Report: Backup & Recovery

1. Introduction

In modern enterprise IT environments, Active Directory Domain Services (AD DS) serves as the backbone for identity, authentication, and authorization across the network. Given its critical role, even minor disruptions or data loss can lead to significant operational downtime, security risks, or data integrity issues. As a result, a robust backup and recovery strategy for AD is essential.

This set of tasks focuses on simulating real-world disaster recovery scenarios by leveraging built-in tools such as wbadmin, ntdsutil, and the AD Recycle Bin. These tools enable administrators to perform full system state backups, restore accidentally deleted objects like Organizational Units (OUs), and conduct authoritative restores to override incorrect replication data across multiple domain controllers.

By mastering these recovery techniques, administrators are better prepared to mitigate threats from accidental deletions, insider threats, ransomware, or software failures, ensuring the availability, integrity, and recoverability of critical domain data. The practical exercises also demonstrate how organizations can meet compliance requirements, such as those outlined in ISO 27001, NIST, or GDPR, by ensuring directory data is regularly backed up and easily restorable.

Ultimately, this module aims to build confidence and readiness for handling AD-related incidents, making recovery a routine operation instead of a crisis response.

2. Objective

The primary objective of this module is to develop practical proficiency in safeguarding Active Directory through effective backup and recovery mechanisms. This includes learning how to perform a **System State backup** of a Domain Controller using wbadmin, which captures critical components such as the AD database, SYSVOL, boot files, and registry. Furthermore, the objective is to simulate real-world scenarios by intentionally deleting Active Directory objects like Organizational Units (OUs) and groups, and then performing both **non-authoritative and**

authoritative restores to recover them. These tasks aim to ensure that administrators can confidently respond to accidental deletions or corruption events and understand the steps necessary to restore AD to a consistent and functional state. Mastery of these techniques is crucial for maintaining business continuity, minimizing downtime, and adhering to best practices for disaster recovery and compliance.

Key goals include:

- **Perform System State Backups**
  Gain hands-on experience using wbadmin to back up critical components of a Domain Controller, including the Active Directory database, registry, boot files, and SYSVOL.

- **Understand AD Object Recovery**
  Learn how to recover accidentally deleted Active Directory objects such as OUs using the AD Recycle Bin and verify restoration without disrupting domain functionality.

- **Execute Authoritative Restores**
  Practice using ntdsutil to perform authoritative restores of specific AD objects, ensuring the restored version replicates across other domain controllers in the forest.

- **Simulate Realistic Disaster Scenarios**
  Build readiness by simulating AD corruption or object loss scenarios and performing complete recovery steps that mimic real-world incidents.

- **Strengthen AD Recovery Readiness**
  Establish a repeatable recovery process to improve resilience, reduce potential downtime, and support organizational compliance with IT governance and security standards.

3. Methodology

This methodology explains the structured process of securing Active Directory infrastructure through reliable backup and restoration practices. It includes creating a System State Backup,

simulating the accidental deletion of directory objects (OU), and validating recovery using both non-authoritative and authoritative methods. These steps are fundamental to disaster recovery, AD availability, and enterprise continuity planning.

3.1 Perform a System State Backup of Domain Controller

A System State Backup is crucial for safeguarding all essential components of a Domain Controller, such as Active Directory, SYSVOL, Registry, and COM+ database. This phase ensures a restorable snapshot of the AD is available for disaster recovery.

(Installed the Windows Server Backup.)

Navigation Path:

