Report: Disaster Recovery & High Availability

1. Introduction

Active Directory (AD) serves as the backbone of identity and access management in enterprise environments. Its continuous availability and integrity are crucial to ensure uninterrupted access to resources and services. However, AD environments are vulnerable to various risks, including hardware failures, accidental deletions, corruption, ransomware attacks, and site-wide disasters like power outages or natural calamities.

To mitigate these risks, organizations implement Disaster Recovery (DR) and High Availability (HA) strategies tailored to their infrastructure. A **site-aware AD backup strategy** is essential in multi-site deployments where each site may have different operational needs, network conditions, and maintenance windows. Customizing backup schedules and retention policies per site helps optimize resource usage and ensures timely recovery options without overloading network bandwidth or storage.

Furthermore, simply backing up AD data is insufficient unless the backups can be successfully restored when needed. Conducting a **full AD forest recovery test in an isolated lab** environment simulates a real disaster scenario without impacting production systems. This practice verifies that the backup data is intact, the recovery procedures are sound, and the IT team is prepared to perform an effective recovery when disaster strikes. It also helps identify gaps or issues in the recovery plan, such as missing system state backups or misconfigured domain controllers.

Together, these activities form a critical part of an organization's business continuity plan, aiming to minimize downtime and data loss while maintaining trust in the AD infrastructure.

2. Objectives

The primary objective of this task is to develop a robust, site-aware Active Directory backup strategy that accommodates the unique needs and schedules of different physical sites within an organization. This ensures that backups are performed efficiently, minimizing disruption while maximizing data protection tailored to each site’s operational context. Additionally, the task aims to validate the effectiveness of disaster recovery procedures by performing a full Active Directory forest recovery in an isolated lab environment. This recovery test will confirm that backups are reliable and that the AD environment can be restored completely and accurately in the event of a real disaster, thereby ensuring business continuity and minimizing downtime.

Key goals Include:

- **Develop Site-Specific Backup Schedules**
  Create tailored backup plans that reflect the operational requirements and constraints of each AD site, optimizing backup timing and frequency.

- **Ensure Backup Integrity and Completeness**
  Implement reliable backup processes that capture all critical AD components, including domain controllers, FSMO roles, and global catalog servers.

- **Minimize Disruption During Backups**
  Schedule backups to reduce network load and avoid interference with normal business activities, especially in sites with limited bandwidth or different time zones.

- **Validate Full Forest Recovery Procedures**
  Conduct comprehensive recovery tests in an isolated lab to confirm that the AD forest can be restored fully and functionally from backups.

- **Enhance Disaster Preparednes**
  Document recovery processes and train IT staff to efficiently execute AD recovery, ensuring rapid response and minimal downtime in real disaster scenarios.

3. Methodology

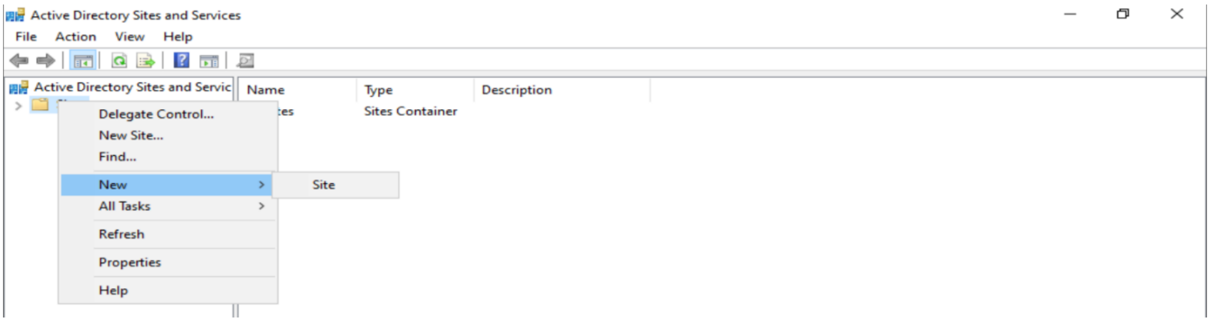
The methodology for establishing a robust disaster recovery and high availability framework for Active Directory involves a phased approach. Each phase addresses critical components—starting from understanding the environment, designing and implementing backup strategies, to validating recovery procedures. This phased approach ensures a systematic and thorough execution, minimizing risks and maximizing the likelihood of successful disaster recovery. Breaking down the task into phases also facilitates better planning, monitoring, and documentation, which are essential for continuous improvement and compliance.

3.1 Design and Implementation of Site-Aware AD Backup Strategy

- **Create Two AD Sites**

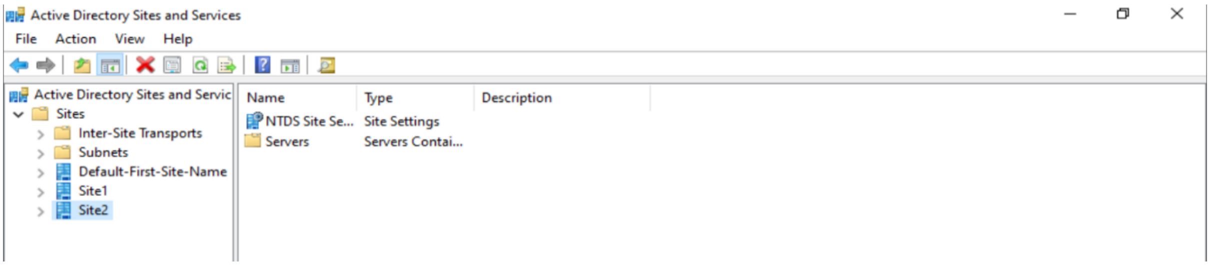
  Using Active Directory Sites and Services, two separate sites were created to simulate a multi-site AD environment. Each site was assigned its own subnet to reflect real-world network segmentation.

  Navigate to Active Directory Sites and Services



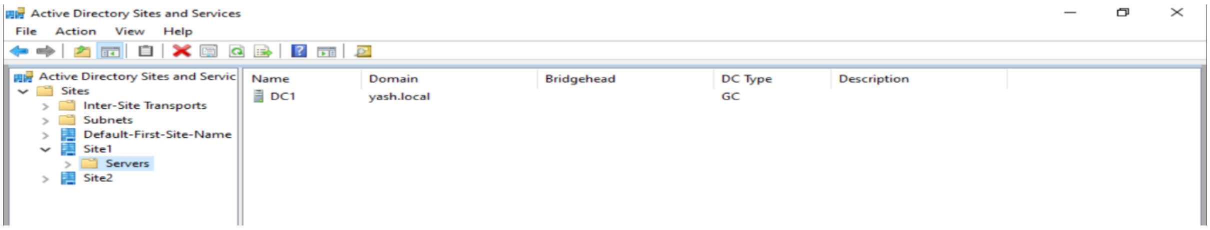
Name	Type	Description
...tes	Sites Container	

  (Created to sites.)



Name	Type	Description
NTDS Site Se...	Site Settings	
Servers	Servers Contai...	

  (Add server to the Site1.)

