WHITEPAPER

Commvault

# Active Directory Forest Recovery

## OVERVIEW

After 25 years, Microsoft Active Directory (AD) remains the cornerstone of most enterprise networks, providing essential authentication and authorization for business-critical applications and resources. However, its central role has also made it a primary target for attackers aiming to compromise enterprises or, in some cases, bring down the entire network. Every minute that AD is unavailable, employees can't log in, critical services come to a halt, and your business is at a standstill.

When disaster strikes, recovering Active Directory is vital, yet it has traditionally been very hard to do, requiring intricate, time-consuming, manual processes.

Having a well-documented and frequently tested recovery plan to restore and rebuild your entire AD environment to a pre-attack state is not just a good idea – it's the key to getting your business back online fast.

## THE COMPLEXITY OF RECOVERING ACTIVE DIRECTORY

Active Directory is a geographically distributed identity system that serves the authentication and authorization needs of business-critical applications and users. Its multi-master design means that every domain controller (DC) holds a copy of the AD database, allowing changes to be made on any DC and then propagated throughout the network.

In many organizations, the Active Directory forest combines several domains linked together, each supported by many domain controllers that serve a distributed employee base. Each domain houses a complex hierarchy of users, groups, computers, Group Policies, and the permissions between them. The seamless operation of these domains relies on the continuous synchronization between domain controllers. To provide structure and order, important roles are delegated amongst domain controllers.

The design of Active Directory provides for high availability and resiliency but introduces complexity that makes the process of rebuilding AD from a disaster or cyberattack, like ransomware, complex and time-consuming.

The hallmark of ransomware is that once it infiltrates an environment, it indiscriminately spreads to any server it can gain access to. Inevitably, some of those servers are domain controllers, and when their files are encrypted and the operating system cannot boot, Active Directory is taken offline. Cyber incidents that impact AD availability have a profound impact on business operations and can bring an organization to its knees.

Unfortunately, the task of recovering an entire Active Directory forest is intricate, complicated, and requires significant upfront planning. When faced with disaster, time is money, and the longer it takes to restore AD components back to a good working state, the greater the disruption to the business.

## ACTIVE DIRECTORY FOREST RECOVERY

Microsoft provides prescriptive guidance on rebuilding an entire AD forest after a catastrophic disaster in their Active Directory Forest Recovery Guide. Due to the complex nature of AD, the elements involved in a full forest recovery are rigid, prescriptive, time-consuming, and highly susceptible to human error. At the highest level, a full forest recovery breaks down into the following components:

### 1 Planning

Knowing how to execute the tasks involved in an AD forest recovery is only part of the battle. Without the appropriate upfront planning, a recovery won't even be possible. Before developing a disaster recovery (DR) or cyber recovery (CR) plan for your AD environment, it's important to understand and document the following:

- What does your organization's AD architecture entail? What domains are part of the forest, and what are the trust relationships between them?
- How many domain controllers support this infrastructure, and what sites do they belong to?
- If AD became unavailable, what is the minimal viable infrastructure that needs to be rebuilt to bring my core business operations back online?
- What are the most critical dependencies on your AD infrastructure? What business applications rely on AD to function?
- Which domains and sites are the highest priority to rebuild so their dependencies are re-established as early as possible during a recovery effort?

### 2 Backups

It's important to identify what type of backups of domain controllers are necessary to support your recovery plans. Are full server backups required? Will backups of the DC's system state satisfy the recovery strategy? When a cyber incident impacts the availability of your AD, it's too late. A backup strategy needs to be proactively defined, implemented, documented as part of your overall disaster recovery plan, and monitored regularly to verify successful backups are created.