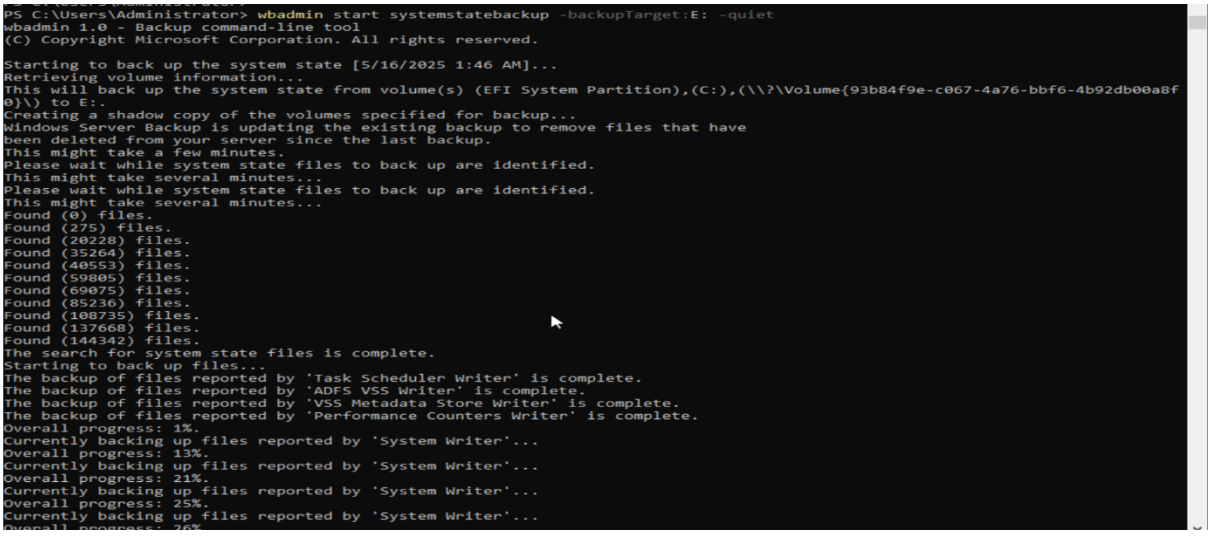
Open Command Prompt as Administrator:

Start Menu → Type cmd → Right-click Command Prompt → Click Run as administrator

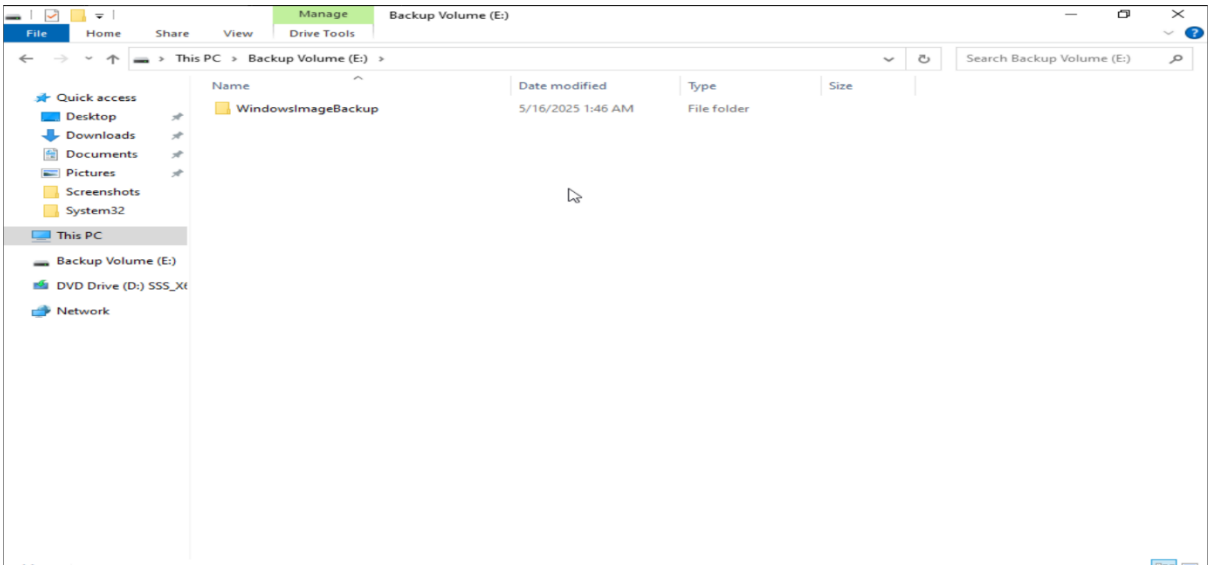
Run wbadmin to initiate backup:

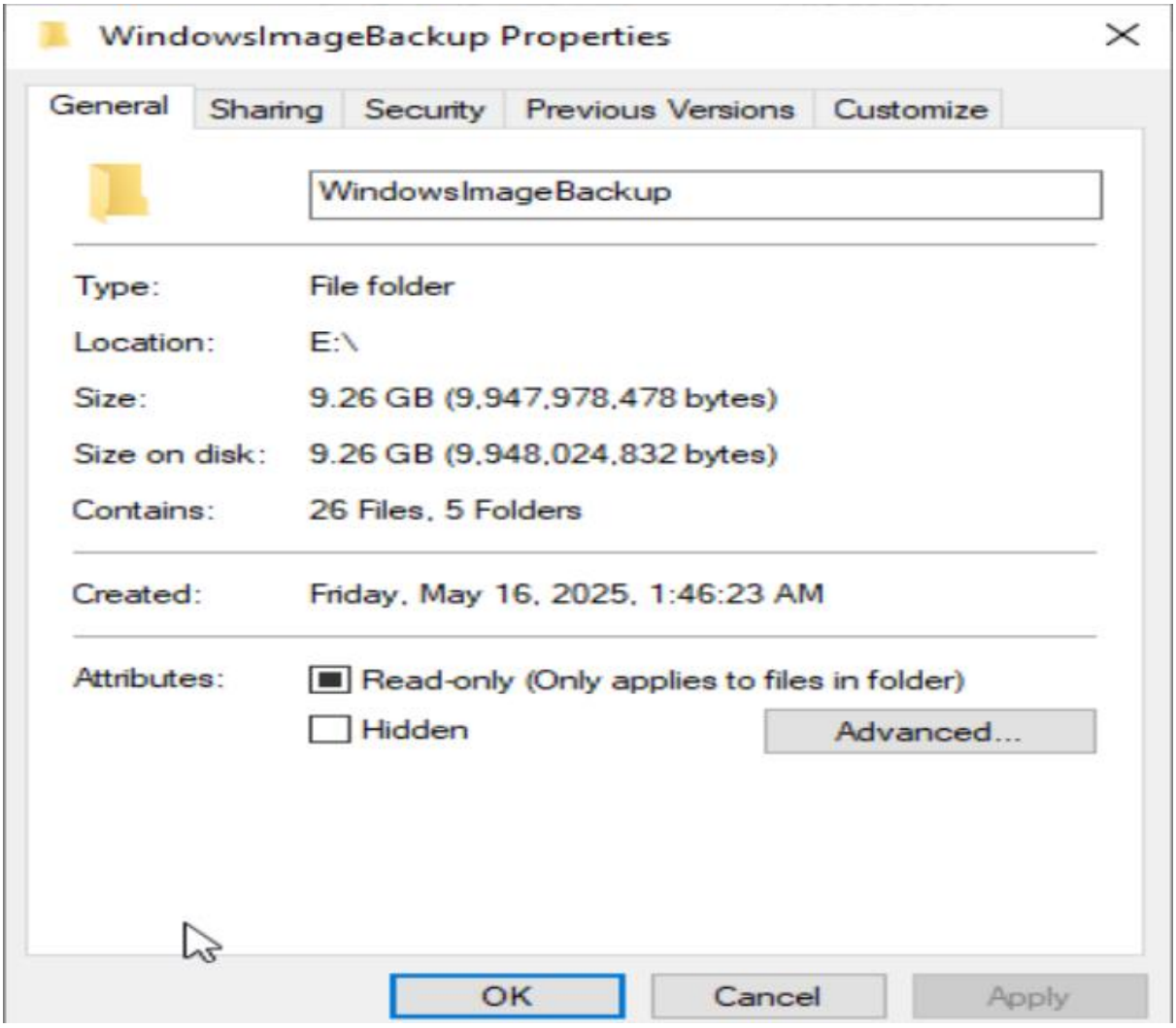
Use the wbadmin start systemstatebackup command in the elevated CMD.

(Backup Started.)



(Backup took place in disk E.)

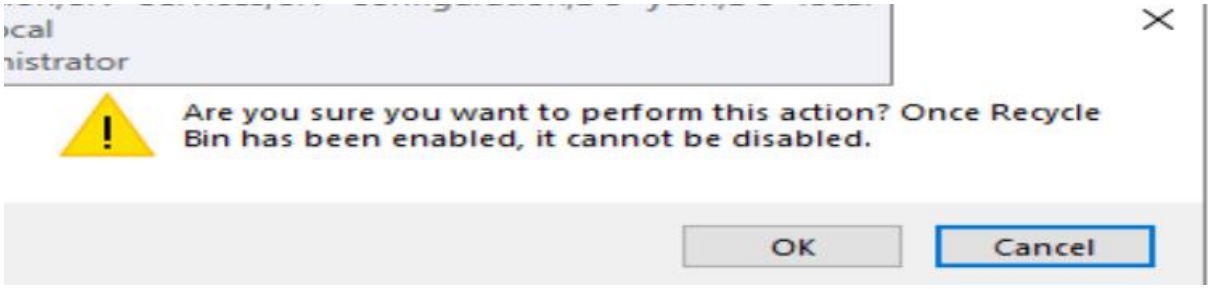




3.2 Simulate Accidental Deletion of an OU

To assess recovery capabilities, this phase simulates a real-world situation where an Organizational Unit (OU) is mistakenly deleted. Such an incident can occur due to human error, scripts gone wrong, or malicious actions. Simulating the deletion provides a safe lab environment to test the backup and recovery process effectiveness and build administrator readiness for real incidents.

