporate networks, traffic between clients and the resources they access most often occurs over the public internet. This traffic is not secured by WHERE you are, but by WHO you are. As Microsoft puts it, "identity is the control plane" by which access to cloud resources is controlled. A user's identity is front and center in cloud security.



Second, AD is the foundation of the hybrid identity architecture commonly used today. In this architecture, organizations synchronize their on-premises identity store—usually AD—into the cloud identity service of their choice such as Azure Active Directory, Okta, or Amazon Web Services (AWS). This approach allows users to use their corporate identity to access resources (for example, Office 365 or Salesforce) that are integrated into the organization's cloud identity service.

Furthermore, many companies do not yet trust services in the cloud as much as they do their in-house controlled systems that are fully managed by their own IT staff—as such, many have decided to set up a federated authentication framework using AD Federation Services (ADFS) or similar solutions to connect with cloud solutions, for example, Azure AD. In this case, the validation of the user's identity, i.e., the authentication, continues to occur against their on-prem AD. ADFS then creates a proper token, the SAML token, confirming to the cloud service (e.g., Azure AD and associated apps) that the connecting user is really who he or she claims to be. As the SAML token is properly encrypted with a key shared only between ADFS and Azure AD, Azure AD fully trusts this token and grants the user access to the respective cloud resources. Essentially, Azure AD fully trusts your on-prem AD in this setup.



*Figure 1: Federation usually relies on your on-prem AD to certify the identity of your users*

Add to this the fact that despite all the hype and shift to cloud computing, all organizations of any size or age have substantial and ongoing on-premises operations that depend on AD. As a result, AD today not only remains essential for accessing on-premises resources, but also is a critical component of today's hybrid enterprise and all its applications.



# HOW THE THREAT LANDSCAPE HAS CHANGED

When the original “Definitive Guide to Active Directory Disaster Recovery” was written, the main disasters AD administrators had to worry about fell into two buckets: physical disasters (such as a power failure, disk crash, or flood), and administrative errors (inadvertent or malicious) that modified or deleted AD objects inappropriately. The third category—a forest-wide service failure—was theoretically interesting, but almost never occurred in real life. Even though the effects of a full-forest failure were disastrous, it was so unlikely that the resulting residual risk was something most organizations just lived with.

In 2021, that risk calculation has been completely turned upside down. AD continues to handle physical server and site problems well, and after 10 to 20 years of experience, most organizations can reliably and securely administer their Active Directory. But cybercriminals, armed with sophisticated phishing tools and the latest reconnaissance, persistence, and data encryption malware, can flatten an entire enterprise Windows environment in a few minutes. The recent ransomware statistics are sobering.

## In 2020:



51% of businesses were hit by a ransomware attack. ([Pentest Magazine](#))



Ransomware costs organizations roughly \$75B annually ([Datto](#))



The average ransom demand was \$178K, with the largest publicized payment of \$11.8M

Losing the entire Active Directory service has moved from the bottom rung of the risk ladder to the top.

## Active Directory is a prime target for cybercriminals

Active Directory is designed well to handle physical disasters. If a DC fails, or even if an entire data center goes offline, AD will continue to function with the remaining domain controllers. Microsoft added the AD Recycle Bin feature in Windows Server 2008 R2, and it supports the recovery of inadvertently deleted objects reasonably well. As far as undoing inadvertent changes to AD objects, you're still pretty much on your own.

It's clear that AD is a critical core service in nearly all organizations. AD stores user, computer, and service credentials, and controls authentication and authorization across the entire on-premises environment. This makes AD a juicy target for threat actors for three reasons:

- As a directory service, AD is a one-stop shop for information that threat actors need to move laterally through the network and elevate their privileges.
- As the primary authentication and authorization service, AD is a single point of attack that can render the rest of the network effectively unusable.
- As the de facto endpoint configuration management solution via group policy, AD is another tool that attackers can use to distribute malware and gain persistence on multiple machines on the network.

