What to Watch for When Using the

Microsoft Active Directory Forest Recovery Guide

By Sean Deuby

Semperis Principal Technologist | North America

15-year Microsoft MVP Alumnus

semperis

Table of Contents

The Complexities of **Active Directory Forest Recovery**

The ability to recover your Active Directory (AD) environment entirely from backup is no longer a nice-to-have response to a highly unlikely event. Given the onslaught of cyberattacks that target AD, the ability to recover AD to a known-secure state following a cyber disaster is a requirement.

Why do so few organizations put together and test a disaster recovery plan for what is unquestionably one of a company's most critical pieces of software plumbing?

Two major reasons: First, AD is notably reliable as a core infrastructure service. It's a distributed application across multiple instances, and failures of one or more of these servers won't prevent the service from continuing. In a properly maintained AD forest, domain or forest failure (without outside interference) is a rare occurrence.

Second, recovery from a domain or forest failure is a decidedly non-trivial task and difficult to replicate in a disaster recovery test environment. Microsoft's Planning For Active Directory Forest Recovery guide is a high-level procedure that you must extensively customize for your environment.

Although it began life as a single document, during the quarter-century of AD's existence the AD forest recovery process has evolved into a collection of web pages on the Microsoft site. These pages also reference many other pages relevant to the process. As a result, if you're just clicking through the web pages, it's easy to underestimate the magnitude of the recovery process: **40 pages of core planning and recovery processes with 109 pages of cross-references to more than 22 appendices.** At 149 pages, the AD forest recovery process isn't something to look at only when a cyber crisis occurs.

In this tour of the Microsoft guide, I'll point out some challenges with manual recovery that can prolong the recovery process—and increase downtime.

Assumptions

The Microsoft guide starts with some assumptions, including that you've worked with Microsoft support to determine the cause of the AD failure and concluded that restoring the entire forest is the best course of action. The guide also assumes that you'll be conducting a "generic" forest recovery—the guide doesn't cover all possible scenarios.

Pay particular attention to Microsoft's assumption that you've followed the best-practice recommendations for using AD-integrated Domain Name System (DNS). "Specifically, there should be an Active Directory-integrated DNS domain for each AD domain":

> **Note**
>
> Although the objectives of this guide are to recover the forest and maintain or restore full DNS functionality, recovery can result in a DNS configuration that is changed from the configuration before the failure. After the forest is recovered, you can revert to the original DNS configuration. The recommendations in this guide do not describe how to configure DNS servers to perform name resolution of other portions of the corporate namespace where there are DNS zones that are not stored in AD DS.

If you're using a third-party DNS, have you planned for this?

Prerequisites

Microsoft also recommends several prerequisites, including having a documented recovery plan with procedures:

You have a documented recovery plan with procedures

You should have a documented recovery plan with procedures for AD DS domain/forest recoveries, object/subtree recoveries, and SYSVOL recoveries that have been tested in a lab environment using production backups. The recovery procedures should be vetted on a routine basis (for example, annually) and the documentation updated as required by OS upgrades, architectural changes to the AD DS environment, or any other changes that ensure the procedures are kept up to date. For more information and guidance on these procedures, refer to the AD Forest Recovery – Procedures section of this guide.

Do you have a documented, tested, and maintained Active Directory disaster recovery (DR) plan?

You should also have a backed up and restored AD forest in a lab environment. If you don't, you'll need to consult a couple of additional guides Microsoft offers on backing up a full server and Performing Nonauthoritative Restore of Active Directory Domain Services:

You have backed up and restored AD DS and SYSVOL in a lab environment

You should have backed up and restored AD DS and SYSVOL in a lab environment on a regular basis. For more information, see AD Forest Recovery - Backing up a full server. and Performing Nonauthoritative Restore of Active Directory Domain Services.

Do you have a backed up and restored AD forest?

Identify the problem

If you take away nothing else from Microsoft's guide, heed this warning: "This guide doesn't cover security recommendations for how to recover a forest that has been hacked or compromised." The guide does not focus on cyber incidents and instead refers you to other resources to secure AD. In other words, the guide implies that you should have hardened your AD so an attack didn't happen in the first place. In today's hybrid environment, it also doesn't cover re-synchronizing your recovered AD forest with your cloud identity provider (such as Entra ID):

> [!IMPORTANT] This guide doesn't cover security recommendations for how to recover a forest that has been hacked or compromised. In general, it's recommended to follow Best Practices for Securing Active Directory and Pass-the-Hash mitigation techniques to harden the environment. For more information, see Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques.