Enable Recycle Bin:



Navigation Path:

Open ADUC:

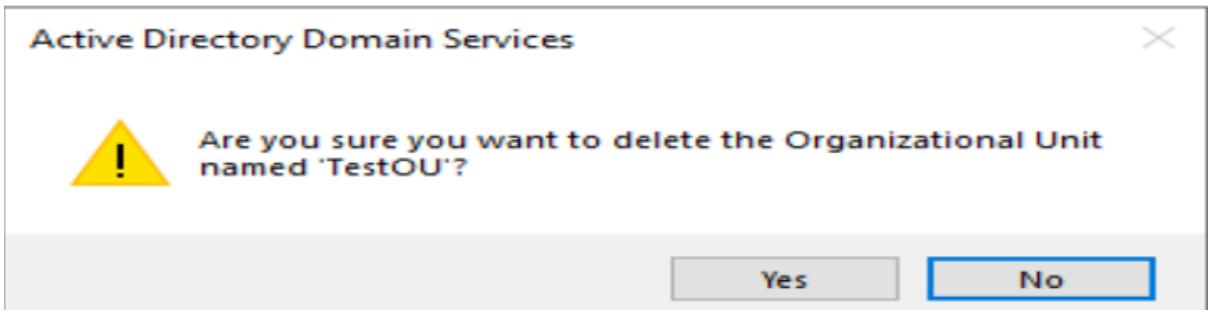
Start Menu → Run (Win + R) → Type dsa.msc → Press Enter

Locate and delete the target OU:

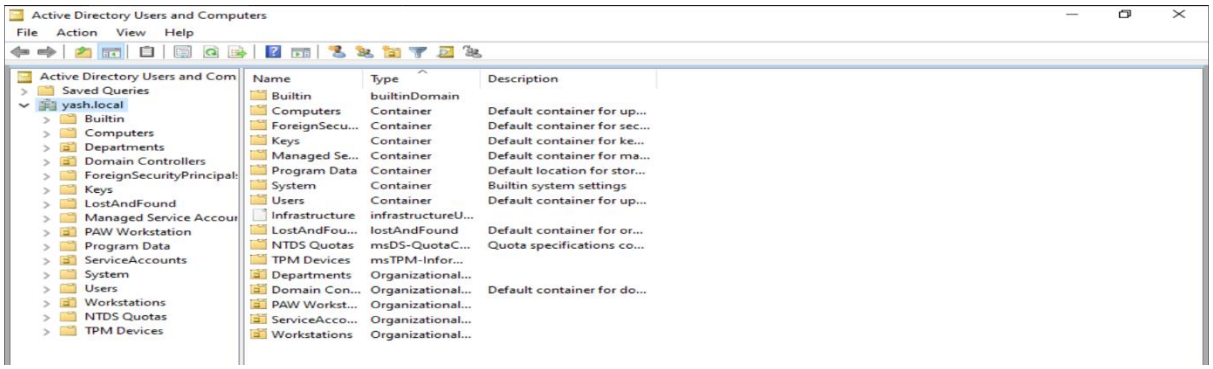
In the left pane, navigate to:

yash.local → Expand → Select OU to delete → Right-click → Click Delete

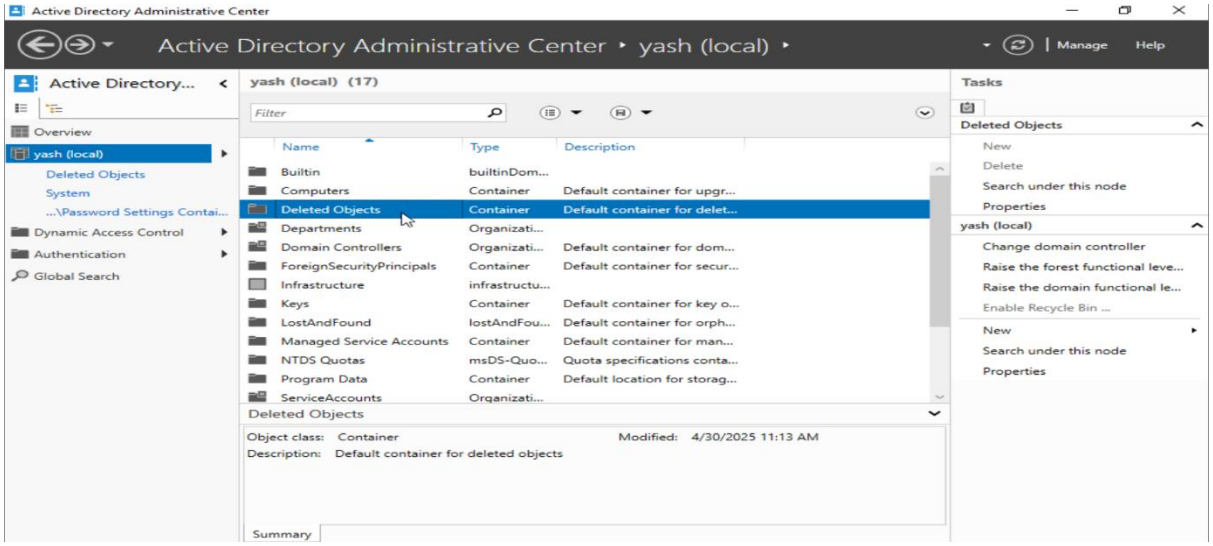
(Deleted the OU.)