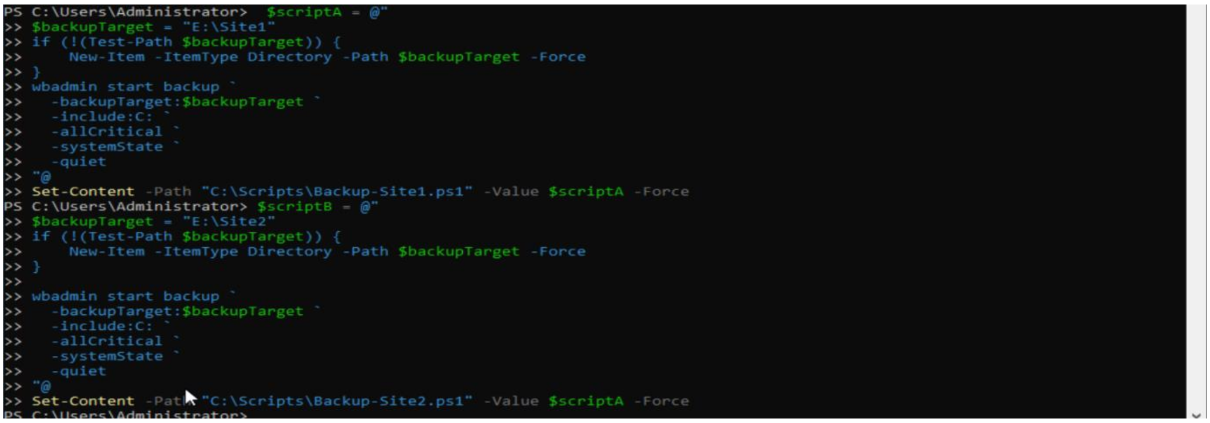


Name	Domain	Bridgehead	DC Type	Description
DC1	yash.local		GC	

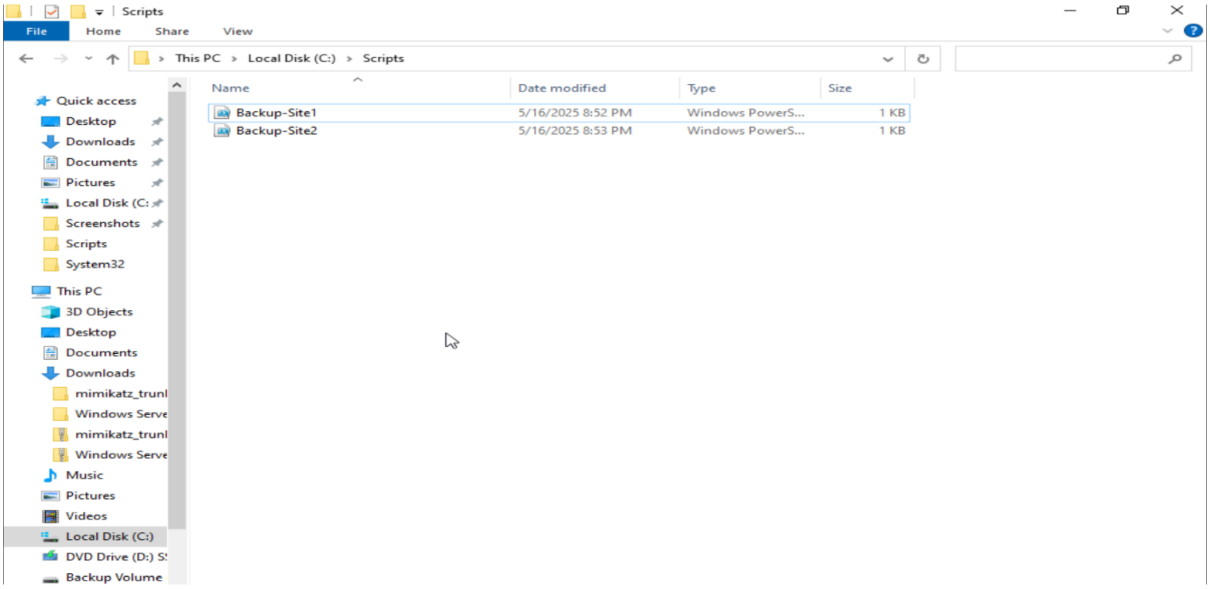
- **Backup Script Development**

  Custom PowerShell scripts were written to perform system state backups of domain controllers at each site. These scripts leveraged Windows native backup utilities (e.g., wbadmin) to capture all critical AD components including the NTDS database, SYSVOL, and system state.

  (Made a script which runs the backup command in powershell.)



```
PS C:\Users\Administrator>  $scriptA = @"
>> $backupTarget = "E:\Site1"
>> if (!(Test-Path $backupTarget)) {
>>     New-Item -ItemType Directory -Path $backupTarget -Force
>> }
>> wbadmin start backup `
>>   -backupTarget:$backupTarget `
>>   -include:C: `
>>   -allCritical `
>>   -systemState `
>>   -quiet
>> "@
>> Set-Content -Path "C:\Scripts\Backup-Site1.ps1" -Value $scriptA -Force
PS C:\Users\Administrator> $scriptB = @"
>> $backupTarget = "E:\Site2"
>> if (!(Test-Path $backupTarget)) {
>>     New-Item -ItemType Directory -Path $backupTarget -Force
>> }
>>
>> wbadmin start backup `
>>   -backupTarget:$backupTarget `
>>   -include:C: `
>>   -allCritical `
>>   -systemState `
>>   -quiet
>> "@
>> Set-Content -Path "C:\Scripts\Backup-Site2.ps1" -Value $scriptA -Force
PS C:\Users\Administrator>
```

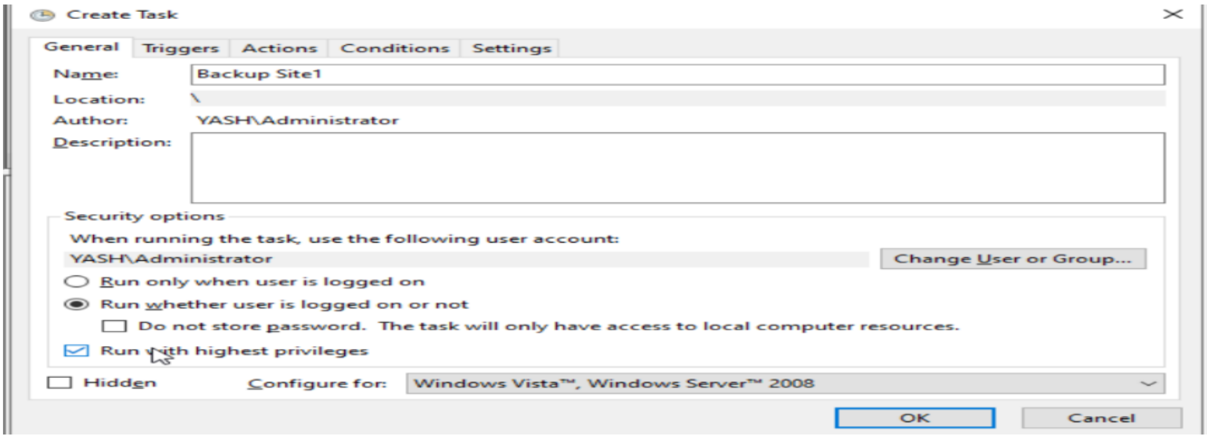


Name	Date modified	Type	Size
Backup-Site1	5/16/2025 8:52 PM	Windows PowerS...	1 KB
Backup-Site2	5/16/2025 8:53 PM	Windows PowerS...	1 KB

- **Scheduling Backups**

  Using Task Scheduler on each domain controller, the backup scripts were scheduled to run at different times for each site. This scheduling considered network load and site operational hours to minimize disruption and optimize resource utilization.

(Created a Task named-Backup Site1.)



Name: Backup Site1

Location: \

Author: YASH\Administrator

Description:

Security options

When running the task, use the following user account:

YASH\Administrator

○ Run only when user is logged on

● Run whether user is logged on or not

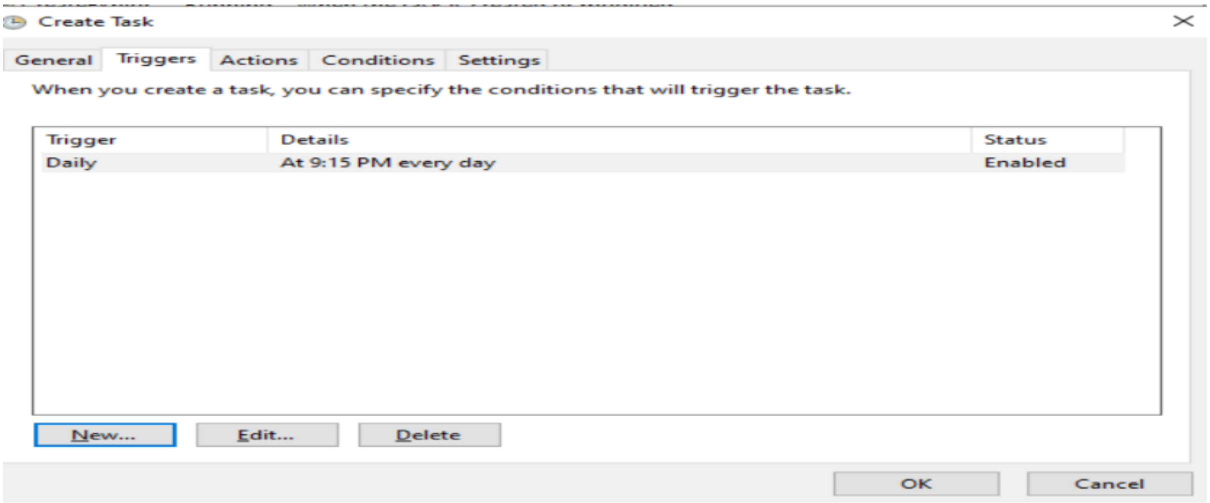
□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

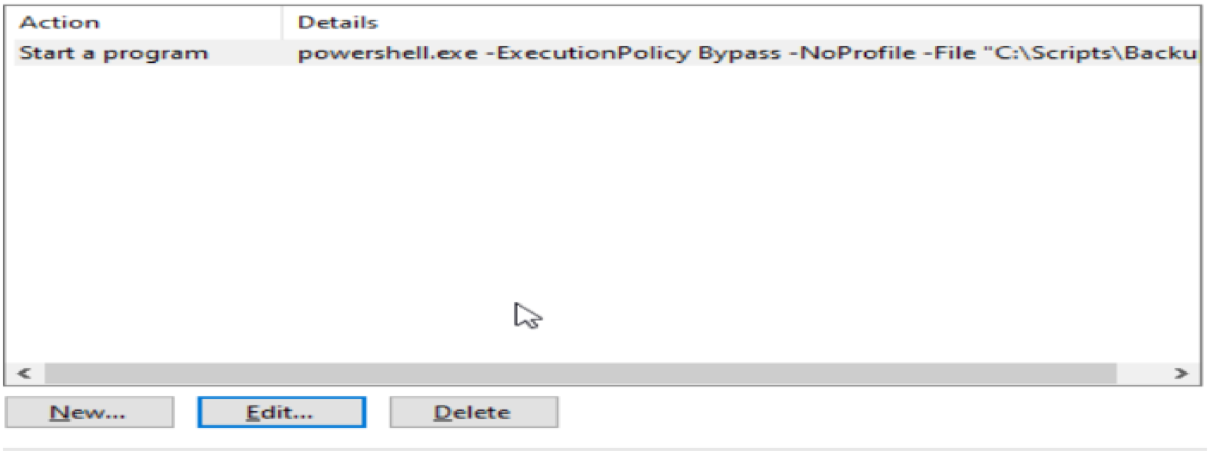
(Set it to trigger daily.)