The following are important to consider when determining what and how to backup to protect your Active Directory:

- Confirm the type of backup you plan to use supports your recovery plan. Depending on how you plan to restore, system state backups of the domain controller could be sufficient, or you may need full server backups.
- Your recovery plans should cover scenarios addressed with in-place restores of AD (to roll back from schema corruption, for example) as well as scenarios that require out-of-place restores to new servers (to rebuild from a ransomware attack).
- Document your AD topology, including the servers that possess critical roles in your AD environment, including forest-level flexible single master operation (FSMO) roles (Schema Master, Domain Naming Master), domain-level FSMO roles (PDC Emulator, RID Master, Infrastructure Master), Global Catalogs, and DNS Servers.
- Combine Microsoft recommendations with knowledge of your AD architecture to determine which domain controllers should be restored first after a disaster. Make sure these DCs are being backed up and can be physically or virtually accessed when core AD services are unavailable.
- Plan for redundancy. Don't rely on backing up just one domain controller per domain. Make sure multiple DCs are backed up regularly. When disaster strikes, you want to have options, as some servers will be unavailable.

- Plan for scale. If your organization is geographically distributed, chances are recovering a single DC from an AD domain will not be sufficient to support the authentication needs of your users and business-critical applications. Define the minimal viable infrastructure required to get your business back up and running and make sure you are backing up enough DCs to support that as part of your recovery plan.
- VM snapshots won't cut it. Because of the multi-master nature of Active Directory, it's not possible to bring back domain controllers at scale using VM snapshots. Dozens of intricate hygiene steps need to be performed on the recovered domain controller and within AD itself at very specific points throughout the forest recovery. Failing to execute these tasks at the correct time will introduce new corruption in the recovered environment. Introducing multiple domain controllers from snapshots will introduce inconsistencies that may not be resolvable.

## 3 Critical hygiene tasks

Only 20% of the tasks in an AD forest recovery involve restoring AD data from backups. The remainder are highly technical AD hygiene tasks that must be executed in specific order before and after the recovery jobs. These tasks help make sure that the operational roles within AD are properly tuned, and new corruption isn't introduced into the rebuilt AD environment.

When designing your recovery plans for AD, consider the following:

- **Read and internalize the Microsoft forest recovery guidance and steps.** Understanding what each task entails and the tools that are required to accomplish them is important to avoid confusion and errors when recovering. Each hygiene task described in the Microsoft documentation compromises multiple steps and often involves subtasks that require navigating between various tools to get all the information needed.
- **Make detailed notes on how to execute the tasks within your AD environment.** The Microsoft guidance offers detailed instruction, but there are still many decisions to be made that are determined by how your AD is configured. For example, if a DC needs to be rebooted, make sure the team carrying out the recovery knows where to locate the DSRM (Directory Services Restore Mode) passwords.
- **Test your plan regularly.** Reading Microsoft documentation is not enough; you need to perform an actual forest recovery to an isolated DR environment. Only through carrying out a full end-to-end recovery will you identify gaps in your recovery plan. Consider testing the AD recovery plan every 3 – 6 months. Use these tests as an opportunity to both validate your plan and update the forest recovery guidance based on any recent changes to the AD architecture or topology.

## THE PHASES OF A FOREST RECOVERY

If you have a single Active Directory domain, only a few domain controllers and a small user population, then consider yourself lucky. In this case, restoring the AD domain from a failure should be straightforward: simply bring back one domain controller from a backup or snapshot, and then recreate the remaining few DCs.