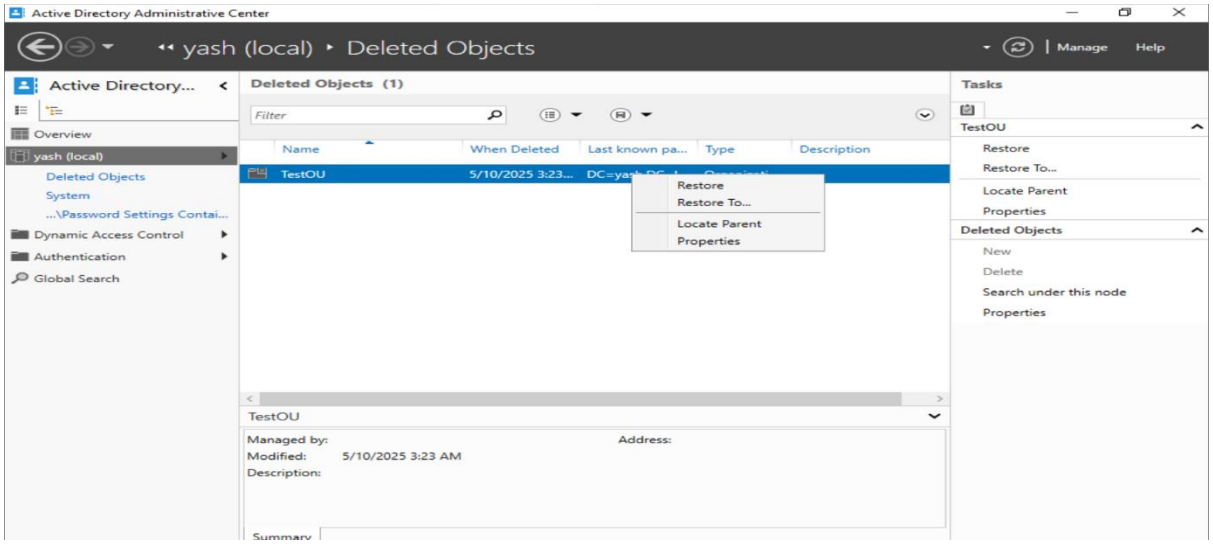
(Confirm the deletion of OU.)



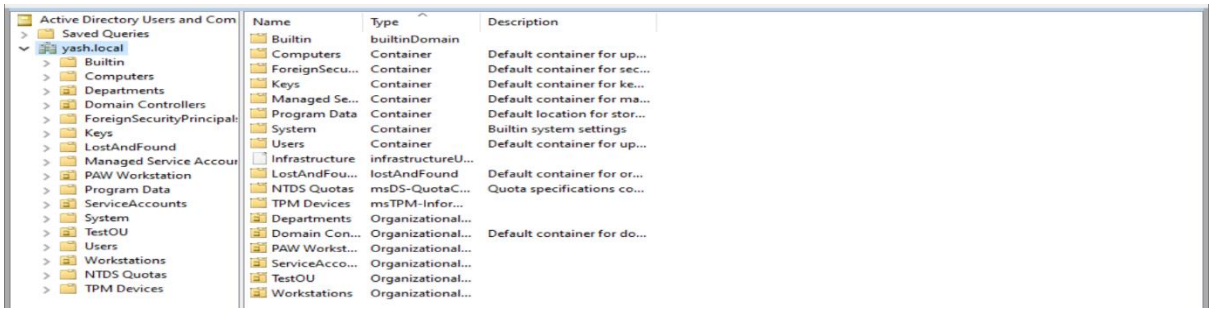
(Navigate to the deleted objects.)