When you create a task, you can specify the conditions that will trigger the task.

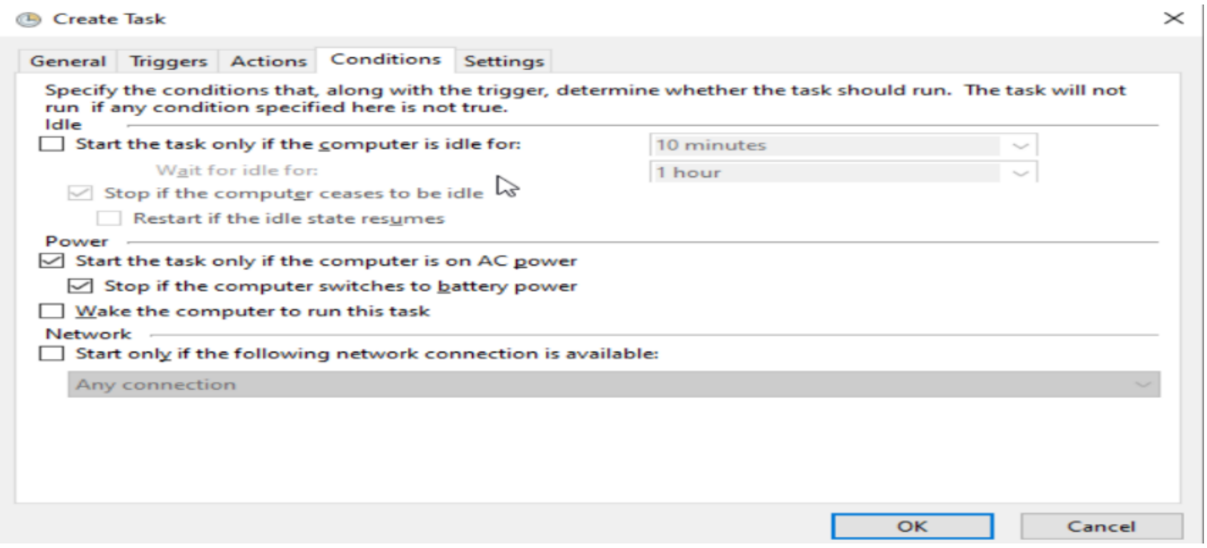
Trigger	Details	Status
Daily	At 9:15 PM every day	Enabled

(Edited Action which is going to perform during backup.)



Action	Details
Start a program	powershell.exe -ExecutionPolicy Bypass -NoProfile -File "C:\Scripts\Backu

(Conditions.)



Create Task

General | Triggers | Actions | Conditions | Settings

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

□ Start the task only if the computer is idle for: 10 minutes

Wait for idle for: 1 hour

☑ Stop if the computer ceases to be idle

□ Restart if the idle state resumes

Power

☑ Start the task only if the computer is on AC power

☑ Stop if the computer switches to battery power

□ Wake the computer to run this task

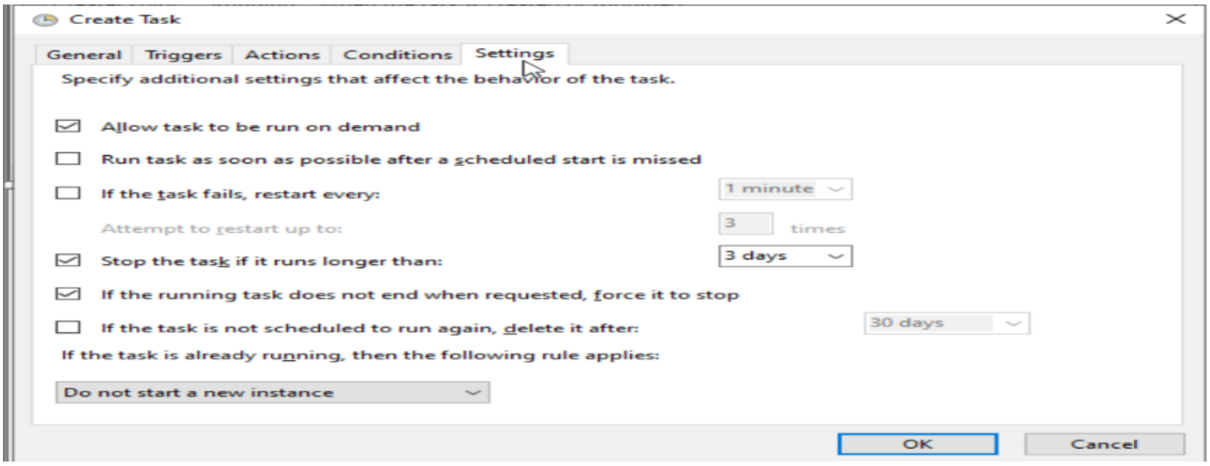
Network

□ Start only if the following network connection is available:

Any connection

OK | Cancel

(Settings)



Create Task

General | Triggers | Actions | Conditions | Settings

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

□ Run task as soon as possible after a scheduled start is missed

□ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

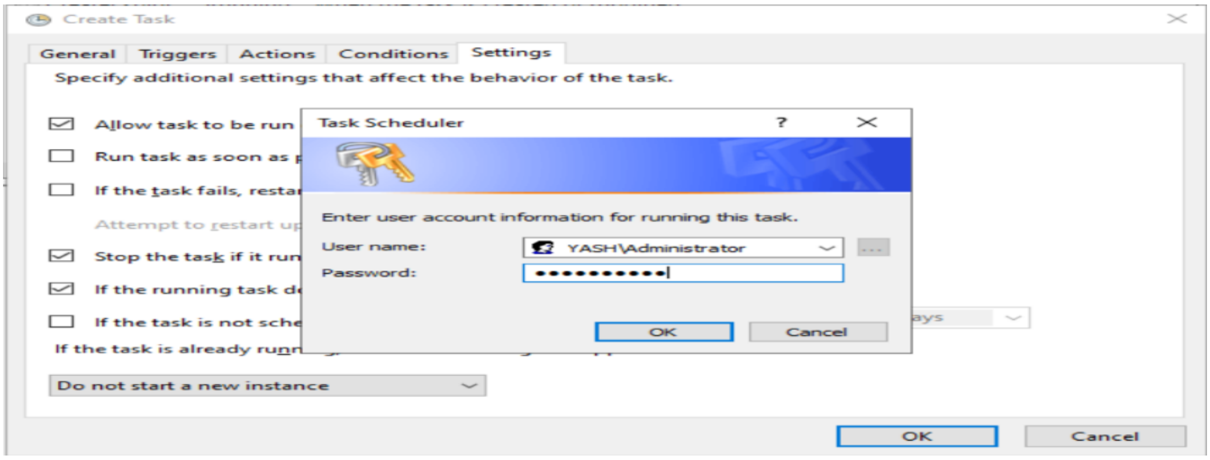
□ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

OK | Cancel

(Provided credentials to run this task as Administrator.)



Create Task

General | Triggers | Actions | Conditions | Settings

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run

□ Run task as soon as p

□ If the task fails, resta

Attempt to restart up

☑ Stop the task if it run

☑ If the running task d

□ If the task is not sche

If the task is already runn

Do not start a new instance

Task Scheduler

Enter user account information for running this task.

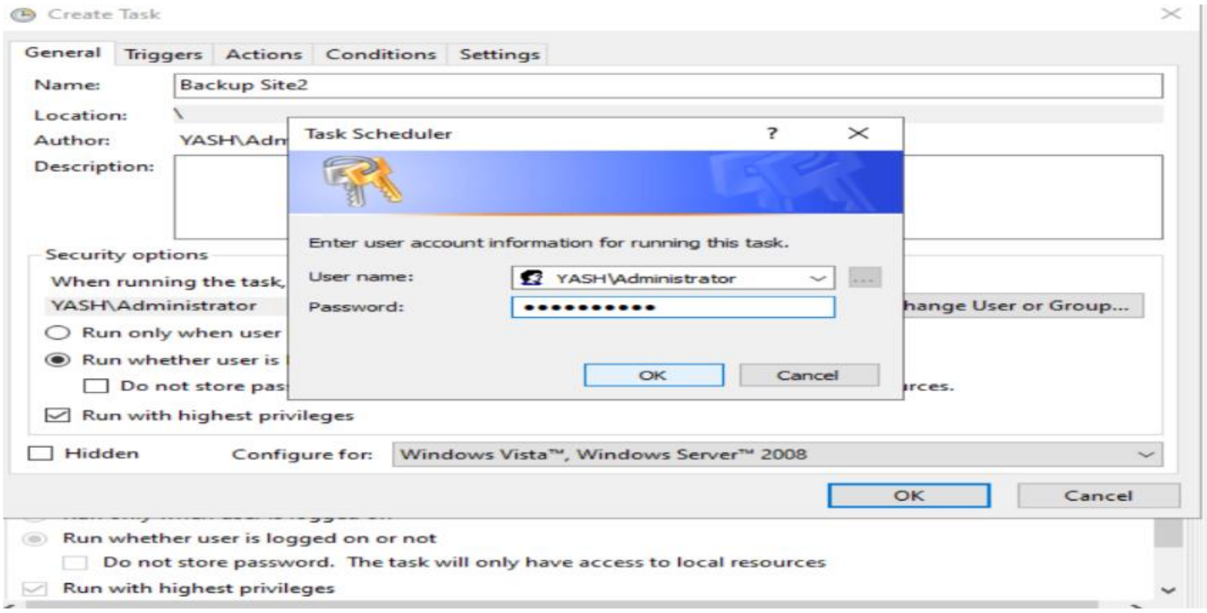
User name: YASH\Administrator

Password: ●●●●●●●●●●●

OK | Cancel

OK | Cancel

(Did same for Site2.)