Microsoft's guide doesn't cover cyber incidents—in other words, they're saying that you should have hardened your AD so this didn't happen.

What will be lost

In this section, the Microsoft guide cautions that the restore operation will result in losing at least some Active Directory data, including "all objects (such as users and computers) that were added after the last trusted backup." A few points to make here:

- It's possible but rare that IT staff are tracking which objects were added or updated since the last backup.
- A medium to large AD forest will have thousands to tens of thousands of changes daily—and most of those will be lost.
- Loss of data and the difficulty of re-syncronizing with your cloud identity provider are why a valid, malware-free, recent backup set is critical.

What will be lost

The restore operation will result in the loss of at least the following Active Directory data:

- All objects (such as users and computers) that were added after the last trusted back up
- All updates that were made to existing objects since the last trusted back up
- All changes that were made to either the configuration partition or the schema partition in AD DS (such as schema changes) since the last trusted back up

Many organizations will have thousands to tens of thousands of AD forest changes daily—most of which will be lost.

Password knowledge

The Microsoft guide specifies that to conduct an AD forest recovery, you must know the "password of a Domain Admin account for each domain in the forest."

Do you have your passwords (and documentation and tools) stored in a location that is **NOT** AD-dependent, such as on paper in a locked safe?

Password knowledge

1. You must know the password of a Domain Admin account for each domain in the forest. Preferably, this is the password of the built-in Administrator account.
2. You must also know the DSRM password to perform a system state restore of a DC.

It's a good practice to archive the Administrator account and DSRM password history in a safe place for as long as the backups are valid. That is, within the tombstone lifetime period or within the deleted object lifetime period if Active Directory Recycle Bin is enabled.

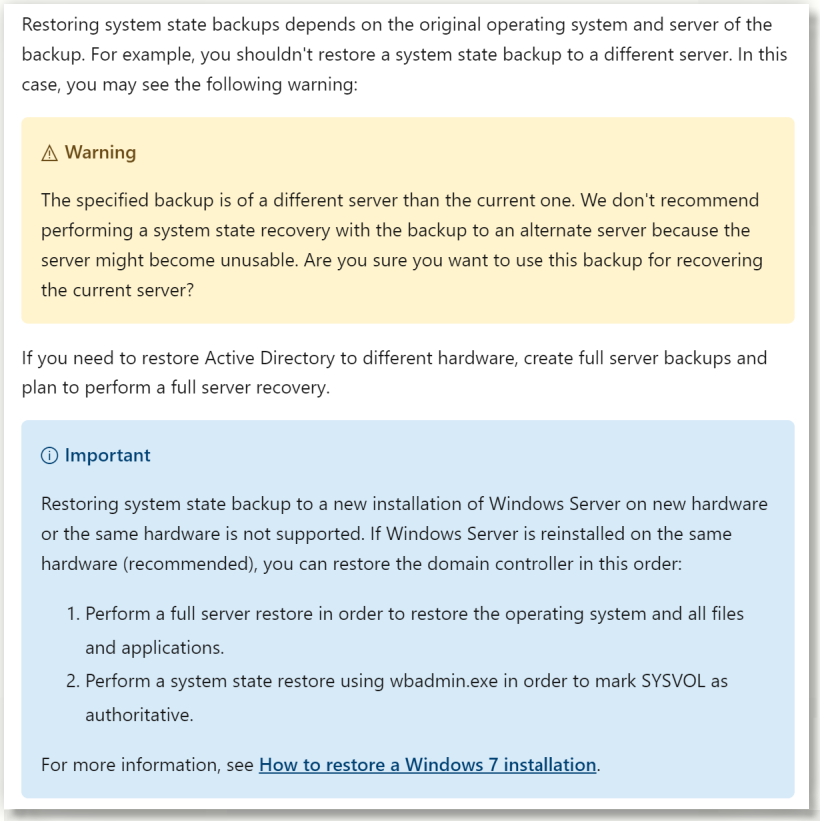
Note that you must know the Directory Services Restore Mode (DSRM) password to perform a system state restore of a DC—and those must be set individually for each DC. (If you don't know what DSRM is, you have some studying to do.) Do you keep track of your previous Administrator and DSRM passwords?

Determine which backups to use

The Microsoft guide points out some complications with restoring system state backups. For example, "you shouldn't restore a system state backup to a different server."