(Restore the deleted OU)



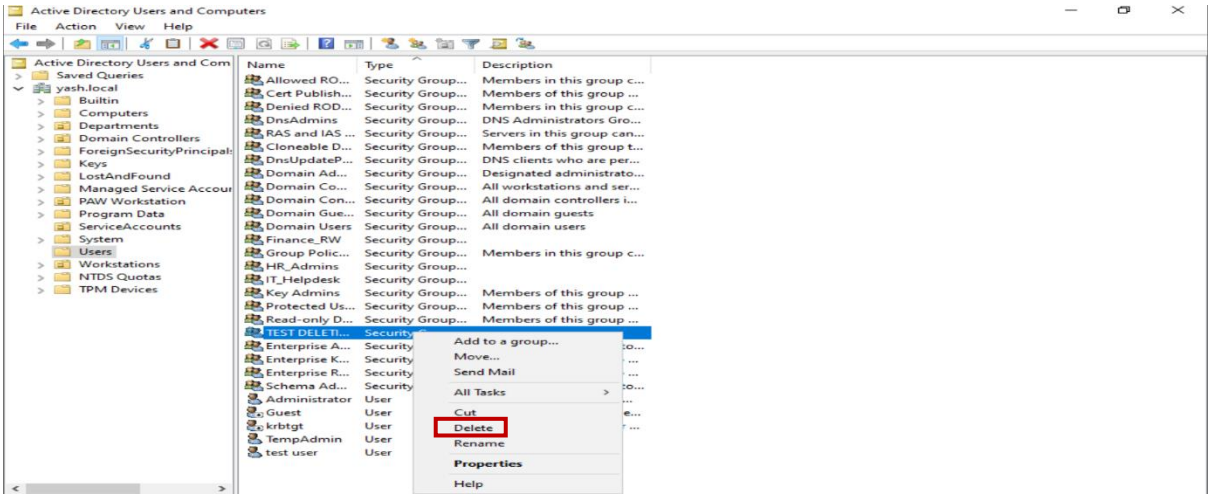
(Verify Restored OU.)



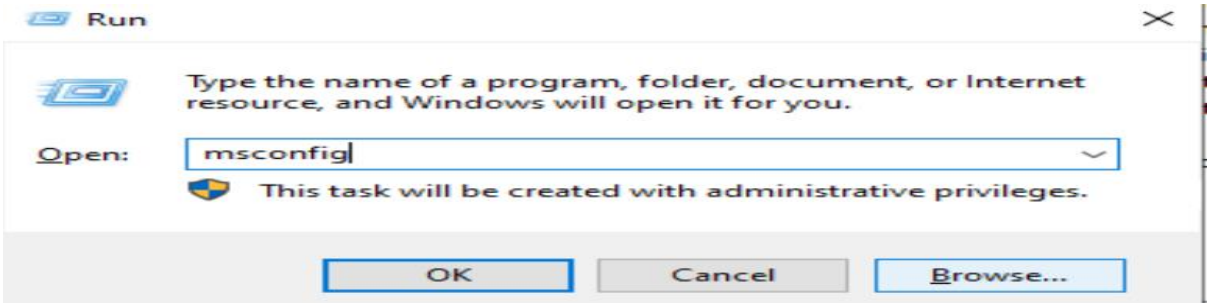
3.3 Perform Authoritative Restore of Deleted Group

This phase covers the **Authoritative Restore** process using ntdsutil, designed to recover a specific AD object (like a security group) and mark it as authoritative, forcing it to replicate across all domain controllers. This is critical when certain objects are deleted and must override newer changes or absence in the AD replication topology.