Name: Backup Site2

Location: \

Author: YASH\Adm

Description:

Security options

When running the task,

YASH\Administrator

○ Run only when user

● Run whether user is

□ Do not store pas

☑ Run with highest privileges

□ Hidden   Configure for: Windows Vista™, Windows Server™ 2008

Task Scheduler

Enter user account information for running this task.

User name: YASH\Administrator

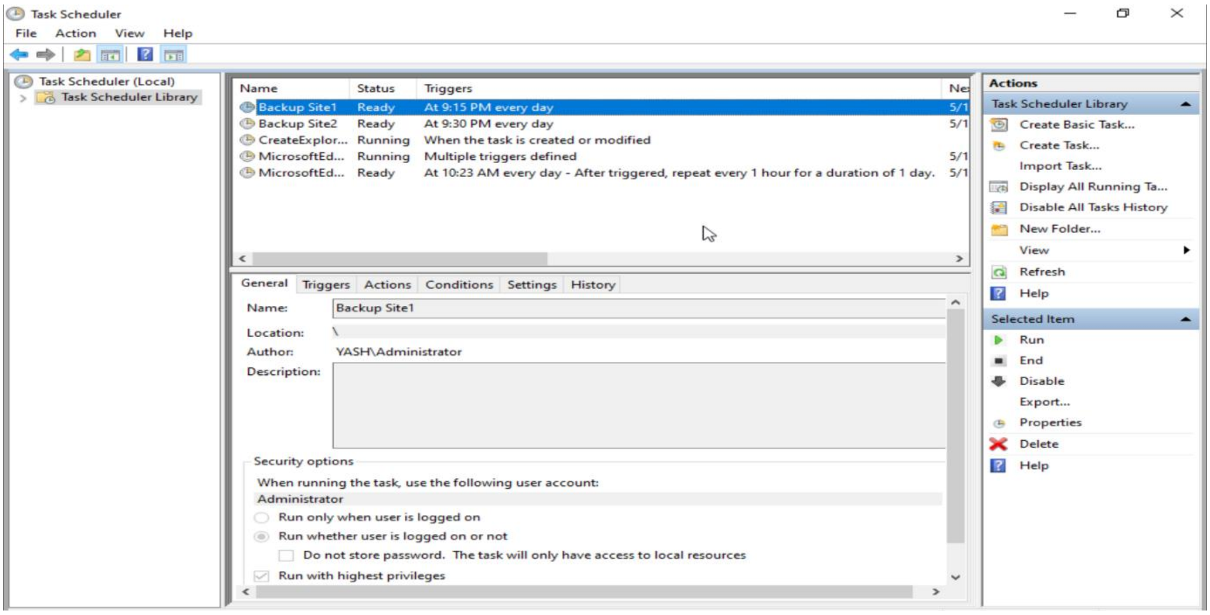
Password: ●●●●●●●●●●●

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

☑ Run with highest privileges

(Created the tasks successfully.)



Name	Status	Triggers	Ne
Backup Site1	Ready	At 9:15 PM every day	5/1
Backup Site2	Ready	At 9:30 PM every day	5/1
CreateExplor...	Running	When the task is created or modified	
MicrosoftEd...	Running	Multiple triggers defined	5/1
MicrosoftEd...	Ready	At 10:23 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	5/1

Name: Backup Site1

Location: \

Author: YASH\Administrator

Description:

Security options

When running the task, use the following user account:

Administrator

○ Run only when user is logged on

● Run whether user is logged on or not

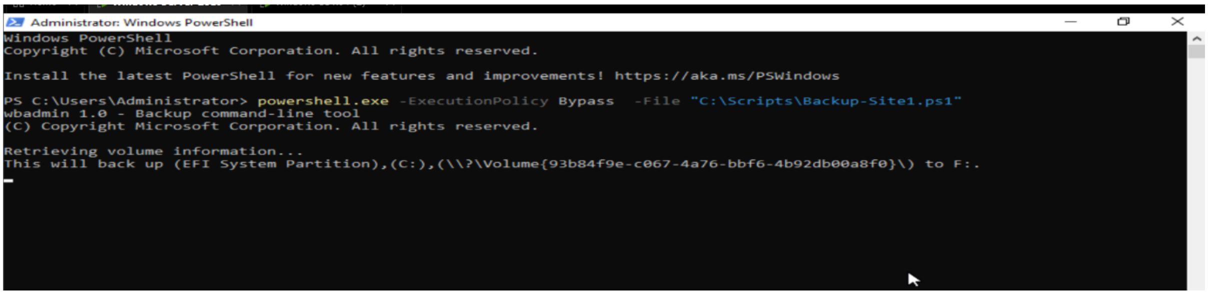
□ Do not store password. The task will only have access to local resources

☑ Run with highest privileges

- **Manual Testing of Backups**

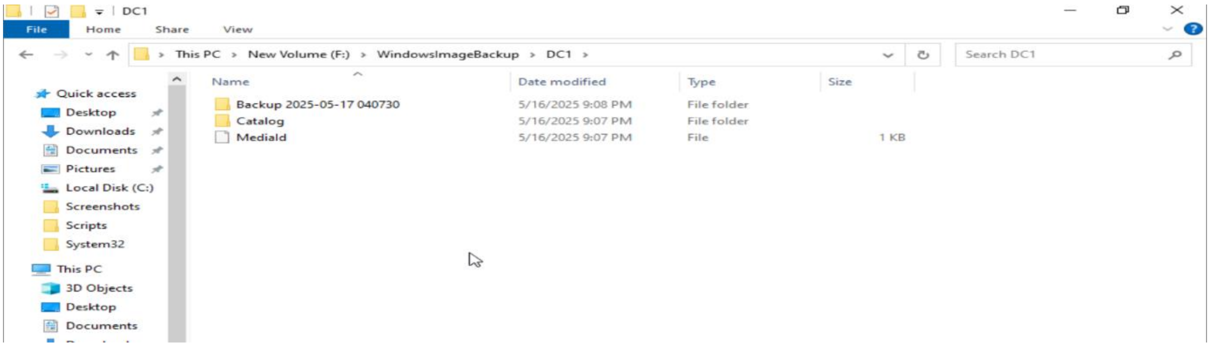
  After scheduling, the scripts were manually triggered to verify correct execution and successful backup creation. Backup logs and system event logs were reviewed to confirm the integrity and completeness of the backups. Any errors or failures were addressed by troubleshooting script parameters or permissions.

(Executed it manually to test.)



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> powershell.exe -ExecutionPolicy Bypass  -File "C:\Scripts\Backup-Site1.ps1"
wbadmin 1.0 - Backup command-line tool
(C) Copyright Microsoft Corporation. All rights reserved.