While we generally never hear about technical specifics in news articles about cyberattacks, we're starting to see Active Directory mentioned far more regularly:

- [Virgin Mobile's Active Directory was compromised](#) and its data sold on the Dark Web.
- [NTT Communication's admitted to their Active Directory being compromised](#) as part of a data breach.
- [Ryuk ransomware has been shown to modify Group Policy](#) to propagate itself to endpoints via a login script.

Truth be told, we always could trace the dotted line knowing that Active Directory was very likely part of an attack; now we have data to prove it.

# WHY ACTIVE DIRECTORY IS VULNERABLE

Active Directory works quite well, and its design has stood the test of time. However, the world has changed around it, with the emergence of crypto versions, its openness to queries, Kerberos, and the increasing sophistication of attacks that employ tools such as Mimikatz.

## Advanced Persistent Threats (APTs): Infiltration and breach

Attacks against AD have dramatically increased in the last few years as malefactors have recognized that if they own AD, they own the organization's IT resources. It is a truism that AD "holds the keys to the kingdom," but even that phrase understates the risk: The service also holds a "treasure map" to all the organization's AD-integrated resources that depend on it. While end users will not be aware of their dependency on AD, the various tools and business processes they use every day could not work if AD is down. This includes apps for critical services such as email (Exchange), file-sharing (SharePoint, normal file shares), collaboration (Skype) or even the capability to print. Many companies further utilize Windows integrated authentication for many of their business apps and databases, where "Windows integrated" is simply a different term for "AD integrated," i.e., the applications do not rely on their own user-list, but they "trust" the access token from a user that is generated by AD to grant proper access to the application. AD does not only control the access to those apps by legitimate users, it also allows intruders to understand which apps have been integrated in an infrastructure and thus use it against you.

As the recognition that AD is a valuable target has grown, so have toolsets to attack it. PowerSploit, Bloodhound, Death Star, Cobalt Strike, and especially Mimikatz have enabled attackers to quickly find credentials, perform horizontal reconnaissance across the network, find the shortest path to domain admin rights, and target that path.

These tools reduce the time to domain dominance from days to hours. As a result, successfully attacking Active Directory is easier now than it has ever been.

## The cyber disaster: DoA attacks

AD is marvelously fault tolerant to natural or physical disasters. Hurricanes, tornadoes, earthquakes, power failures and other events that take out a data center will impact a well-designed AD locally but allow the rest of the network to continue to use the service. When that crippled section of AD

is restored to operation, any changes that have happened in the network during the outage will automatically flow into the restored section. An incident that took out an entire AD domain or forest would be very high impact, but it would also be extremely rare because of the precautions companies have taken to geographically distribute their AD infrastructures. Thus, the risk of AD being completely unavailable was never classified as more than moderate. Coupling this with the fact that Active Directory business continuity and disaster recovery (BCDR) is very expensive (more on that later), BCDR planning has traditionally neglected forest recovery.

Enter denial-of-availability (DoA) attacks. The best-known variants of this breed are ransomware and wiperware. Almost everyone knows what ransomware is. Barely a day goes by without news of some company's clients, servers, and data being encrypted and requiring some amount of bitcoin to get the decryption key from the attackers. Wiperware destroys your computers and data, whether it is through encryption or outright data deleting, without recourse for recovery.

The 2017 NotPetya attack is the best-known example of this breed to date. The [container shipping company Maersk was one of the major victims](#). NotPetya wiped out thousands of Maersk's computers, servers and, yes, all of their AD domain controllers globally, including their backups. They were just lucky that a power outage prevented the malware from spreading to the domain controller in their Ghana site: They were finally able to use that DC to recover their AD. After undergoing a very expensive recovery, estimated to have cost Maersk between \$250 million and \$300 million, they decided to publicly talk about their situation to make other companies aware of the risks of modern malware attacking their infrastructure. Companies need to prepare against this threat as most would not survive a nine-day outage of their central IT, which is how long it took Maersk to completely recover their Active Directory.

Other heavily hit victims of the NotPetya attack included FedEx, Saint-Gobain, Reckitt Benckiser, and Mondelēz. And the NotPetya attack was by no means the last attack against AD. It was merely the beginning of a new era of fast-spreading ransomware attacks that use and impact Active Directory. Sadly, the attack vectors against AD are plentiful—just recently, a successful attack by Nefilim was able to use a [highly privileged domain admin account of a deceased employee](#) to open all doors for the intruders.