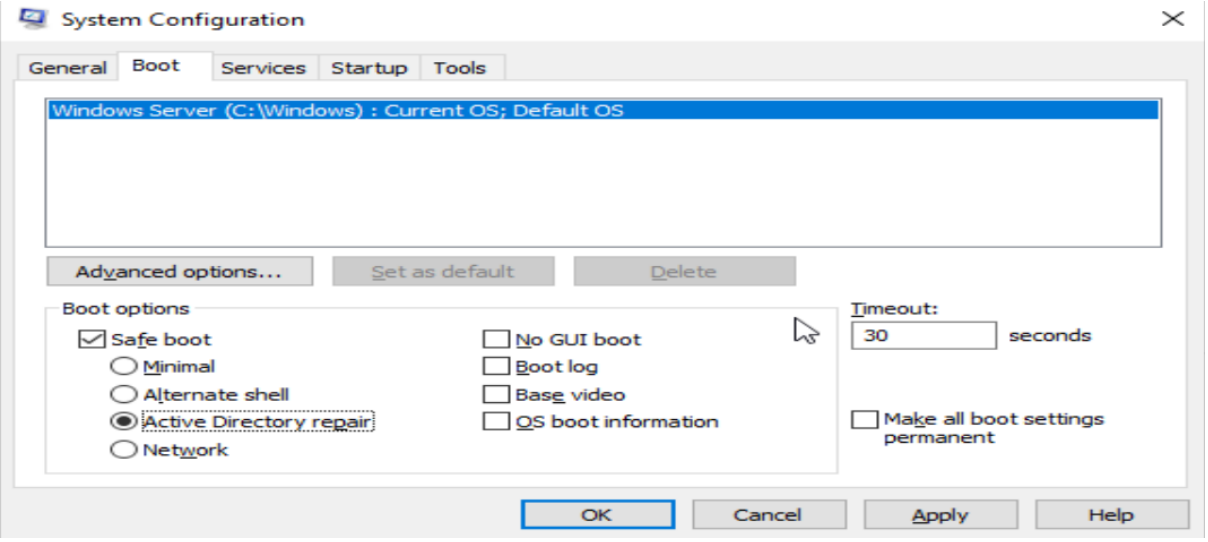
(Deleted a group Name: TEST DELETION.)



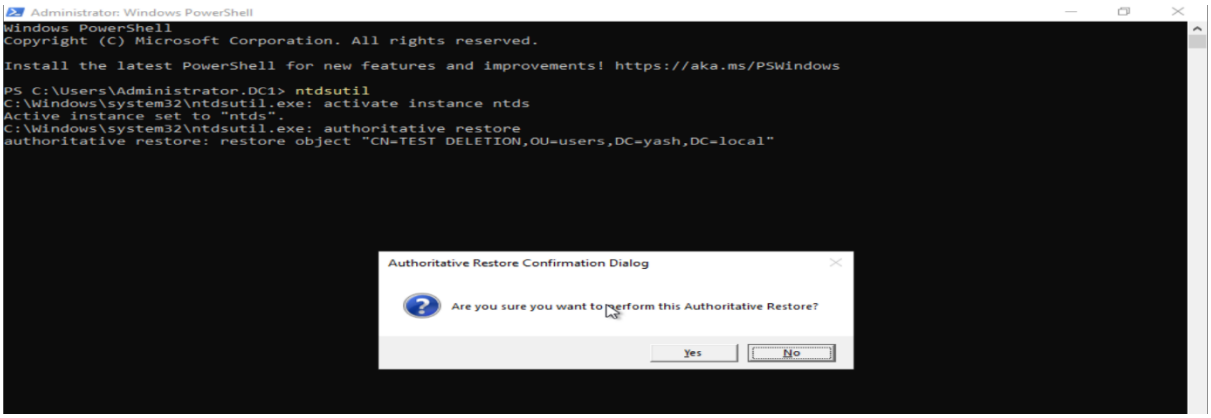
(Run this to open boot menu.)



(Check safe boot.)

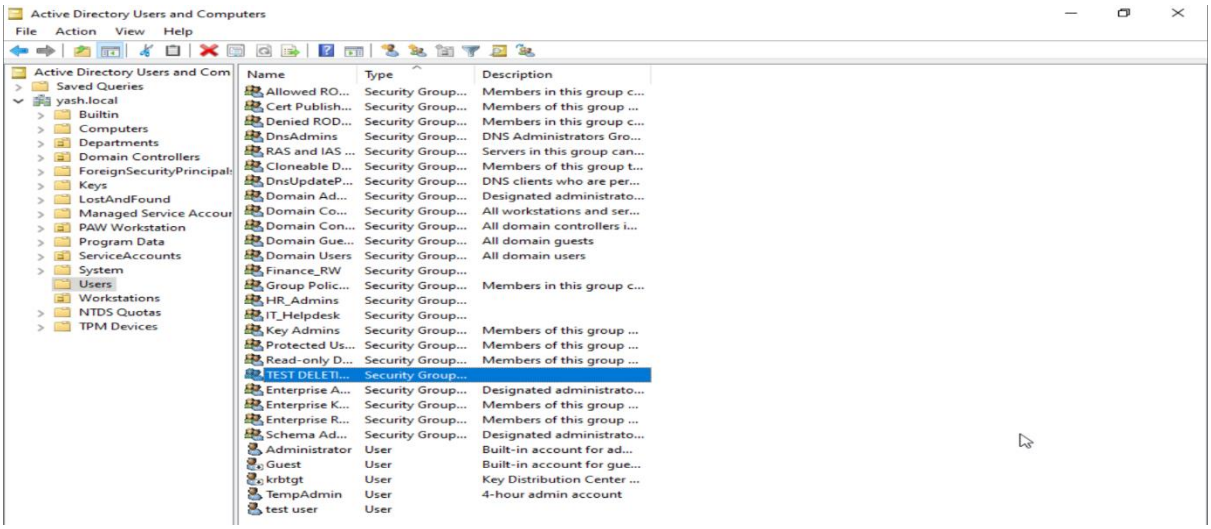


(Restoring the file.)