Here are some further points to consider when selecting AD backups for recovery:

- Conventional backups back up the entire OS, including the hardware abstraction layer (HAL), which ties the OS and the backup to the hardware. Thus, you're restricted as to what hardware you can recover to.
- Conventional backups also contain any malware that lingers in the OS since you're backing up the whole OS.
- You can't move forward in recovery until you've found a clean backup or are sure you'll be able to eliminate the malware after you restore it.
- The older your backup, the more challenging it becomes to re-synchronize with your cloud identity provider—another reason to use the most recent backup available.



Restoring system state backups depends on the original operating system and server of the backup. For example, you shouldn't restore a system state backup to a different server. In this case, you may see the following warning:

⚠ Warning

The specified backup is of a different server than the current one. We don't recommend performing a system state recovery with the backup to an alternate server because the server might become unusable. Are you sure you want to use this backup for recovering the current server?

If you need to restore Active Directory to different hardware, create full server backups and plan to perform a full server recovery.

ⓘ Important

Restoring system state backup to a new installation of Windows Server on new hardware or the same hardware is not supported. If Windows Server is reinstalled on the same hardware (recommended), you can restore the domain controller in this order:

1. Perform a full server restore in order to restore the operating system and all files and applications.
2. Perform a system state restore using wbadmin.exe in order to mark SYSVOL as authoritative.

For more information, see How to restore a Windows 7 installation.

Two factors that can significantly delay your AD recovery: Restrictions on the hardware you can recover to, and the possibility that your AD backups contain malware.

Determine which domain controllers to restore

The Microsoft guide lays out an exhaustive list of criteria for deciding which domain controllers to restore, with this rather obvious preamble: "A good backup is a backup that can be restored successfully, was taken a few days before a failure, and contains as much useful data as possible."

> ⓘ Important
>
> Maintain security procedures when handling or restoring backup files that include Active Directory. The urgency that accompanies forest recovery can unintentionally lead to overlooking security best practices.

Note the warning about handling the AD backups with care to avoid security risks—especially important during a cyber incident.

Recover the forest in isolation

Microsoft recommends that you shut down all writeable domain controllers before bringing the first restored DC back into production to avoid replicating dangerous data.

> ⓘ Note
>
> There may be cases where you move the first DC that you plan to recover for each domain to an isolated network while allowing other DCs to remain online in order to minimize system downtime. For example, if you are recovering from a failed schema upgrade, you may choose to keep domain controllers running on the production network while you perform recovery steps in isolation.

Though response tactics vary, the recommendation about keeping some DCs running on the production network while performing recovery in isolation can be particularly applicable in a cyber incident.

Identify the current forest structure and DC functions

Making a list of all the DCs in the domain is a good idea—has your team done this? And is the list available if AD is down?

> ### Identify the current forest structure and DC functions
>
> Determine the current forest structure by identifying all the domains in the forest. Make a list of all of the DCs in each domain, particularly the DCs that have backups, and virtualized DCs which can be a source for cloning.
>
> A list of DCs for the forest root domain is the most important because you'll recover this domain first. After you restore the forest root domain, you can obtain a list of the other domains, DCs, and the sites in the forest by using Active Directory snap-ins.

This inventory of DCs and backups should be done in advance—not during a cyberattack.

Virtualized DCs

Microsoft recommends that you move virtualized DCs to a virtual network that's isolated from the production network to avoid propagating problems and to facilitate testing the DCs before you put them back into production.

Virtualized DCs

If you're running virtualized DCs, you can move them to a virtual network that is isolated from the production network where you'll perform recovery. Moving virtualized DCs to a separate network provides two benefits:

- Recovered DCs are prevented from reproducing the problem that caused the forest recovery.
- Virtualized DC cloning can be performed on the isolated network so that a critical number of DCs can be running and tested before they're brought back to the production network.

Does management of your virtual infrastructure (e.g., VMware vCenter) depend on AD? If you don't have access to AD, you don't have access to vCenter.

Large forests

Forest recovery in a large, multi-site deployment is a huge logistical challenge—especially in a crippled network. The guide's recommendation to deploy remote management technology begs the question: What if that system depends on AD for authentication?

Large forests

In a large forest spread across multiple locations, it can be difficult to guarantee that all writeable DCs are shut down. For this reason, the recovery steps—such as resetting the computer account and krbtgt account, in addition to metadata cleanup—are designed to ensure that the recovered writeable DCs don't replicate with dangerous writeable DCs (in case some are still online in the forest).

However, only by taking writeable DCs offline can you guarantee that replication doesn't occur. Therefore, whenever possible, you should deploy remote management technology that can help you to shut down and physically isolate the writeable DCs during forest recovery.

But does your remote management technology depend on AD for authentication? And where are you storing all those passwords? Does that system depend on AD?

