Commvault

Commvault's Guide to Active Directory Forest Recovery Scenarios

Commvault

Table of Contents

CONTENTS

WHITE PAPER

Executive Summary

This document outlines various Microsoft Active Directory (AD) forest recovery scenarios to serve as a foundational guide for organizations. For enterprises managing multiple forests, it is critical to develop a separate recovery strategy for each one. The guidance provided here focuses on recovery options available through Commvault® Cloud Backup & Recovery for Active Directory Enterprise, enabling organizations to tailor their recovery plans to meet specific business and technical requirements.

Key Considerations In Forest Recovery Planning

Effective forest recovery planning is essential so that Active Directory (AD) can be restored quickly and securely following a major event such as corruption, ransomware, or a catastrophic infrastructure failure. A well-prepared recovery plan must account for both the technical architecture of the environment and the business priorities of the organization. The complexity of an AD forest—particularly with multiple domains, global catalogs, and replication dependencies—requires careful analysis and predefined procedures. The following considerations are critical when designing and validating a forest recovery strategy, regardless of whether it is a single-domain or multi-domain forest.

Physical Topology

In environments where all domain controllers are accessible from any user location (e.g., a single-site forest), physical topology is a minor factor in recovery planning. However, for organizations with distributed users across multiple geographic regions or isolated networks, physical location becomes a significant consideration. Recovery plans must account for authentication requirements in each location.

Logical Topology

The domain hierarchy must be factored into forest recovery plans. Many enterprises follow Microsoft's original recommendation of using an "empty forest root" design, resulting in one or more child domains beneath the root and potentially even grandchild domains. Each layer introduces dependencies that can affect the recovery sequence and strategy.

Recovery Objectives and Planning

Recovery strategies will differ based on organizational priorities and technical capabilities. Some organizations may aim to restore a minimum viable AD environment as quickly as possible, while others may focus on restoring full production parity. It is essential to clearly define what constitutes a "recovered" state and to understand the trade-offs associated with each recovery path.

Global Catalog (GC) Dependencies

Identify which domain controllers hold the Global Catalog role. In a recovery scenario, especially one involving child or grandchild domains, recovering a GC early may be essential for logon and directory lookups. However, for clean recovery, GCs should be removed and rebuilt post-restore to avoid stale data.

FSMO Role Placement

The recovery process should include identification and restoration of FSMO (Flexible Single Master Operations) role holders. If FSMO roles are not available or are inconsistent post-recovery, directory functionality could be impaired. Role reassignment may be necessary during the recovery flow.

DNS Configuration

Active Directory is tightly integrated with DNS. Recovery planning must account for restoring DNS zones (especially ForestDNSZones and DomainDNSZones), rebuilding authoritative DNS servers, and validating name resolution early in the process.

RECOVERY WORKFLOWS

Commvault's Active Directory forest recovery provides automated, orchestrated recovery of an entire AD forest following events such as corruption, ransomware attacks, or domain controller failures. It enables comprehensive restoration of domain controllers, configuration partitions, domain data, trust relationships, FSMO roles, and SYSVOL, across all domains in a multi-domain forest. Recovery workflows are customizable

and support isolated, test-mode restores for validation, along with parallel domain controller rebuilds to reduce recovery time. Integrated automation and secure bootstrapping enable consistency, reduce manual intervention, and support fast forest-level recoveries in high-impact scenarios.

A successful Active Directory forest recovery requires careful execution in the correct order—starting with the first domain controller (DC) in the forest root domain. This DC acts as the cornerstone of the entire forest recovery process, housing critical components such as the schema, configuration partition, and forest-wide FSMO roles. Without it, no other domain in the forest can be safely or correctly restored. Once the forest root DC is recovered and validated, subsequent domain controllers—both in the root and child domains—can be brought online. The recovery tasks that follow are designed to provide stability, eliminate potential corruption, and establish a clean and authoritative foundation for rebuilding the forest.

Recovery of the First DC in the Forest Root

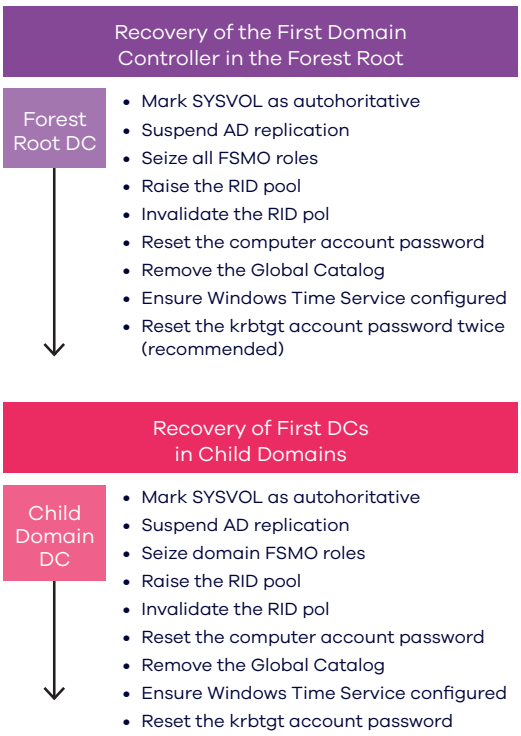
When recovering an Active Directory (AD) forest, recovery must begin with the first domain controller (DC) in the forest root domain. This DC will temporarily serve as the only controller in the forest and is critical for reestablishing forest-wide services. Once this DC is restored, a series of initial recovery operations must be performed to confirm a clean and functional environment:

- Mark SYSVOL as authoritative for the first DC in the domain/forest
- Suspend initial replication
- Seize forest and domain FSMO roles
- Raise the RID pool on the RID master
- Invalidate the RID pool
- Reset the computer account password
- Remove the Global Catalog
- Confirm Windows Time is correct on the PDC emulator
- Reset krbtgt account password twice (recommended but not required)

Recovery of Child Domains

Once the forest root DC has been successfully restored and stabilized, recovery of first DCs in child domains (immediate children of the forest root) can begin. These recoveries follow a similar procedure, but with one key difference: only domain-level FSMO roles need to be seized during child domain recovery.

- Mark SYSVOL as authoritative for the first DC in the domain
- Suspend initial replication
- Seize domain FSMO roles
- Raise the RID pool on the RID master
- Invalidate the RID pool
- Reset the computer account password
- Remove the Global Catalog
- Confirm Windows Time is correct on the PDC emulatorReset krbtgt account password twice (recommended but not required)



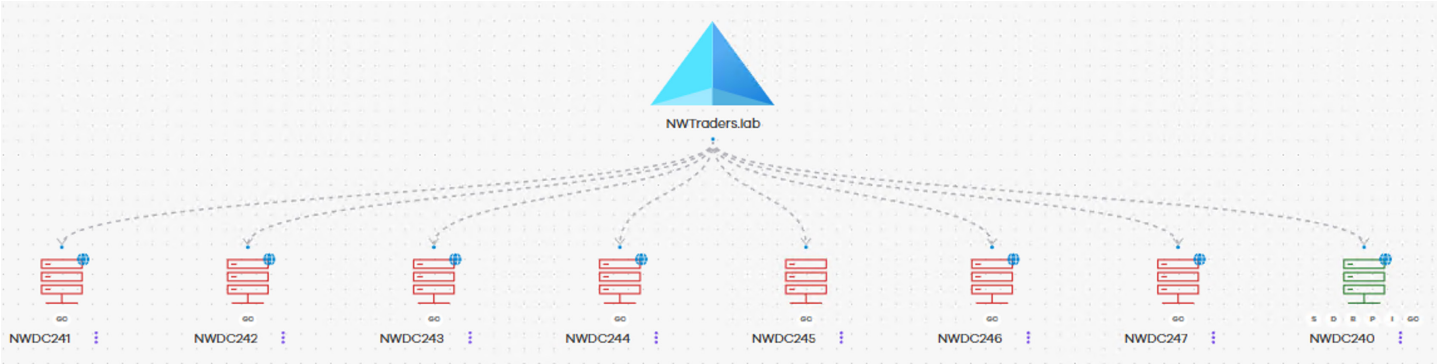
Single Domain Forest Recovery

A single-domain forest in Active Directory is the simplest logical structure for an AD environment. It consists of:

- One forest – the top-level security boundary in AD, containing the schema and global catalog.
- One domain – all users, groups, and computers exist within this domain and share the same namespace (e.g., corp.local or contoso.com). One domain tree – there are no child or sibling domains.
- One set of domain controllers (DCs) – multiple DCs can exist to provide redundancy and load balancing, but all operate within the same domain.

Key Characteristics:

- Unified security boundary – all objects share the same security policies and trust model.
- Single schema and configuration partition – simplifies management.
- No trust relationships required – since all resources reside within the same domain.
- Simpler replication topology – replication occurs only within one domain partition.



When planning for the recovery of a single-domain Active Directory forest, the primary considerations are the physical topology of the environment and the desired speed of recovery. Commvault Cloud Backup & Recovery for Active Directory Enterprise provides flexibility in recovery approaches, enabling organizations to align their recovery strategy with available resources and objectives:

Restore a Single DC and Rebuild Others via DCPromo: This method involves restoring a single domain controller from backup to a virtual machine, then using DCPromo to promote additional standby servers as DCs. This approach minimizes backup storage requirements but requires pre-staged standby servers for each additional DC to be rebuilt. It also introduces additional replication traffic as each newly promoted DC needs to replicate the entire AD database from a DC that was restored from backup.

Restore All Domain Controllers to VMs: In this scenario, all domain controllers are restored from backup directly to virtual machines. This provides a complete and direct restoration of the environment but requires backups of each DC and typically involves a longer recovery time.