## Your Active Directory backups won't help you recover your AD service

In the case of a cyber disaster, normal Active Directory backups won't help you recover business operations after the attack. The "Protect objects from accidental deletion" feature will help to avoid human failure, but won't address malicious activity in your AD.

The same is true for the Recycle Bin, which allows you to recover deleted objects but can't help you with undoing changes at the attribute level, nor changes to GPOs or the configuration in your AD. Recycle bin is also unable to help in recovering your whole domain or forest and related application partitions.

Utilizing snapshots can support detection of attribute-level changes and help to undo them but will add a great deal of complexity to the recovery process.

But none of these methods for restoring Active Directory data will be enough to help you recover the actual AD service—your complete domain or forest. While we all hope to never need it, a Schema corruption due to a malicious change performed by an intruder or the encryption of all your DCs by malware might require a forest-level recovery of your AD. For this, we still need a proper backup of the AD DCs.

## Preparing a backup that allows malware-free Active Directory service recovery

Recovery of the Active Directory service, which means the recovery of the NTDS.dit and related OS files and settings to allow proper replication of AD data, is a much more challenging task than just recovering specific AD objects. If all changes to all objects and attributes were kept on a single AD database server—a single domain controller—then the recoverability of the server would be a simple matter, similar to that of a file server.

However, the great power and success of Active Directory is based on the fact that, unlike its predecessors, the changes performed in the directory are not restricted to occur on a single server, or a single master. Instead, AD was designed as a multi-master database architecture, which allows changes to occur on any (writeable) domain controller in a company's network. This is what made the scalability and the geographic spread of the Active Directory service possible and allows an AD domain or forest to service many sites that are spread around the globe.

We cover specific points about global DC backup in more detail in the full “Definitive Guide,” but thinking about the geographical distribution of your AD DCs and their backups is just as important as performing the backup itself. At any time during your AD backup planning, you should consider whether the chosen DC backups are sufficient to bring back your AD forest quickly. This is particularly challenging in a multi-domain forest, i.e., a forest that has multiple child domains or parallel trees that are part of the same AD forest structure. As soon as you have more than one domain in your AD forest, the Global Catalog is a necessary AD functionality that will have to be rebuilt and re-activated during a forest recovery process, before authentication services can commence again. And rebuilding that Global Catalog will take much longer if you don't have at least one DC of every domain in your forest located in the same AD site. Further below, we'll discuss more challenges of bringing your forest back quickly.

## Integrating with Volume Shadow Copy Service

It goes without saying that the backup tool you use to back up your Active Directory DCs should integrate with the Volume Shadow Copy Service (VSS) feature of the Windows Server operating system. This integration ensures a consistent state

of your AD database at the time of performing a backup—i.e., all ongoing write operations will have been finished and written to disk, while new incoming changes to the AD database are halted at the time that a snapshot of the AD database is performed. This process takes only seconds, after which the backup tool has all the time it needs to copy the consistent state of the AD database to a target of your choice, while the write operations to the original AD database can continue to keep the AD domain controller running as usual.

The built-in Windows Server Backup (WSB) is a good example of a backup tool that is fully integrated with VSS and allows you to perform two types of backups:

1. SSB (System State Backup)
2. BMR (Bare Metal Recovery)

The two options are quite different in their use cases, so beware of the different features when planning your backup strategy.

### System state backups might contain malware

The system state backup option backs up all critical parts of the server operating system of a DC, including the AD database (NTDS.dit), the SYSVOL folder, COM+ class registration database, the registry of the server, and the boot files—but avoiding any user data, extra disks, and data that might have been added for other applications running on the same server. While the backup uses the VSS capabilities to create a proper snapshot of the disks used by the server, the transfer of the actual system state backup is a file-based copy of the relevant files to the backup target, which does not allow performing any incremental backups—i.e., you must always transfer your full system state to the target backup location. In addition to your AD database, a system state backup stores about 11GB of the Windows Operating System files into each DC backup.