Restore the first writeable domain controller in each domain

You can get a sense of how tedious and time-consuming a full AD forest recovery is by the number of times the guide states "repeat the same steps." Manual recovery is an arduous, error-prone process. And if you make a mistake, you have to start over.

The guide makes passing reference to the important of restoring a writeable DC from backup "that hasn't been influenced by whatever caused the forest to fail." If the cause was a cyberattack, it's likely that the backup contains malware. As a side note, restoring a DC from backup is the only step in the recovery process where conventional backup and recovery solutions are helpful.

Here are some important considerations to keep in mind about restoring the first domain—and these are **just some** of the steps in the process.

> ### Restore the first writeable domain controller in each domain
>
> Beginning with a writeable DC in the forest root domain, complete the steps in this section in order to restore the first DC. The forest root domain is important because it stores the Schema Admins and Enterprise Admins groups. It also helps maintain the trust hierarchy in the forest. In addition, the forest root domain usually holds the DNS root server for the forest's DNS namespace. Consequently, the Active Directory–integrated DNS zone for that domain contains the alias (CNAME) resource records for all other DCs in the forest (which are required for replication) and the global catalog DNS resource records.
>
> After you recover the forest root domain, repeat the same steps to recover the remaining domains in the forest. You can recover more than one domain simultaneously; however, always recover a parent domain before recovering a child to prevent any break in the trust hierarchy or DNS name resolution.

If you don't have a good backup of the root domain, you can't recover the forest.

> For each domain that you recover, restore one writeable DC from backup. This is the most important part of the recovery because the DC must have a database that hasn't been influenced by whatever caused the forest to fail. It's important to have a trusted backup that is thoroughly tested before it's introduced into the production environment.

Critical questions: Is the AD backup malware-free? Has the threat actor made changes to AD itself—possibly leaving backdoors open to persistence?

> - Perform a full server recovery and then force an authoritative synchronization of SYSVOL. For detailed procedures, see Performing a full server recovery and Perform an authoritative synchronization of DFSR-replicated SYSVOL.

The processes of performing a full server recovery and synchronizing SYSVOL are long, involved procedures in themselves.

> 1. If you plan to restore a physical server, ensure that the network cable of the target DC isn't attached and therefore isn't connected to the production network. For a virtual machine, you can remove the network adapter or use a network adapter that is attached to another network where you can test the recovery process while isolated from the production network.

Anyone planning to restore to a physical server should heed this warning about network cabling and adapters. If you don't have an ILO or some other out-of-band management solution, someone must be present to manage this process.

> 8. Clean up metadata of all other writeable DCs in the forest root domain that you aren't restoring from backup (all writeable DCs in the domain except for this first DC). If you use the version of Active Directory Users and Computers or Active Directory Sites and Services that is included with Windows Server 2012 or later or RSAT for Windows 10 or later, metadata cleanup is performed automatically when you delete a DC object. In addition, the server object and computer object for the deleted DC are also deleted automatically. For more information, see Cleaning metadata of removed writable DCsand Clean up AD DS server metadata.

You need to clean up the metadata for every DC in the forest except what you restored.

Until the metadata of all other DCs in the domain is removed, this DC, if it were a RID master before recovery, won't assume the RID master role and therefore won't be able to issue new RIDs. You might see event ID 16650 in the System log in Event Viewer indicating this failure, but you should see event ID 16648 indicating success a little while after you have cleaned the metadata.

In other words, until you've removed this metadata, you can't proceed with recovery.

9. If you have DNS zones that are stored in AD DS, ensure that the local DNS Server service is installed and running on the DC that you have restored. If this DC wasn't a DNS server before the forest failure, you must install and configure the DNS server role on the DC or a DNS server needs to be available on the restoration environment.

Important point about installing and configuring the DNS server role.

In the _msdcs and domain DNS zones, delete NS records of DCs that no longer exist after metadata cleanup. Check if the SRV records of the cleaned up DCs have been removed. To help speed up DNS SRV record removal, run:

```
nltest.exe /dsderegdns:server.domain.tld
```

Don't forget this manual step.

10. Raise the value of the available RID pool by 100,000. For more information, see Raising the value of available RID pools. If you have reason to believe that raising the RID Pool by 100,000 is insufficient for your particular situation, you should determine, taking into account the average RID consumption on your environment, the lowest increase that is still safe to use. RIDs are a finite resource that shouldn't be used up needlessly.

Configuring the RID pool for recovery involves additional steps covered in other sections of the guide.