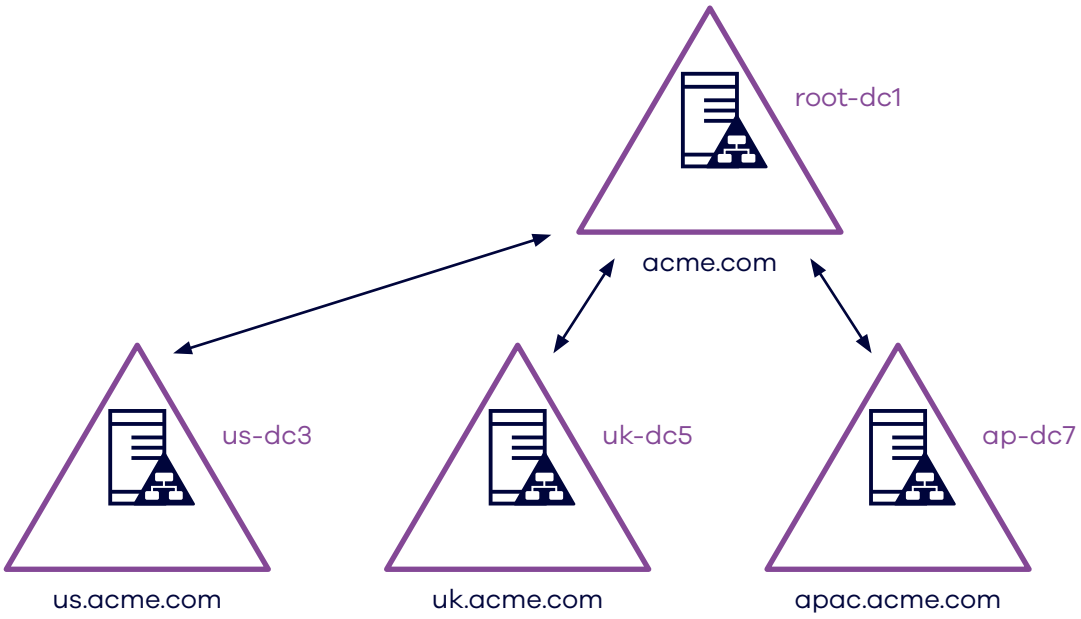
However, if your AD architecture comprises multiple domains and supports a user base that is geographically distributed across multiple offices, countries, and even continents, the considerations outlined in the Microsoft Active Directory Forest Recovery Guide are relevant and important to your ability to restore AD services after an outage.

At scale, an AD forest recovery approach is divided into three distinct phases. Each phase serves to accomplish a key milestone on the journey to rebuilding the entire original AD topology.

## **Phase 1** – Restore the first DC from backup for every AD domain

The first phase involves restoring the first domain controller from each domain in the forest to re-establish the basic structure of the original AD architecture. With a single DC supporting each AD domain, you can verify trust relationships, confirm replication, and test basic administrative operations (such as creating new objects) to confirm that all roles have been properly reconfigured.

In this phase, the root domain must be restored first. Only after the root domain has been recovered and all AD hygiene tasks addressed, can child domains be restored. If there are multiple levels of child domains, each child domain will have to wait until its parent domain recovery has been completed.

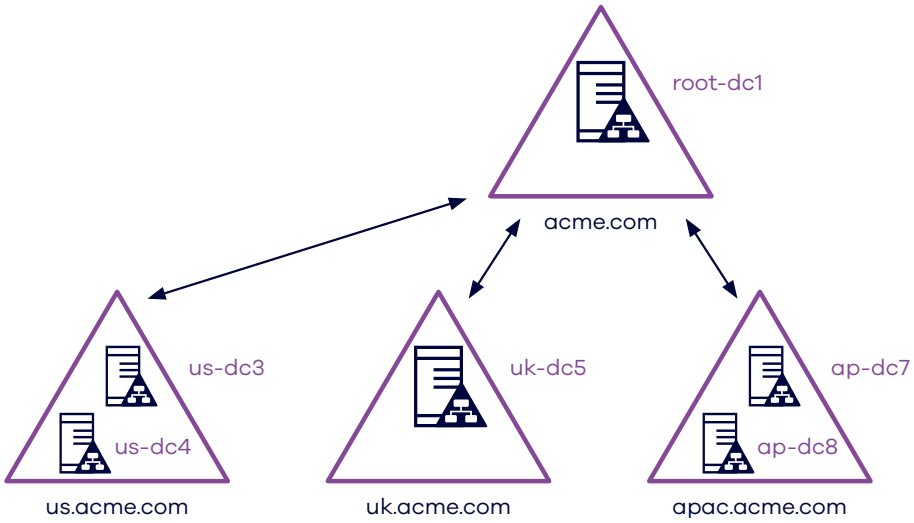



**Phase 1:** After restoring the first domain controller of the root domain, acme.com, from backup and completing the necessary hygiene tasks, the first domain controller of each child domain is restored from backup, with the essential hygiene steps completed after each domain controller restoration.