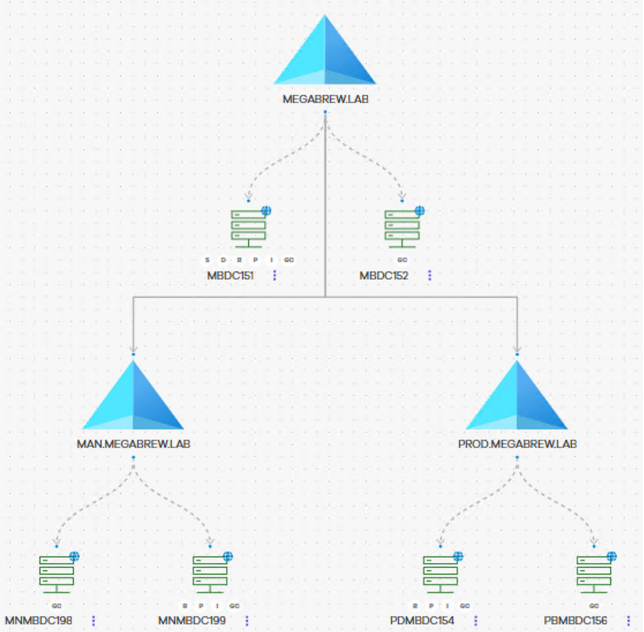
Hybrid Approach (VM Restore + DCPromo): A mixed strategy can also be used, where more than one DC is restored from backup, and the remaining DCs are rebuilt using DCPromo. This allows organizations to balance recovery time, resource availability, and infrastructure readiness.

Recovery of a Multi-Domain Forest

A multi-domain forest in Active Directory is a logical structure where a single AD forest contains two or more domains. While all domains within the forest share a common schema, configuration, and global catalog, they maintain separate security boundaries, authentication scopes, and domain-level policies.

Key Characteristics of a Multi-Domain Forest:

- Shared Forest-Level Infrastructure:
  - All domains share a single AD schema, configuration partition, and global catalog.
  - Forest-level roles (e.g., Schema Master, Domain Naming Master) are managed centrally.
- Unique Domain Namespaces: Domains can be part of the same domain tree (e.g., corp.local, hr.corp.local) or different trees (e.g., corp.local, sales.int), all within the same forest.
- Transitive Trusts: Domains within the forest automatically trust each other via two-way transitive trusts, enabling resource access while preserving security separation.
- Domain-Specific Policies: Each domain can have its own set of Group Policies, OU structures, and administrative boundaries.
- Separate FSMO Roles per Domain: Each domain has its own domain FSMO roles (RID, PDC Emulator, Infrastructure Master), in addition to shared forest FSMOs.



When planning for a multi-domain forest recovery, additional complexity must be considered beyond physical topology and speed of recovery. Key planning elements include the logical domain hierarchy, inter-domain dependencies, and the correct order of domain recovery—especially where parent-child relationships exist. Using Commvault Cloud Backup & Recovery for Active Directory Enterprise, recovery scenarios for multi-domain forests include:

Recovering the Forest Root Domain First: Recovery must begin with the first domain controller in the forest root domain. This DC is critical for re-establishing forest-wide services, including the schema and configuration partitions, and must be fully stabilized before recovering any child domains.

Sequential Child Domain Recovery: Once the root domain is recovered and operational, first DCs in each child domain can be recovered. Each domain-level recovery involves seizing domain FSMO roles and completing SYSVOL and replication tasks similar to the root domain recovery process.

Mixed Recovery Strategy (VM Restore + DCPromo): Organizations may opt to recover one DC per domain from backup to VM, then promote additional standby domain controllers using DCPromo. This approach reduces storage and backup requirements while maintaining domain resilience.

Full DC VM Recovery for Each Domain: In scenarios requiring full fidelity restoration, all DCs in every domain can be recovered to VMs. This provides a more complete restore of the environment but requires that each DC has a valid and isolated backup and increases the overall recovery time.

Hybrid Domain Recovery Model: Commvault Backup & Recovery for Active Directory Enterprise supports combining recovery strategies across domains. For example, the forest root DC may be restored from backup, while child domains could use a mix of backup and DCPromo depending on available infrastructure and backup policies.

IN SUMMARY

Active Directory forest recovery is a complex but critical component of enterprise resiliency planning. Whether operating a simple single-domain forest or a complex multi-domain environment, organizations must account for both technical dependencies and recovery objectives. By leveraging Commvault Cloud Backup & Recovery for Active Directory Enterprise, IT teams can streamline and automate many of the intricate steps required for forest restoration, enabling faster, secure, and more predictable recoveries. The strategies outlined in this document provide a flexible framework to build a recovery plan tailored to your organization's structure, risk tolerance, and operational needs. Most importantly, regular testing and validation of the recovery process in an isolated environment is essential to confirm preparedness when a real-world event occurs.

ACTIVE DIRECTORY RECOVERY REFERENCES

Microsoft Forest Recovery Guide

Commvault Cloud Active Directory – Enterprise Edition

Commvault Cloud Active Directory – Solution Brief