Recovery of the system state backup is meant to be performed to the same Windows Server instance and OS installation that it was created from, which means that it's intended to help in case of a problem at the OS or data level, but not in case of a hardware issue that requires rebuilding the complete server. As such, a system state backup is fine to use for recovering the AD database in cases where you need to authoritatively restore parts of an AD database to recover accidentally deleted objects from AD. However, a system state backup is not meant to help you recover your backup to a freshly deployed server and certainly not one with dissimilar hardware or even a change of architecture from physical to virtual, or vice versa. Granted, a system state backup might be your only option if—after a cyberattack—you need to recover your AD DCs quickly to other hardware or virtual machines that might be made available to you more quickly. In any case, beware that the system state backup includes various files from the OS that were backed up—meaning that the likelihood of a re-infection from malware that was backed up with your AD is significant.

***“Beware that the system state backup includes various files from the OS that were backed up—meaning that the likelihood of a re-infection from malware that was backed up with your AD is significant.”***



*“As with system state backups, caution is needed when restoring AD from BMR backups after a cyberattack to avoid re-introducing malware.”*

### **BMR backups also might contain malware**

As the name implies, backups created with the bare metal recovery (BMR) option, also called “full server” backups, allow you to recover a given server to its backed-up state, including full recovery of the OS and services running on it, as well as Active Directory. The goal is to protect you from the classic hardware-level failures such as broken disks. But BMR backups also have the potential to reintroduce malware if used to restore AD.

The BMR option backs up all disks that are used by the OS, which includes the system state as well. You can also choose to back up additional disks on the respective server. As a BMR backup is created with the block-based backup method, you also have the option to configure backups of only those blocks that were changed since the last backup: You can run an incremental backup, further speeding up your backups. Incremental backups work if you have configured the proper option in the backup performance settings on your server and your backup target disk is hosted on the same server that you are backing up. The latter approach might be counter-intuitive but will work if you have additional mechanisms at hand to store the created backup files on some other safe storage target afterward.

At recovery time, you must boot the repaired server with a proper Windows Server OS installation disk before you can recover it from the respective backup file. Note that this server installation also needs to be of the same type of hardware and architecture. For example, the BMR option does not allow you to recover a backup of a Dell server to a new one from HPE or to choose a virtual machine as the target for recovery. Because of this limitation, and because there's an easy option to stand up a new replica of an AD domain controller by promoting it after a clean-OS installation to hardware of any choice, the BMR method is seldomly used for backing up Active Directory DCs. As with a system state backup, the BMR backups are subject to the same risk of including the malware that might have affected your AD DCs prior to becoming active and harming your AD forest. As with system state backups, caution is needed when restoring AD from BMR backups after a cyberattack to avoid re-introducing malware.

Also note that neither SSB nor BMR backups are encrypted by the Windows Server Backup feature—which means your backups are vulnerable in transit and certainly at rest, if you have not encrypted the disk that holds your backups. This also means that you should not copy the backup files to another target storage system accessible to non-domain admins without properly encrypting them first.

*Be sure to store backup files safely, ensuring that only the AD service administrators have access to them.*

## **Use caution with snapshots**

Snapshots are bad! Snapshots to the rescue!

Both statements make some level of sense. Until the release of Windows Server 2012, which added a proper identifier of a VM's version when using VM-level snapshots (VMGenID), Microsoft had to continuously warn about the non-supportability of taking snapshots of DCs in virtual environments. Admins could too easily make the mistake of rolling a DC “back in time” without using the proper AD recovery method of letting other DCs in the environment know about this rollback. That oversight could cause all sorts of replication issues by interrupting the built-in replication logic of the complex AD ecosystem. Update sequence number (USN) rollback would occur, and with it, an unreliable object state in the AD forest with the potential of creating duplicate SIDs and lingering objects.

Assuming that by now all your DCs globally are operating at least with Windows Server 2012 and you're using a hypervisor that supports the VMGenID logic (all major hypervisors have been doing so for years now), we can spare the details of why reverting DCs back to a previous version via a VM snapshot was really bad. While it is still by no means a backup mechanism for your AD forest, you can at least no longer do harm to your AD when using VM snapshotting technology.