This first phase is an important milestone to confirm the structure of AD is supporting the infrastructure. However, in any mid- to larger size organization, and any environment that is spread across multiple geographical locations, more work is required before the recovered environment can be re-introduced into production.

## **Phase 2** – Restore additional DCs from backup

The second phase is where additional DCs are restored from backup to quickly establish a minimal viable AD infrastructure. This minimal viable infrastructure should be sufficient to service the authentication needs of business-critical applications and support users distributed across multiple geographies.



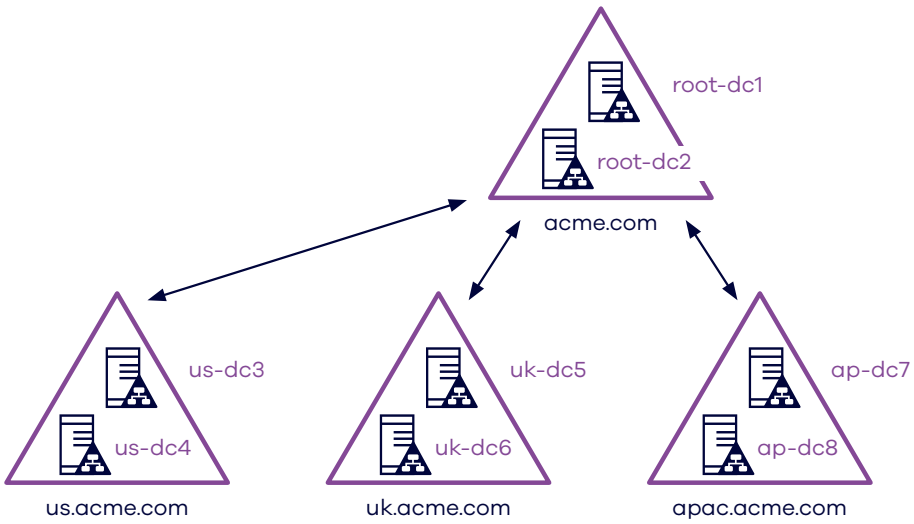

**Phase 2:** Additional domain controllers in child domains us.acme.com and apac.acme.com are restored from backup to enable a minimal viable infrastructure to service user and application authentications across all geographies.

Restoring the additional domain controllers from backup enables the minimal viable infrastructure is in place more quickly, allowing business operations to resume sooner. Other methods of re-establishing the remaining DCs – like those discussed in the third phase – can take much longer. Restoring as many DCs from backup as possible accelerates the overall recovery process and helps minimize disruption and costs associated with downtime.

During this phase, many DCs can be restored in parallel, although this requires significant coordination and resources to monitor the various recovery jobs and execute the necessary hygiene tasks following each restore. For example, after each DC is restored from backup, its computer password in the directory needs to be reset twice. It's also a good idea to disable Windows Update during the recovery to minimize any additional disruptions until the entire forest has been rebuilt.

## **Phase 3** – Promote the remaining AD infrastructure

The final phase is where the remaining infrastructure is promoted or repromoted to mirror the AD architecture before the disaster.




**Phase 3:** Remaining domain controllers are promoted in the root domain acme.com and remaining child domain uk.acme.com to complete the original AD architecture.

This can be accomplished by demoting and re-promoting domain controllers from the original forest or promoting new servers to replace the DCs that were present in the original topology.

Promoting these remaining servers (historically referred to as a "DCPromo") creates a brand new domain controller that will replicate the entire AD database from its nearest replication partners. For this reason, the third phase should be timed to prevent the network traffic created due to replication from interfering with short term business continuity goals. Using the "Install from media" option during the DC promotion can help minimize the amount of changes that need to be replicated to the newly promoted DC.

## KEY TAKEAWAYS

Active Directory forest recovery is foundational to maintaining continuous business after a cyberattack, but using traditional methods can make it a daunting task.