Retrieving volume information...
This will back up (EFI System Partition),(C:),(\\?\Volume{93b84f9e-c067-4a76-bbf6-4b92db00a8f0}\) to F:.
_
```

(As we can see backup is created in F)



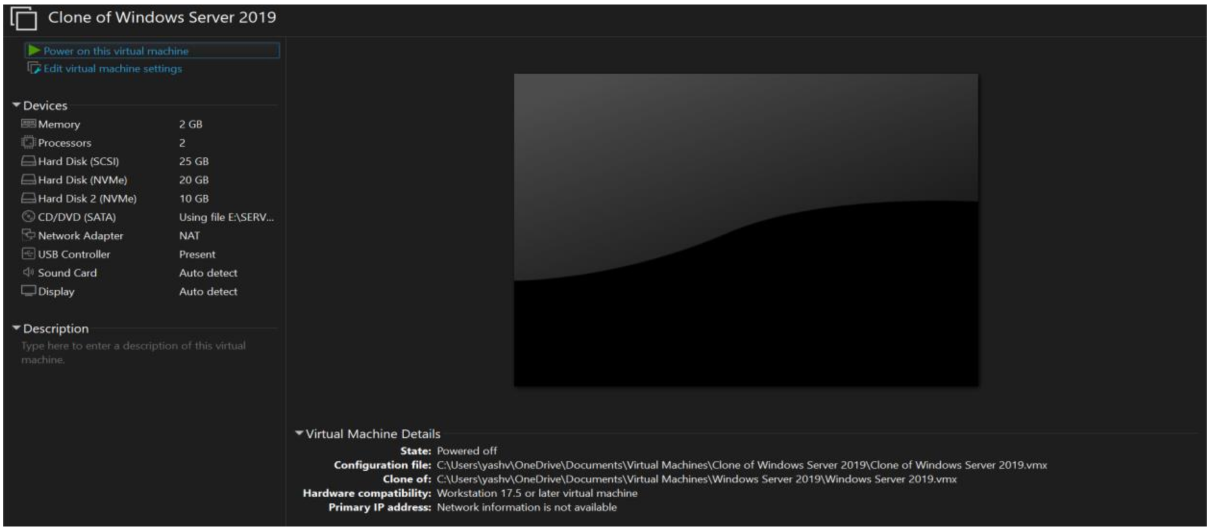
Name	Date modified	Type	Size
Backup 2025-05-17 040730	5/16/2025 9:08 PM	File folder	
Catalog	5/16/2025 9:07 PM	File folder	
MediaId	5/16/2025 9:07 PM	File	1 KB

3.2 Full AD Forest Recovery Testing in Isolated Lab

- **Clone the Domain Controller**

  A virtual machine clone of the original domain controller was created to serve as the recovery target in an isolated lab environment.

(Clone created.)


Clone of Windows Server 2019
Power on this virtual machine
Edit virtual machine settings
Description
Type here to enter a description of this virtual machine.

Devices

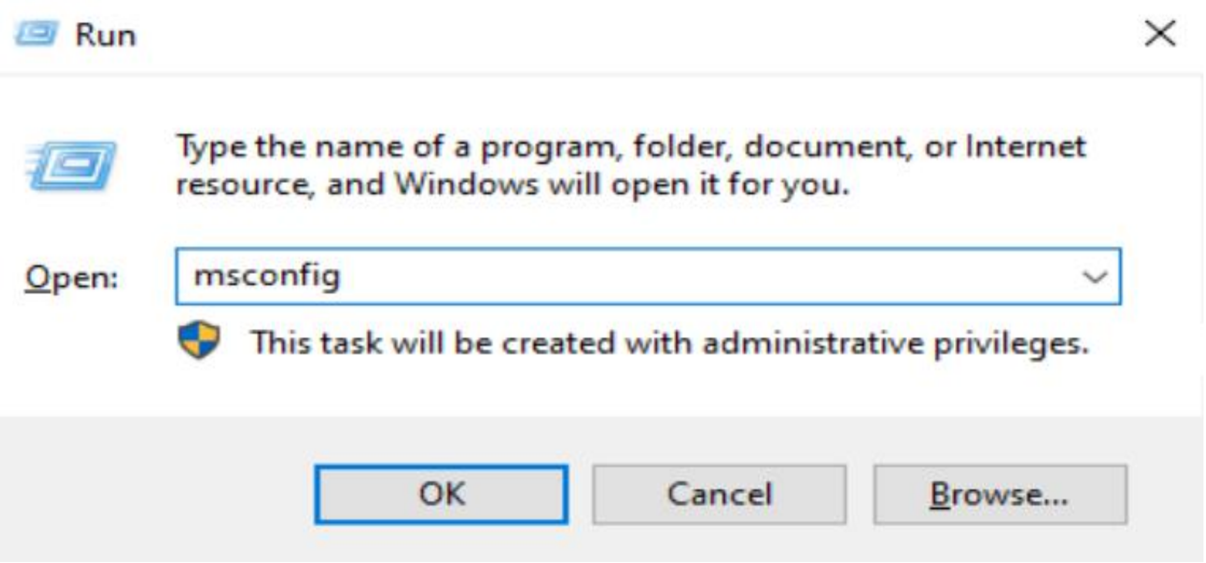
Memory	2 GB
Processors	2
Hard Disk (SCSI)	25 GB
Hard Disk (NVMe)	20 GB
Hard Disk 2 (NVMe)	10 GB
CD/DVD (SATA)	Using file E:\SERV...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Virtual Machine Details

State: Powered off
Configuration file: C:\Users\yashv\OneDrive\Documents\Virtual Machines\Clone of Windows Server 2019\Clone of Windows Server 2019.vmx
Clone of: C:\Users\yashv\OneDrive\Documents\Virtual Machines\Windows Server 2019\Windows Server 2019.vmx