In the forthcoming whitepaper, “The New Definitive Guide to Active Directory Disaster Recovery,” we'll cover critical changes Microsoft introduced with Windows Server 2008 that impacted native AD backup and recovery: The integration of the AD database with the VSS capabilities of the OS. We'll also cover the revamped Windows Server Backup (WSB) feature, also introduced with Windows Server 2008, that made backup data accessible as a VHD file. And we'll provide details on the practical feature that Microsoft added with the 2012 release, the ability to mount VHD files directly into an existing Windows client, which enables the fast lookup of a previous version of the AD database.

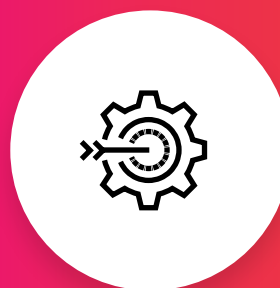
All these changes make it easier for admins to, for example, retrieve files from a previous version of your SYSVOL folder, or use a read-only version of your AD data to recover overwritten attributes of any of your objects. The key here from the perspective of closing Active Directory security gaps is to properly safeguard your backup files, as anyone who has access to those sensitive files can do anything you can. They can even use other offline editing tools to reap the password hashes and other sensitive data from the AD backup. Be sure to store backup files safely, ensuring that only the AD service administrators have access to them.

## Beware the limitations of third-party backup tools

Essentially any backup tool that claims to back up AD today will also be integrated with the VSS capabilities of the OS or might even leverage the Windows Server Backup (WSB) feature and simply wrap in more intelligence to centrally back up a proper choice of your DCs.

However, as with the built-in WSB tool, being able to back up AD domain controllers does not automatically mean that a tool can help you quickly recover your AD forest in case your schema is corrupted or all your DCs have been infected by malware or some other cyberattack. Be aware that most backup solutions concentrating on OS-level backups might function well for recovering individual servers—even domain controllers—but (as the next section clarifies) aren't capable of coordinating the complex recovery process that is required to bring your AD forest back to life after a cyber-attack.

Another sobering consideration: The risk of re-introducing the malware that might have been stored in the Windows OS of your AD DCs for many weeks or months without being detected. Such malware would likely be stored in your AD backups if the third-party tool performs the standard System State Backup or BMR backup of your DCs, as is the case with the built-in WSB tool.



## MORE RESOURCES

### WHITE PAPERS

[Assessing the ROI of a Quick Active Directory Recovery](#)

[Report: Recovering Active Directory from Cyber Disasters](#)

### WEBINAR

[A Cyber-First Approach to Disaster Recovery](#)

### BLOGS

[Now's the Time to Rethink Active Directory Security](#)