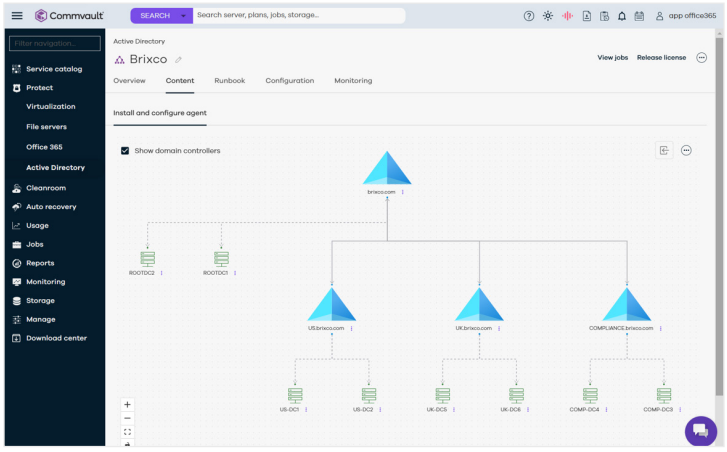
- If your Active Directory consists of multiple domains and geographies, there are significant challenges to recovering the entire AD forest quickly in the face of disaster.
- While the Microsoft guidance is prescriptive, it is also detailed and involved. Depending on the complexity of your AD architecture, there can easily be 50 to 100 or more individual tasks involved in restoring AD back to a previous good state.
- Relying on a manual disaster or cyber recovery plan and out-of-box Microsoft tools, could mean it takes days to restore an entire AD forest. Given the high cost of business disruption caused by an AD outage, consider automating the recovery process wherever possible.

## COMMVAULT® CLOUD BACKUP & RECOVERY FOR ACTIVE DIRECTORY

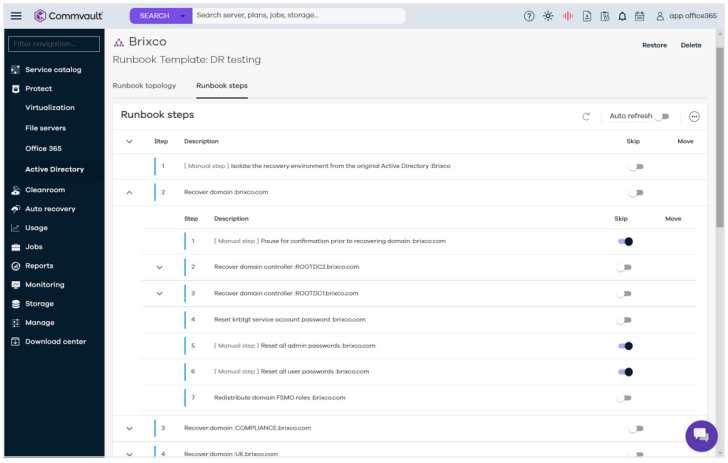
### Accelerate Active Directory Recovery and Advance Resilience with Commvault Cloud

In the face of deletion, corruption, or cyberattacks, Commvault Cloud Backup & Recovery for Active Directory delivers fast recovery and enables continuous business across the enterprise. Commvault Cloud enables rapid, automated recovery of the Active Directory forest, allowing you to recover the business-critical system in hours compared to days or weeks with manual recovery processes.

**Enable fast recovery of the most important Active Directory infrastructure:** Visual topology views of your Active Directory environment enable simple and rapid identification of which domain controllers to restore first and how they should be recovered to accelerate the availability of Active Directory services.



**Accelerate Active Directory recovery via automated runbooks:** Automated forest recovery runbooks orchestrate the multi-step process required for Active Directory forest recovery, including the critical hygiene tasks required to verify consistency in the recovered AD. These runbooks can also be used for regular testing in non-production environments to enhance cyber readiness.




**Track recovery progress with prescriptive runbook views:** Prescriptive runbook views of the recovery process provide total transparency and fine-grained control, allowing you to easily tailor the workflow to your environment. During recovery, you have total visibility into where you are in the process and how long until your Active Directory is back online.