REPORT
Active Directory Bare Metal Recovery (BMR) Backup and Restore

v1.0.0

Author:

Eldon Gabriel

February 12, 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 *Active Directory* and restoring the domain onto a new Windows Server 2016 system in a controlled environment. It reflects my independent understanding and execution of Active Directory backup and recovery procedures using Windows Server Backup and System State restoration techniques. No MCSI video content, lab materials, or proprietary instructions have been shared or distributed. All information presented follows MCSI's disclosure and academic integrity policies.

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/12/2026	Eldon G.	Initial draft.

1.0 ACTIVE DIRECTORY DISASTER RECOVERY AND IDENTITY RESTORATION

1.1 Project Description

This project simulated a **Bare Metal Recovery (BMR)** disaster recovery event in a Windows Server 2016 Active Directory environment. The goal was to create a backup of the **Active Directory** and confirm that it could be restored successfully after a system failure.

This exercise focused on restoring **Active Directory** onto a new server and confirming that all **user accounts** and **security groups** were recovered and working correctly.

1.2 Technical Environment

The lab environment used the following setup:

- **Operating System:** Windows Server 2016
- **Service Installed:** *Active Directory Domain Services (AD DS)*
- **Users Created: 100** user accounts
- **Groups Created: 50** security groups
- **Backup Tool Used:** *Windows Server Backup*
- **Recovery Method:** *System State Restore* using *Directory Services Restore Mode (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 make sure the Active Directory database could be backed up and restored correctly.

Stage 1: Active Directory 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 Active Directory components, including:
  - **NTDS database** (`ntds.dit`)
  - **SYSVOL** folder
  - Registry and system boot files needed for 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: Active Directory Restoration

- Booted the server into *Directory Services Restore Mode (DSRM)*
- Restored the *System State* backup from the backup media
- Recovered the Active Directory onto the new server

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 restore 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 could not connect to the domain correctly.
- **Cause:** The server IP address and DNS settings did 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 fully start, and the server did not advertise as a domain controller.
- **Cause:** *SYSVOL* was not marked as ready, which prevented Active Directory services from finishing startup.
- **Fix Applied:** A registry change was applied to set the `SysvolReady` flag so services could complete initialization.

1.5 Post-Recovery Security Hardening

After the Active Directory was restored, basic security controls were applied to improve the protection of the domain.

- **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 still correct after the recovery process.
- **Restore Validation:** Confirmed that the restored objects matched the expected Active Directory environment.

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

- *System State* backups are required to recover Active Directory after a failure.
- *Directory Services Restore Mode (DSRM)* is needed to restore Active Directory safely.
- DNS and IP settings must be correct for Active Directory to work after restoration.
- SYSVOL and Netlogon issues are common after a restore and must be checked before putting the system back into use.

2.2 Security Implications and Recommendations

Active Directory controls authentication and access inside an organization. If it becomes corrupted or unavailable, users may not be able to log in, security policies may stop working, and systems may become harder to manage. If recovery is done 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:

- Perform *System State* backups regularly for all domain controllers.
- Store backups offline or in immutable storage to reduce ransomware risk.
- Encrypt backup storage and restrict access to authorized administrators.
- Test disaster recovery procedures regularly to confirm backups work.

- After restoration, verify 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 matches disaster recovery expectations used in enterprise environments.