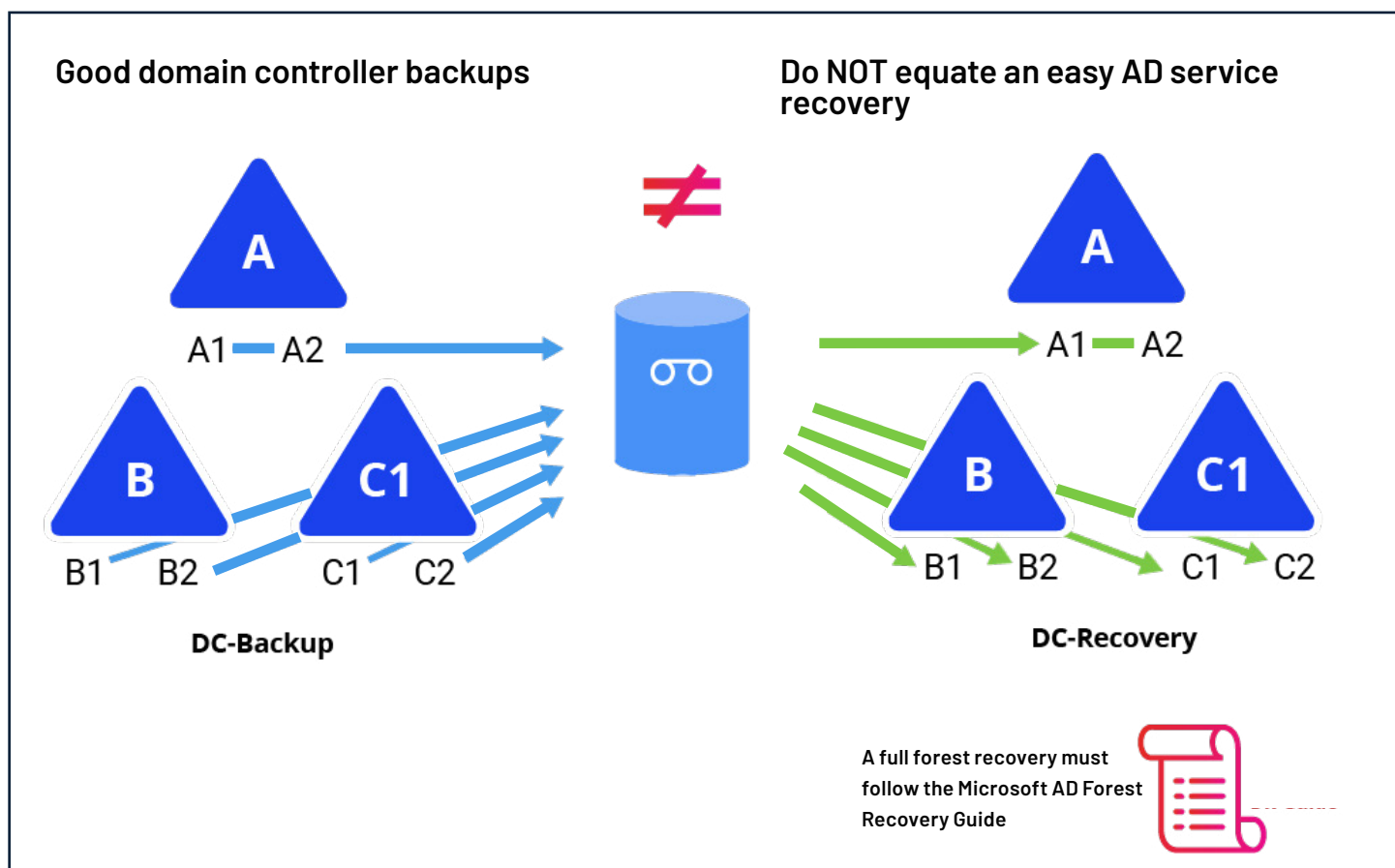
[Time to Leave ADFS Behind for Authenticating in Hybrid Environments?](#)

[The Dos and Don'ts of Active Directory Recovery](#)

[Timeline of a Hafnium Attack](#)

# RECOVERING ACTIVE DIRECTORY

When talking about Active Directory recovery, it's important to distinguish between recovering data (users, groups, computers, Group Policy, etc.) and recovering the AD service—the distributed application running on designated multiple servers containing the Active Directory domain services workload, configured in a specific topology. The fact that all domain controllers in the forest share the configuration of the AD topology, and the database schema within their own AD database, does not make this task any easier.



Just because you have backed up all the necessary AD domain controllers does not mean that you have an “easy way” to restore the complete AD service—the whole AD forest—should you need to do so in the event of a true disaster. When malware is wiping out all of your DCs, you’ll need to follow the painful process of recovering your AD from a bare minimum installation.

## The Active Directory forest recovery process can be painful

As discussed, in the increasingly vulnerable threat landscape that IT systems are facing, networks, applications, and identity security—not geography—determine the scope of a disaster. The fault tolerance established by having multiple data centers is rendered useless in the face of sophisticated malware that spreads across a network in minutes.



As a result, the specter of an entirely destroyed AD forest has gone from the troubled dreams of AD administrators to a very real possibility.