14. If the forest has multiple domains and the restored DC was a global catalog server before the failure, clear the **Global catalog** check box in the NTDS Settings properties to remove the global catalog from the DC. The exception to this rule is the common case of a forest with just one domain. In this case, it isn't required to remove the global catalog. For more information, see Removing the global catalog.

Removing (unhosting) the Global Catalog is a slow process you have little control over. In a large environment, this can take hours.

The presence of lingering objects can lead to problems. For instance, e-mail messages might not be delivered to a user whose user object was moved between domains. After you bring the outdated DC or global catalog server back online, both instances of the user object appear in the global catalog. Both objects have the same e-mail address; therefore, e-mail messages can't be delivered.

"The presence of lingering objects can lead to problems." This is an understatement.

Reconnect each restored writeable domain controller to a common network

As the guide points out, at this point, you should have one DC restored for every domain in your forest, and all the recovery steps completed. You now have a seed forest of one DC per domain. Some important questions to ask at this point:

- Is it working correctly?
- Is it malware-free?
- What changes has the threat actor made to AD—and how do you find out?
- What changes to the forest have been lost due to the recovery

At this stage, you should have one DC restored (and recovery steps performed) in the forest root domain and in each of the remaining domains. Join these DCs to a common network that is isolated from the rest of the environment and complete the following steps in order to validate forest health and replication.

Congratulations, you now have the start of a recovered AD forest—but it cannot yet handle prime time (a production load).

Verify forest replication health

Next, the guide says "After validation, join the DCs to the production network and complete the steps to verify forest replication health." This is **not** the recommended order of operations in a cyber incident: You should validate health before you restore to a corporate network.

> After validation, join the DCs to the production network and complete the steps to verify forest replication health.

NO! Validate health before you restore to the corporate network. Validate in an isolated AD before thousands of clients and servers hit it simultaneously.

Add the Global Catalog to a DC in the forest root domain

The guide discusses the importance of the Global Catalog, but the lengthy process of adding the GC to the forest root domain is contained in a separate section of the guide.

> **Note**
>
> A DC will not be advertised as a global catalog server until it has completed a full synchronization of all directory partitions in the forest. Therefore, the DC should be forced to replicate with each of the restored DCs in the forest.

Note that adding (rehosting) the GC takes even longer than removing it.

Redeploy remaining DCs

At this point, you have a clean forest but it doesn't have the capacity to support your production network of servers and PCs. The next step describes the need to add capacity to your recovery forest by rebuilding the remaining DCs from your old forest to be a part of the new forest. This entails forcibly removing the AD DS role from each DC (now a server) and repromoting it, either "over the wire" or with "install from media," to support the new forest.If you're well-organized, you could start this process in parallel with the forest recovery. However, you must also ensure DCs remain preserved in their corrupted state for legal and forensic reasons.

> The next step is to install AD DS on all DCs that were present before the forest recovery took place. If the DCs still exist, the AD DS service will need to be removed forcibly, or the DCs can be reinstalled. Any existing backups for these DCs can't be reused, because the corresponding metadata has been removed during forest recovery. In an uncomplicated environment this redeployment process can be as simple as reconnecting the recovered DCs to the production network, and promoting new DCs as needed.
>
> In a large enterprise faced with a worldwide infrastructure, a more sophisticated plan is needed. The first phase is usually to restore AD as a service; install strategically placed DCs such that all critical business divisions and applications can start working again. (It may be acceptable for branch offices to temporarily have reduced performance as a result of this.) As a second phase, all remaining and less critical DCs are redeployed.

Redeploying DCs is a complicated process and geographically distributed effort, executed while everyone is highly stressed. Automation tools can significantly expedite the promotion process.

Need Help
Recovering Active Directory?

In our engagements with customers who have suffered attacks that wiped out their AD infrastructure, we've learned that many organizations don't yet have a fully tested AD recovery plan. This puts organizations at risk of prolonged downtime given that that 90% of cyber incidents involve AD and 33% of organizations have no AD defense in place.

If you need help developing and testing an AD recovery plan, **contact us**. Semperis has a deep bench of AD forest recovery experts who can help you through the process. Our comprehensive cyber resilience solution, Semperis Active Directory Forest Recovery (ADFR), automates AD forest recovery to a malware-free environment, reducing recovery time by up to 90%. Our incident response team can help you set up and run AD disaster drills and set RTO objectives. Our mission is to be a "force for good" by defending against escalating cyberattacks.

semperis

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

5 Marine View Plaza, Suite 102, Hoboken, NJ 07030