(Successfully Restored.)

(Verify it after disable safe mode.)



4. Results And Findings

This section presents the observed outcomes from the backup and recovery tasks performed on the Domain Controller. It highlights the effectiveness of system state backup, the success of recovery operations, and confirms the accuracy and consistency of restored directory objects.

4.1 System State Backup Completed Successfully

The system state backup of the Domain Controller was executed using wbadmin, and a valid backup version was confirmed. This ensured that Active Directory and other critical system components were properly captured for restoration.

4.2 OU Deletion Simulated and Confirmed

An Organizational Unit (OU) was deleted from ADUC to simulate an accidental deletion. The object was moved to the deleted state (tombstone), which was validated using PowerShell queries, confirming the simulation was accurate.

4.3 Recycle Bin Recovery Worked (If Enabled)

If the Active Directory Recycle Bin was enabled, the deleted OU was restored using PowerShell, and its attributes, memberships, and permissions were fully retained. This demonstrated the Recycle Bin’s value in efficient recovery.

4.4 System State Recovery Validated

Using Directory Services Restore Mode (DSRM), the previously taken backup was restored with wbadmin. The system rebooted normally and restored the domain to its earlier state, proving that the system state backup was usable.

4.5 Authoritative Restore Replicated Across DCs

A group object was restored authoritatively using ntdsutil. After rebooting the DC, replication logs confirmed that the restored object successfully propagated to other DCs, validating the effectiveness of authoritative restore.

5. Recommendations

Based on the tasks performed, this section outlines best practices to enhance Active Directory backup and recovery strategies. These recommendations aim to improve resilience, automate critical tasks, and ensure recovery readiness in enterprise environments.

5.1 Schedule Regular System State Backups

System state backups should be scheduled routinely using automation tools. Keeping backups on separate, secured storage helps ensure recoverability during incidents like corruption, hardware failure, or ransomware attacks.

5.2 Enable AD Recycle Bin in All Environments

Enabling the Active Directory Recycle Bin simplifies object recovery without needing DSRM. It retains complete object metadata and structure, making it a recommended first-layer recovery feature for modern AD deployments.

5.3 Perform Regular DR Drills

Disaster recovery drills involving object deletion and restoration should be conducted periodically. These drills test administrative preparedness and help identify weaknesses in current backup or restore processes.

5.4 Maintain Documentation for DSRM Credentials

The DSRM account is critical for low-level recovery. Its credentials should be securely stored and periodically tested, ensuring availability and usability when access to AD in normal mode is not possible.

5.5 Monitor Backup Health and AD Replication

Backup operations and AD replication should be actively monitored using tools like Event Viewer, repadmin, and backup logs. This proactive approach ensures that any failures or inconsistencies are detected and resolved early.

6. Conclusion

The comprehensive evaluation and execution of Active Directory backup and recovery operations reaffirm the foundational role these processes play in maintaining the integrity, availability, and resilience of enterprise IT infrastructures. Through the use of wbadmin, a reliable System State Backup was created, capturing critical AD components such as the NTDS database, SYSVOL, and registry settings. The controlled simulation of an accidental OU deletion tested the recovery preparedness of the domain environment and emphasized the real-world risks posed by administrative errors or malicious actions. The subsequent restoration process — including recovery via the Active Directory Recycle Bin and authoritative restore using ntdsutil — proved effective in recovering directory objects with full metadata and ensuring consistent replication across all domain controllers. These operations validated not only the technical feasibility but also the operational readiness for responding to directory-related incidents. Furthermore, this exercise highlights the need for regular disaster recovery drills, comprehensive documentation, and proactive monitoring to ensure that backup mechanisms are not only implemented but also functional and aligned with recovery time objectives (RTOs) and recovery point objectives (RPOs). By institutionalizing these practices, organizations can enhance their Active Directory resilience posture, reduce service downtime, and maintain continuous access to authentication and directory services — all of which are essential for modern enterprise operations and compliance mandates.