Hardware compatibility: Workstation 17.5 or later virtual machine
Primary IP address: Network information is not available

- **Boot into Directory Services Restore Mode (Safe Mode):** The cloned DC was started in Directory Services Restore Mode (DSRM), which allows offline AD database restoration without interference from normal AD operations.

Navigate to:

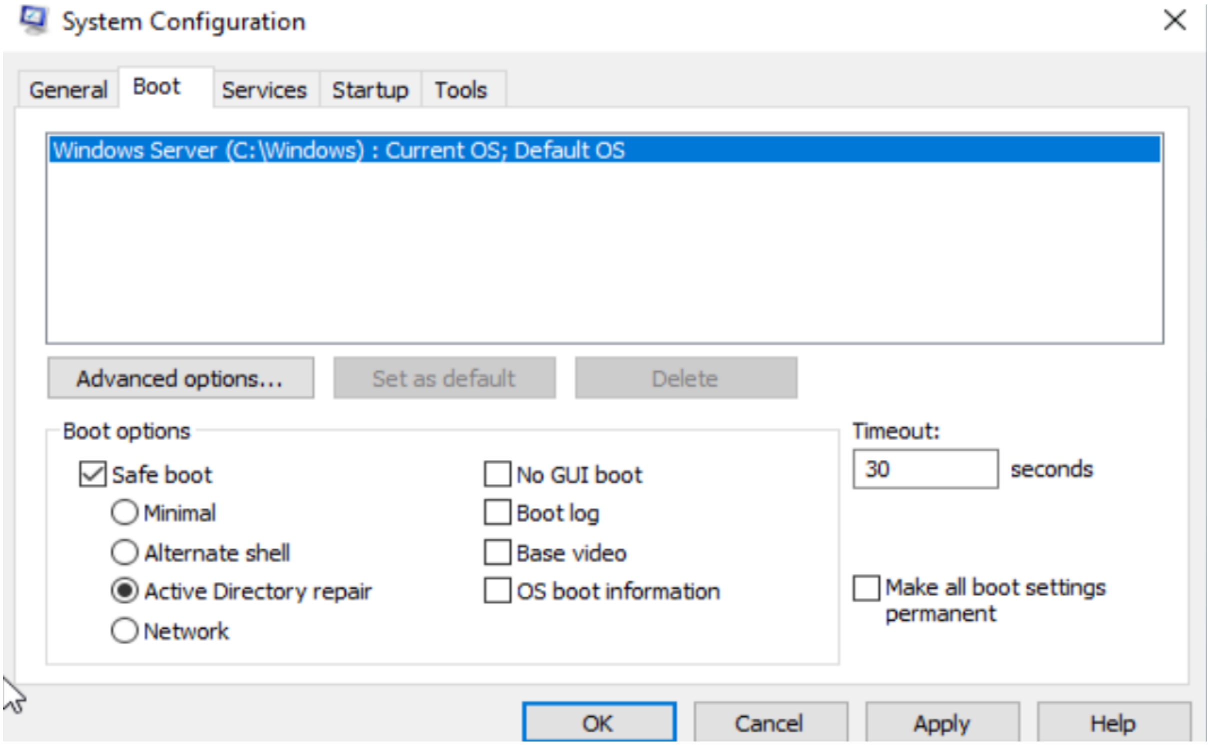


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: msconfig

This task will be created with administrative privileges.

(Check safe mode.)



Windows Server (C:\Windows) : Current OS; Default OS

Boot options

☑ Safe boot

○ Minimal

○ Alternate shell

● Active Directory repair

○ Network

□ No GUI boot

□ Boot log

□ Base video

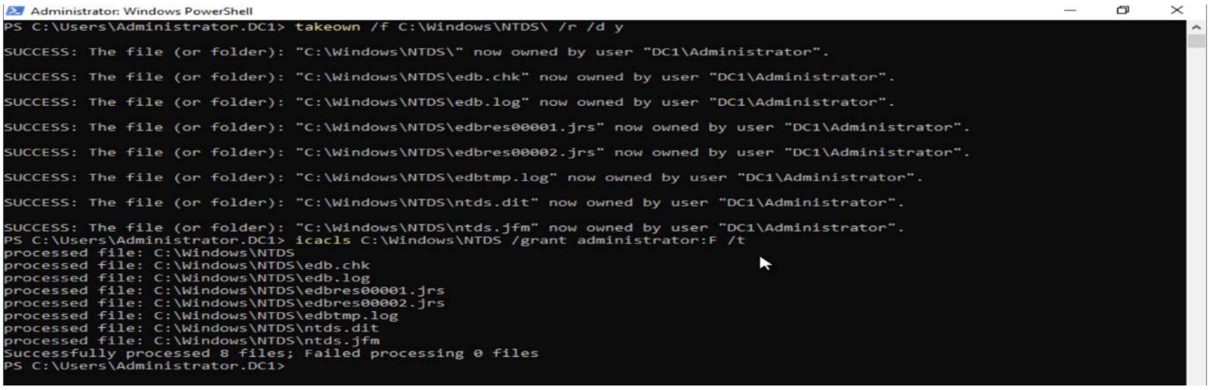
□ OS boot information

Timeout: 30 seconds

□ Make all boot settings permanent

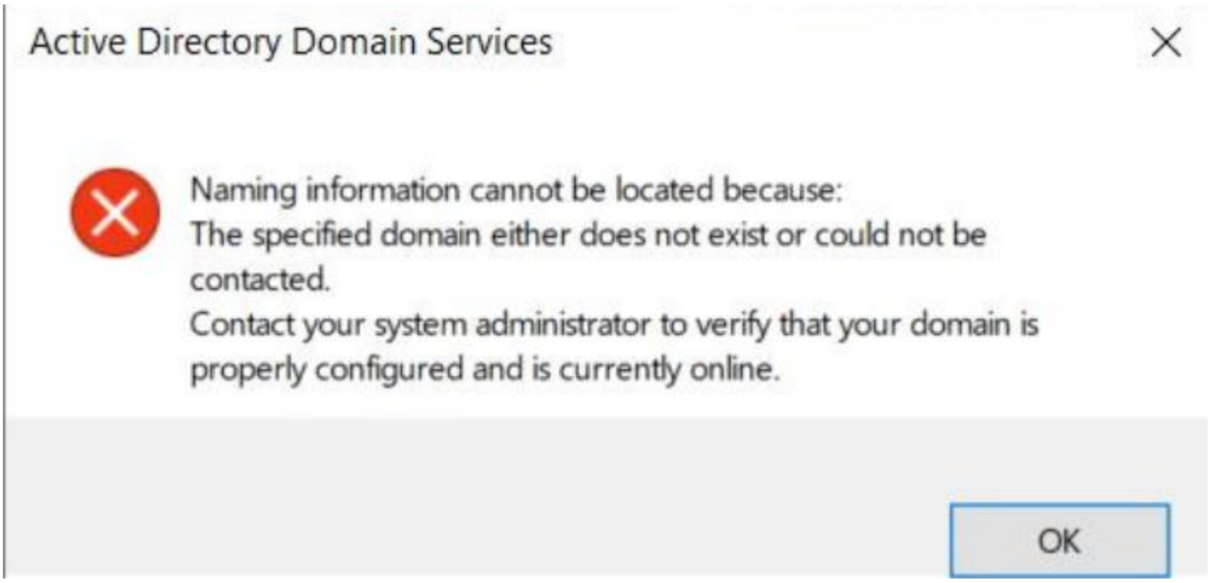
- **Reset Permissions:** Using the takeown and icacls commands, ownership and access permissions on critical AD database files and backup folders were reset to ensure full administrative control during recovery.

(Deleted the Active Directory database files.)



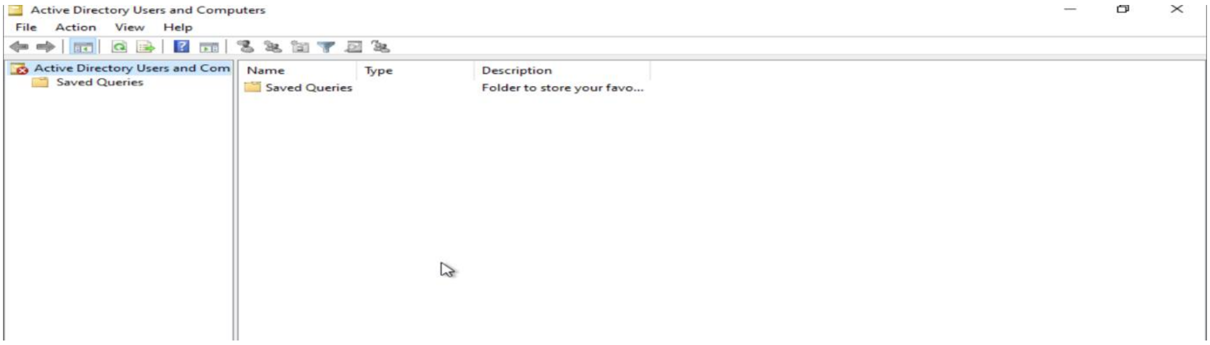
```
PS C:\Users\Administrator.DC1> takeown /f C:\Windows\NTDS\ /r /d y

