SOP
AD Disaster Recovery & Identity Restoration

v1.0.2

Author:

Eldon Gabriel

March 17, 2026

Table of Contents

Disclaimer: This report documents my personal work completing an MCSI lab exercise focused on simulating a *bare-metal recovery (BMR)* incident by creating a backup of the *Active Directory* (AD) and restoring the domain onto a new Windows Server 2016 system in a controlled environment. It reflects my independent understanding and execution of AD backup and recovery procedures using Windows Server Backup and System State restoration techniques. No MCSI video content, lab materials, or proprietary instructions were shared or distributed. All information presented follows MCSI's disclosure and academic integrity policies.

Revision History

Version	Date	Author	Description of Changes
1.0.0	02/12/2026	Eldon G.	Initial draft.
1.0.1	03/17/2026	Eldon G,	Title update.
1.0.2	03/20/2026	Eldon G.	Expanded validation section to include industry-standard active directory (AD) diagnostic commands (`dcdiag`, `repadmin`) for production-readiness alignment.

0.0 Executive Summary

0.1 Project Overview: AD Disaster Recovery

This report explains how a full recovery of an Active Directory (AD) environment is performed. The project simulates a complete system failure and demonstrates how to restore the system on new hardware using Windows Server 2016.

The goal is to recover all system data, including user accounts and domain services, in order to maintain business operations.

Project Objective

The main goal was to test a full disaster recovery process for a Domain Controller (DC). This involved creating a backup, simulating a system failure, and restoring the system using **Directory service restore Mode (DSRM)**.

The focus was on ensuring that the SYSVOL folder and Active Directory data were restored correctly and were ready for use.

Technical Specifications

The recovery process uses the following key components:

Recovery Method: A **Bare Metal Recovery (BMR)** was used to restore the full system, including the operating system, important data, and Active Directory.

Service Authentication: The DSRM was used to safely restore the system without causing conflicts with other domain controllers.

Data Integrity: The System State was restored to recover important system data, such as the registry, system files, and boot settings.

Infrastructure Hardening: Security improvements were planned, such as using offline backups and protected storage to reduce the risk of ransomware attacks.

Validation & Quality Assurance

To confirm that the system functioned correctly after recovery, the following checks were performed.

Service Verification: Verified that key services, such as Domain Name Server (DNS), Netlogon, and Active Directory Domain Services (AD DS), were running.

Database Integrity: Verified that the Active Directory database (`ntds.dit`) was restored correctly and was not corrupted.

Replication Health: Used tools such as `repadmin /replsummary` and `dcdiag /v` to confirm that the system was healthy and working with other domain controllers.

1.0 AD Disaster Recovery & Identity Restoration

1.1 Project Description

This project simulated a BMR disaster recovery event in a Windows Server 2016 AD environment. The goal was to create a backup of the AD and confirm that it could be successfully restored after system failure.

This exercise focused on restoring the AD to a new server and confirming that all **user accounts** and **security groups** were recovered and functioning correctly.

1.2 Technical Environment

The laboratory environment was set up as follows:

- **Operating System:** Windows Server 2016
- **Service Installed:** AD DS
- **Users Created: 100** user accounts
- **Groups Created: 50** security groups
- **Backup Tool Used:** Windows Server Backup
- **Recovery Method:** System State Restore using DSRM
- **Restore Type:** Non-authoritative restore (single domain controller environment)

1.3 Backup and Restore Procedure

The recovery process followed a clear set of steps to ensure that the AD database was correctly backed up and restored.

Stage 1: AD Setup

- Installed and configured *AD DS* on the first Windows Server
- Created **100** user accounts
- Created **50** security groups
- Confirmed the domain was working before the backup

Stage 2: Backup Creation

- Installed Windows Server Backup
- Performed a System State backup to capture AD components, including the following:
    - **New Technology Directory Services (NTDS) database** (`ntds.dit`)
    - SYSVOL folder
    - Registry and system boot files needed for recovery

Note: *Note: We verified the backup recency against the Tombstone Lifetime (TSL) to prevent the introduction of lingering objects and ensure successful replication post-recovery.*

Stage 3: New Server Deployment

- Set up a second Windows Server as a clean system
- Prepared the server for the restore process

Stage 4: AD Restoration

- Booted the server into DSRM
- Restored the System State backup from the backup media
- Recovered the AD onto the new server

Note: *A Non-Authoritative restore was performed to allow the recovered DC to receive inbound replication from healthy peers, ensuring identity consistency across the forest.*

Stage 5: Post-Restore Validation

- Confirmed user accounts and groups were restored
- Verified the domain services were working after recovery

1.4 Troubleshooting and Root Cause Analysis (RCA)

After the restoration was completed, network and service issues occurred. Troubleshooting steps were used to identify the causes and apply fixes.

Issue 1: Console Connection Failure

- **Observation:** Management consoles cannot connect to the domain correctly.
- **Cause:** The server's Internet Protocol(IP) address and DNS settings do not match the restored domain environment.
- **Fix Applied:** IPv4 settings and DNS loopback settings were corrected to match the restored DNS records.

Issue 2: Service Synchronization Hang (Netlogon/SYSVOL Issues)

- **Observation:** `Netlogon` did not start fully, and the server did not advertise as a domain controller.
- **Cause:** SYSVOL was not marked as ready, which prevented AD services from completing the startup.
- **Fix Applied:** A registry change was applied to set the `SysvolReady` flag so that services could complete initialization.

1.5 Post-Recovery Security Hardening

After AD was restored, basic security controls were applied to improve the domain protection.

- **Account Lockout Policy:** Group Policy settings were configured to reduce brute-force login attempts.
- **User and Group Review:** Verified user accounts and group memberships were correct after the recovery process.
- **Verify Restoration:** Confirmed that the restored objects matched the expected AD environment.

2.0 Conclusion

2.1 Key Takeaways

- System State backups are required to recover AD after a failure.
- DSRM is required to safely restore AD.
- The DNS and IP settings must be correct for AD to work after restoration.
- SYSVOL and `Netlogon` issues are common after a restore and must be checked before the system is put back into use.

2.2 Security Implications and Recommendations

An AD controls the authentication and access inside an organization. If it becomes corrupt or unavailable, users may not be able to log in, security policies may stop working, and systems may become more difficult to manage. If recovery is performed incorrectly, it can also create security risks, such as incorrect permissions or unauthorized access.

Risks Identified

- Loss of user login access and authentication
- Group Policy may stop working
- User accounts or groups may restore incorrectly if recovery is incomplete
- Privileged accounts may become a security risk if permissions are not reviewed

Recommendations

- Regularly back up the System State for all domain controllers.
- Store backups offline or in immutable storage to reduce ransomware risk.
- Encrypt backup storage and restrict access to authorized administrators.
- Regularly test disaster recovery procedures to confirm that backups are working.
- After restoration, verify the DNS, SYSVOL, and domain services before returning to production.

- Review **Domain Admin** and privileged group memberships after recovery.

This exercise supports real-world backup and recovery practices and aligns with disaster recovery expectations in enterprise environments.

2.3 Post-Recovery Validation Protocol

To ensure the long-term health of the restored Active Directory database and forest replication, the following industry-standard diagnostics **should be executed** as part of the final validation phase:"

- `dcdiag /v`: To perform a verbose test of all Domain Controller roles and DNS health.
- `repadmin /replsummary`: To verify that the restored DC is successfully replicating with all peers without latency or errors.