Only recently, Microsoft customers faced the next major attack on a product very tightly integrated with their on-prem AD: [four new zero-day vulnerabilities in Microsoft Exchange](#) allowed the cyber-criminal group from China called “Hafnium” to inject malicious code into Exchange Servers of [more than 30,000 organizations](#), before the servers could be patched properly. The attack gives the intruders total, remote control over affected systems. Because of the pervasive permissions that Microsoft Exchange has in Active Directory, the latter is an easy next target. AD would usually first be infiltrated to further elevate the privileges of the intruders to reap sensitive data from the attacked organization that is copied to an external target under the control of the intruders. In a next step, the intruders typically take a day or weeks to spread and distribute ransomware to as many systems that they can reach. In the meantime, the target organization doesn’t realize yet that it has been hacked and is happily backing up the infected systems with their daily backup routines (on average, [according to FireEye, an attacker lingers about 72 days undetected in a compromised network](#)). Eventually, they trigger the ransomware that encrypts the affected systems, which would include all the organization’s member systems in AD, as well as all AD domain controllers themselves. In a last step, the responsible cybercriminals request a huge ransom from the affected organization for the promise (but no guarantee) of a decryption key and of not selling the stolen data.

### Why not just restore from backups?

So, in the event of a true disaster of your AD service, why not just restore all your DCs from backups? As mentioned before, a “good backup” of those services with the AD DS role installed—the domain controllers—does not equal an easy path to recovering the Active Directory service. There are many steps you need to follow to restore your AD service to a trusted state.

**Getting through the recovery process successfully requires coordination between AD engineers, recovery operations teams, and most likely virtualization management teams—at every location you intend to recover your DCs.**

### The AD recovery process

Over time, many AD admins have convinced themselves that they have it covered, but you can’t just “follow the doc” in the online [AD Forest Recovery Guide](#) when the time comes. And it’s not just the process that makes forest recovery difficult; it’s also a logistical and training challenge. Getting through the recovery process successfully requires coordination between AD engineers, recovery operations teams, and most likely virtualization management teams—at every location you intend to recover your DCs. Everyone must execute their tasks flawlessly, in the right order, in probably the highest stress environment of their careers.

## High-level roadmap for AD forest recovery

Here’s a quick snapshot of the steps involved in recovering an AD forest to a known-secure state:

1. Determine forest structure and available backups
  2. Identify single DC for each domain with valid backup
  3. Shut down all DCs in the forest
  4. First recover Forest Root Domain
  5. Then recover one DC of each child domain
  6. Clean up and re-promote all other DCs in the forest
- Ensure recovery of trust hierarchy and critical DNS resource records
  - Ensure recovery of parent domains prior to their child domains to maintain trust hierarchy

## AD disaster recovery isn’t easy

AD disaster recovery is not a simple task. Ideally, you prepare with a thorough risk analysis for your own environment: Is the mitigation strategy too expensive, or the residual risk too high?