SUCCESS: The file (or folder): "C:\Windows\NTDS\" now owned by user "DC1\Administrator".

SUCCESS: The file (or folder): "C:\Windows\NTDS\edb.chk" now owned by user "DC1\Administrator".

SUCCESS: The file (or folder): "C:\Windows\NTDS\edb.log" now owned by user "DC1\Administrator".

SUCCESS: The file (or folder): "C:\Windows\NTDS\edbres00001.jrs" now owned by user "DC1\Administrator".

SUCCESS: The file (or folder): "C:\Windows\NTDS\edbres00002.jrs" now owned by user "DC1\Administrator".

SUCCESS: The file (or folder): "C:\Windows\NTDS\edbtmp.log" now owned by user "DC1\Administrator".

SUCCESS: The file (or folder): "C:\Windows\NTDS\ntds.dit" now owned by user "DC1\Administrator".

SUCCESS: The file (or folder): "C:\Windows\NTDS\ntds.jfm" now owned by user "DC1\Administrator".
PS C:\Users\Administrator.DC1> icacls C:\Windows\NTDS /grant administrator:F /t
processed file: C:\Windows\NTDS
processed file: C:\Windows\NTDS\edb.chk
processed file: C:\Windows\NTDS\edb.log
processed file: C:\Windows\NTDS\edbres00001.jrs
processed file: C:\Windows\NTDS\edbres00002.jrs
processed file: C:\Windows\NTDS\edbtmp.log
processed file: C:\Windows\NTDS\ntds.dit
processed file: C:\Windows\NTDS\ntds.jfm
Successfully processed 8 files; Failed processing 0 files
PS C:\Users\Administrator.DC1>
```

(We can see that our AD in damaged.)



Naming information cannot be located because:
The specified domain either does not exist or could not be contacted.
Contact your system administrator to verify that your domain is properly configured and is currently online.

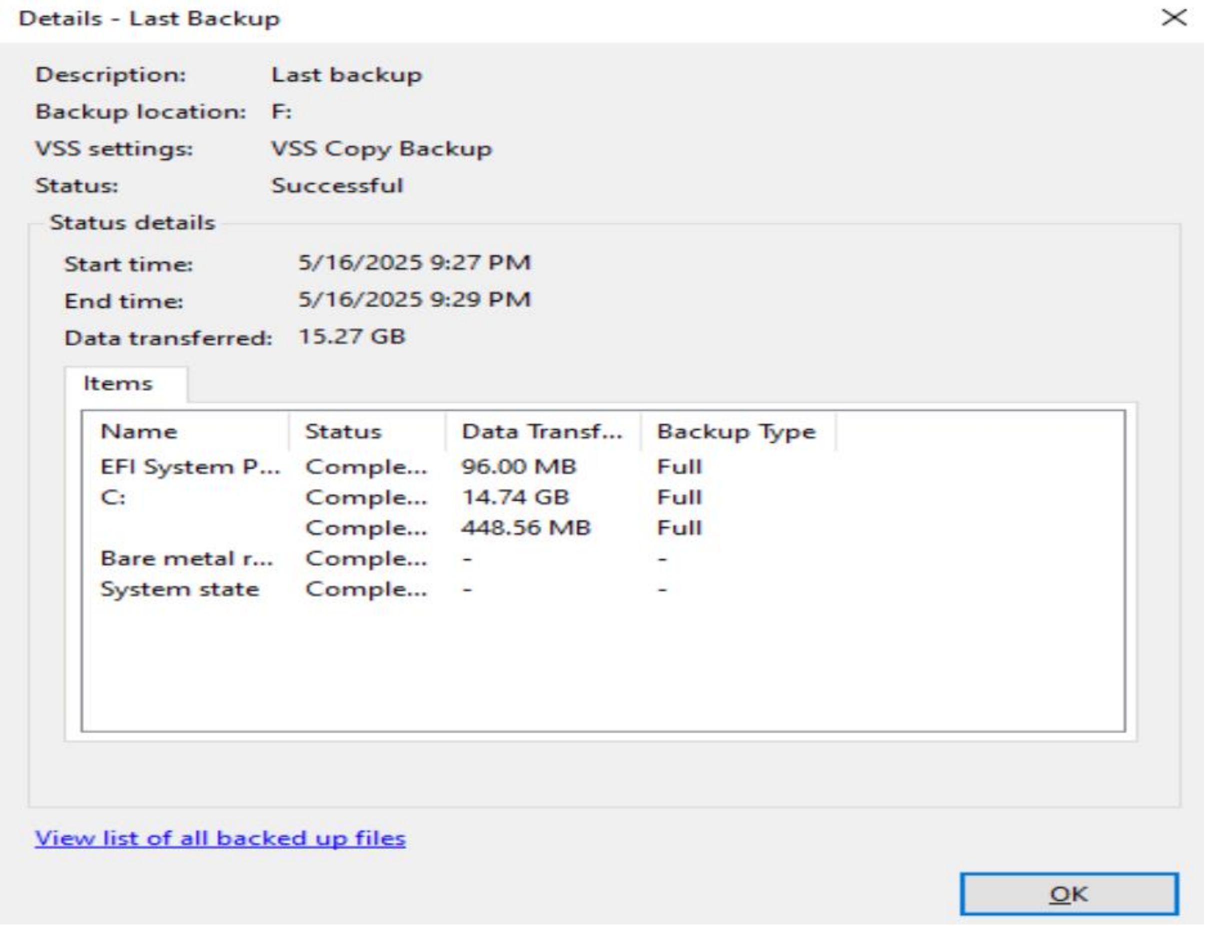
(This is empty as well.)


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries

Name	Type	Description
Saved Queries		Folder to store your favo...

- **Locate Backup:** The system state backup created in Task 54 was identified and prepared for restoration on the cloned DC.

(Backup took place in last task.)



Details - Last Backup

Description: Last backup
Backup location: F:
VSS settings: VSS Copy Backup
Status: Successful

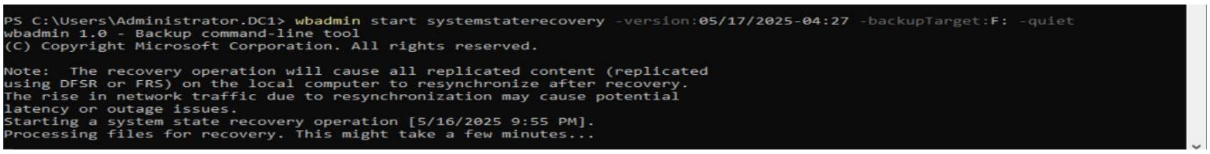
Status details
Start time: 5/16/2025 9:27 PM
End time: 5/16/2025 9:29 PM
Data transferred: 15.27 GB

Items

Name	Status	Data Transf...	Backup Type
EFI System P...	Comple...	96.00 MB	Full
C:	Comple...	14.74 GB	Full
	Comple...	448.56 MB	Full
Bare metal r...	Comple...	-	-
System state	Comple...	-	-

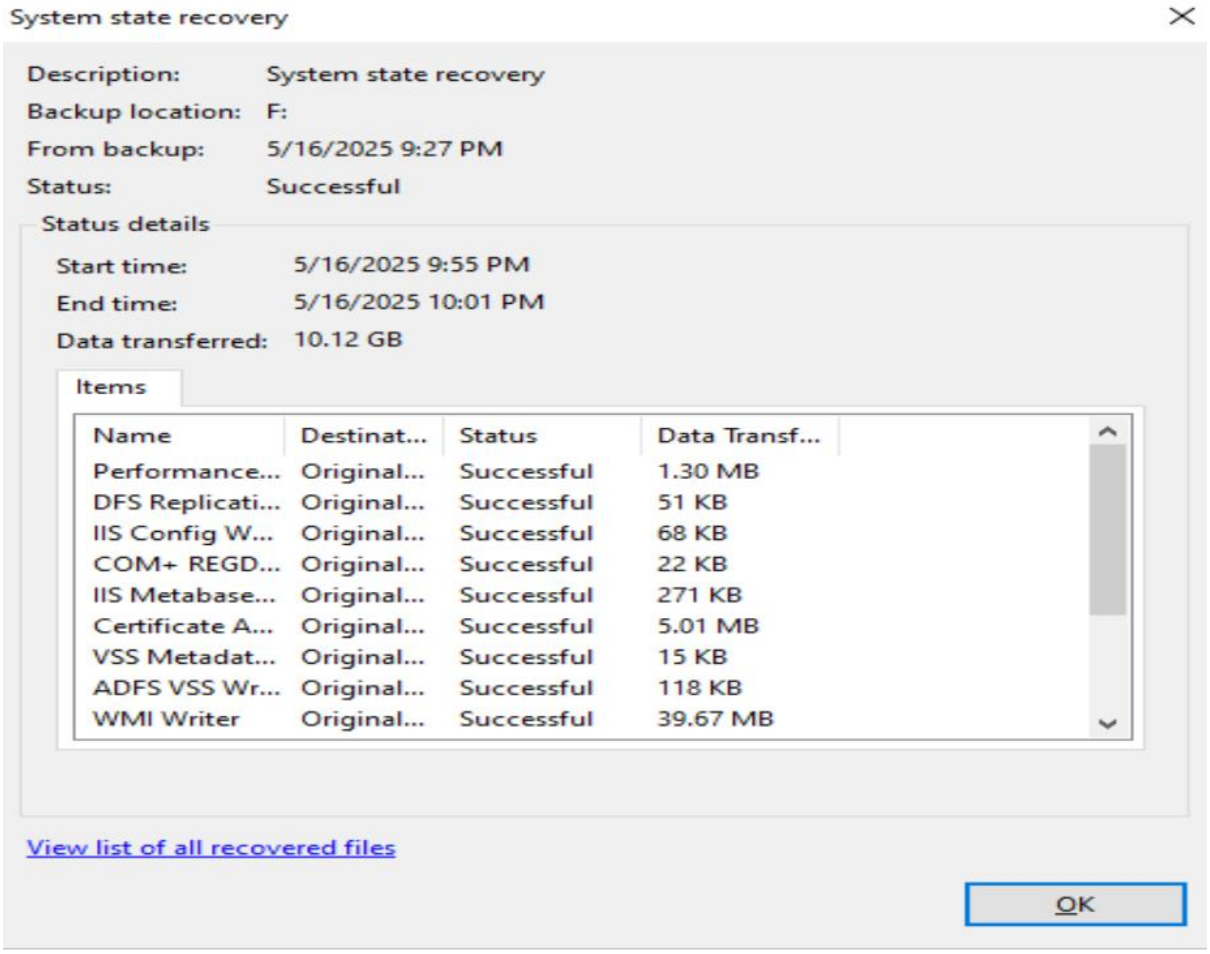
- **Restore Using PowerShell:** The backup was restored with PowerShell cmdlets (wbadmin or similar), recovering the system state including the NTDS database, SYSVOL, and AD configuration.

(Restoring the system state.)



```
PS C:\Users\Administrator.DC1> wbadmin start systemstaterecovery -version:05/17/2025-04:27 -backupTarget:F: -quiet
wbadmin 1.0 - Backup command-line tool
(C) Copyright Microsoft Corporation. All rights reserved.

Note:  The recovery operation will cause all replicated content (replicated
using DFSR or FRS) on the local computer to resynchronize after recovery.
The rise in network traffic due to resynchronization may cause potential
latency or outage issues.
Starting a system state recovery operation [5/16/2025 9:55 PM].
Processing files for recovery. This might take a few minutes...
```

(Successfully completed.)



System state recovery

Description: System state recovery

Backup location: F:

From backup: 5/16/2025 9:27 PM

Status: Successful

Status details

Start time: 5/16/2025 9:55 PM

End time: 5/16/2025 10:01 PM

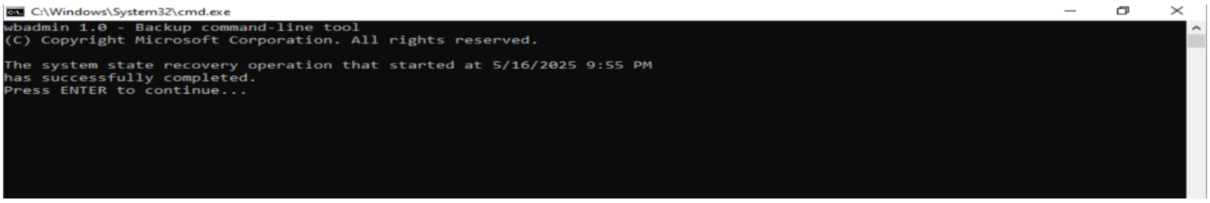
Data transferred: 10.12 GB

Items

Name	Destinat...	Status	Data Transf...
Performance...	Original...	Successful	1.30 MB
DFS Replicati...	Original...	Successful	51 KB
IIS Config W...	Original...	Successful	68 KB
COM+ REGD...	Original...	Successful	22 KB
IIS Metabase...	Original...	Successful	271 KB
Certificate A...	Original...	Successful	5.01 MB
VSS Metadat...	Original...	Successful	15 KB
ADFS VSS Wr...	Original...	Successful	118 KB
WMI Writer	Original...	Successful	39.67 MB

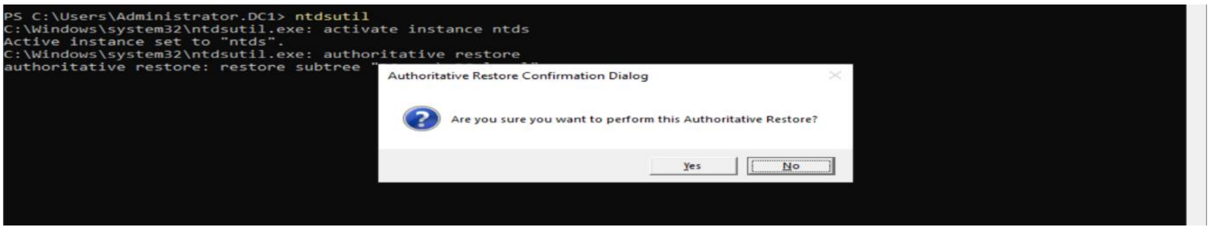
- **Reboot and Authoritative Restore:** After the initial restoration and reboot, the ntdsutil tool was used to perform an authoritative restore. This step marks the restored data as the master copy, ensuring it replicates correctly to other domain controllers once back online.

(After reboot we can see it id done.)