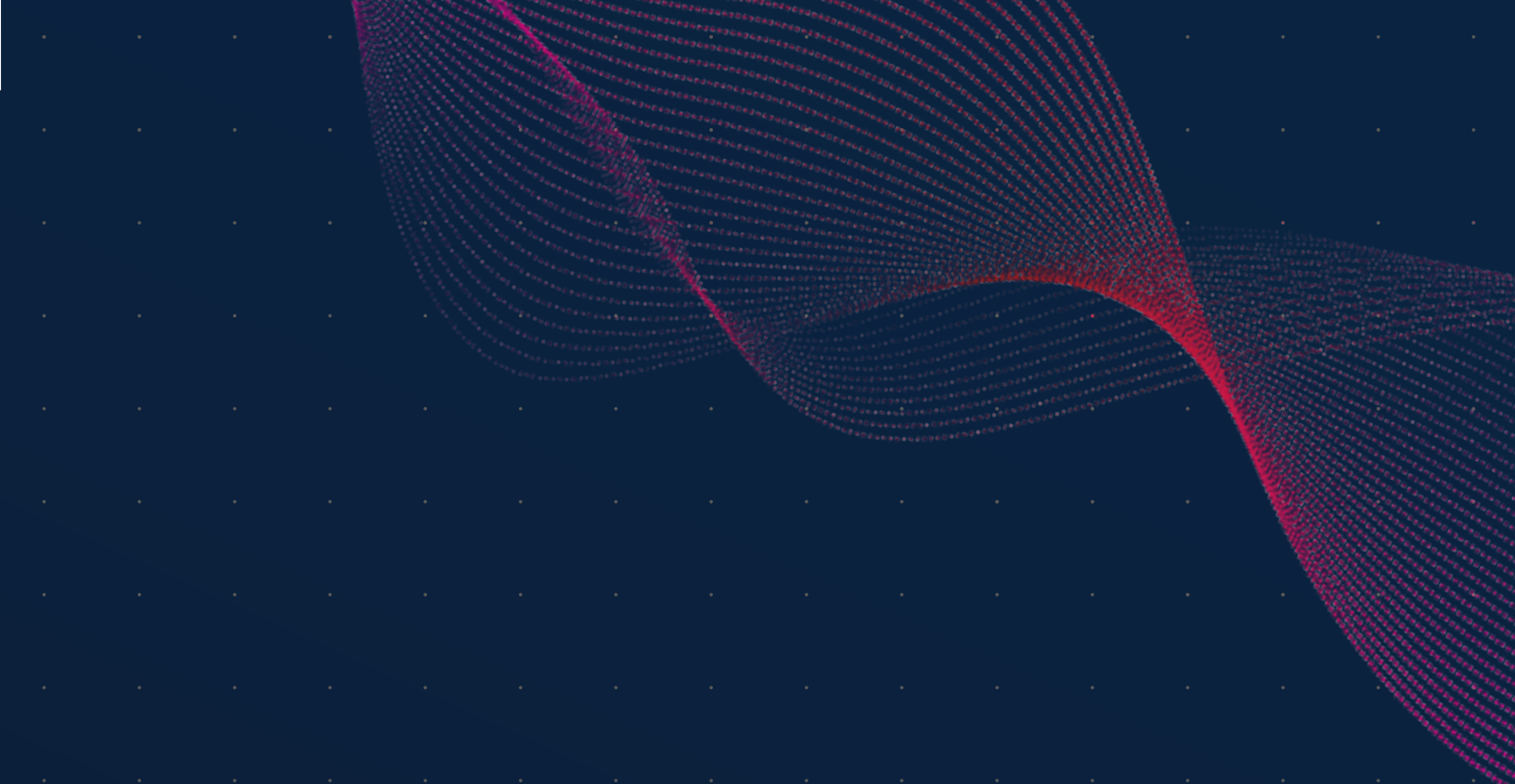
Besides the team that manages Active Directory, you need to involve other teams, such as your incident response team, in your planning to challenge this task. Have clear criteria in place for invoking the AD DR plan and clear responsibilities for executing it. Combine this with a clear communications strategy.

Above all, carefully consider investments for disaster prevention—this can be cheaper than disaster recovery.

## ABOUT THE AUTHORS

**GUIDO GRILLENMEIER** is Chief Technologist with Semperis. Based in Germany, Guido was a Microsoft MVP for Directory Services for 12 years. He spent 20+ years at HP/HPE as Chief Engineer. A frequent presenter at technology conferences and contributor to technical journals, Guido is the co-author of Microsoft Windows Security Fundamentals. He’s helped various customers secure their Active Directory environments, and supported their transition to Windows 10/m365 and Azure cloud services.

**GIL KIRKPATRICK** is Chief Architect for products at Semperis. Gil has been building commercial products for enterprise IT for many years, focusing primarily on identity management and security-related products. He is a 15-time Microsoft MVP for Active Directory and Enterprise Mobility, author of Active Directory Programming, and founder of the Directory Experts Conference. Gil speaks on cyber-security, identity, and disaster recovery topics at IT conferences around the world.



+1-703-918-4884  
info@semperis.com  
www.semporis.com

221 River Street  
9th Floor  
Hoboken, NJ 07030

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 50 million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in New Jersey and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winning Hybrid Identity Protection conference ([www.hipconf.com](http://www.hipconf.com)). The company has received the highest level of industry accolades, most recently ranked #157 in the Inc. 5000 and the fourth fastest-growing company in the tri-state area and 35th overall in Deloitte's 2020 Technology Fast 500™. Semperis is accredited by Microsoft and recognized by Gartner.