```
wbadmin 1.0 - Backup command-line tool
(C) Copyright Microsoft Corporation. All rights reserved.

The system state recovery operation that started at 5/16/2025 9:55 PM
has successfully completed.
Press ENTER to continue...
```

(Authoritative restore.)

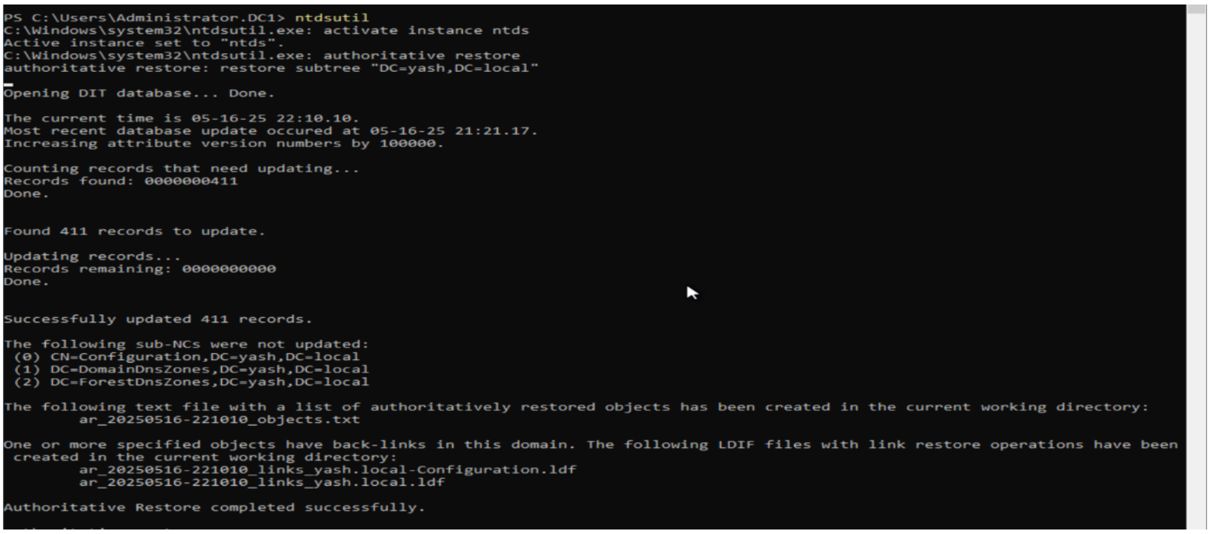


```
PS C:\Users\Administrator.DC1> ntdsutil
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: authoritative restore
authoritative restore: restore subtree "
```

Authoritative Restore Confirmation Dialog

Are you sure you want to perform this Authoritative Restore?

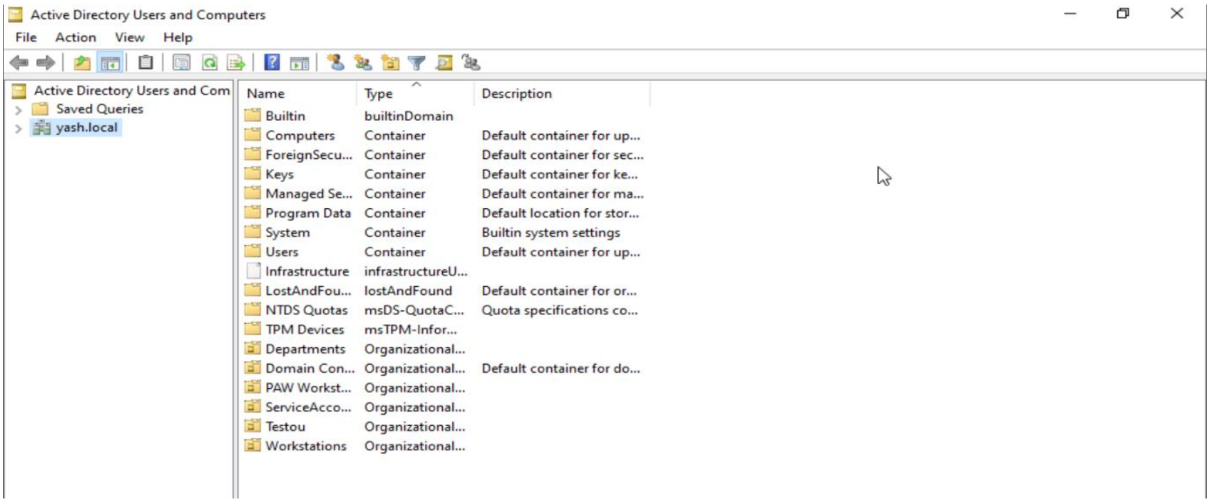
(Completed Successfully.)



```
PS C:\Users\Administrator.DC1> ntdsutil
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: authoritative restore
authoritative restore: restore subtree "DC=yash,DC=local"

Opening DIT database... Done.

The current time is 05-16-25 22:10.10.
Most recent database update occured at 05-16-25 21:21.17.
Increasing attribute version numbers by 100000.

Counting records that need updating...
Records found: 0000000411
Done.


Found 411 records to update.

Updating records...
Records remaining: 0000000000
Done.


Successfully updated 411 records.

The following sub-NCs were not updated:
 (0) CN=Configuration,DC=yash,DC=local
 (1) DC=DomainDnsZones,DC=yash,DC=local
 (2) DC=ForestDnsZones,DC=yash,DC=local

The following text file with a list of authoritatively restored objects has been created in the current working directory:
        ar_20250516-221010_objects.txt

One or more specified objects have back-links in this domain. The following LDIF files with link restore operations have been
 created in the current working directory:
        ar_20250516-221010_links_yash.local-Configuration.ldf
        ar_20250516-221010_links_yash.local.ldf

Authoritative Restore completed successfully.
```

- **Verify AD Recovery:** Post-recovery, AD functionality was validated by checking domain controller health, replication status, and user authentication to confirm that the forest had been successfully restored.

(Recovered Successfully.)



Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
yash.local

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
ForeignSecu...	Container	Default container for sec...
Keys	Container	Default container for ke...
Managed Se...	Container	Default container for ma...
Program Data	Container	Default location for stor...
System	Container	Builtin system settings
Users	Container	Default container for up...
Infrastructure	infrastructureU...	
LostAndFou...	lostAndFound	Default container for or...
NTDS Quotas	msDS-QuotaC...	Quota specifications co...
TPM Devices	msTPM-Infor...	
Departments	Organizational...	
Domain Con...	Organizational...	Default container for do...
PAW Workst...	Organizational...	
ServiceAcco...	Organizational...	
Testou	Organizational...	
Workstations	Organizational...	

4. Results And Findings

This section summarizes the outcomes observed during the implementation of the site-aware AD backup strategy and the full AD forest recovery testing. It highlights the successes, challenges, and key observations that inform the effectiveness of the disaster recovery plan.

4.1 Successful Creation of Site-Aware Backup Strategy

Backup scripts tailored to each AD site executed as scheduled without interfering with normal network operations, demonstrating effective site-specific backup management.

4.2 Backup Integrity Verified Through Manual Testing

Manual execution and verification confirmed that backups included all necessary AD components such as system state and NTDS database, ensuring recoverability.

4.3 Cloned Domain Controller Restoration Validated

The cloned DC booted into Directory Services Restore Mode successfully, and backup restoration procedures worked as expected, showing the lab environment's fidelity.

4.4 Authoritative Restore Ensured Forest Consistency

Using ntdsutil to perform an authoritative restore maintained replication integrity across the AD forest, preventing outdated or corrupted data from propagating.

4.5 Identified Gaps in Permissions and Automation

Initial challenges with file ownership and permissions required manual intervention using takeown and icacls, indicating a need for improved automation and permission management in recovery scripts.

5. Recommendations

Based on the results and findings, several recommendations are proposed to enhance the AD backup and recovery process, improve reliability, and reduce recovery time in case of disasters.

5.1 **Implement Centralized Backup Management**

Utilize centralized tools like Microsoft System Center Data Protection Manager (SCDPM) to automate backups across sites, simplifying management and reporting.

5.2 **Enhance Backup Automation and Monitoring**

Develop robust automated alerting and logging mechanisms to detect backup failures immediately and reduce manual oversight requirements.

5.3 **Regularly Update and Test Recovery Procedures**

Schedule periodic full AD forest recovery drills in isolated labs to keep recovery plans current and IT staff proficient.

5.4 **Strengthen Permissions and Access Controls**

Refine permissions on backup files and recovery environments to minimize manual permission resets during restoration, improving efficiency.

5.5 **Document Detailed Runbooks and Checklists**

Create comprehensive step-by-step documentation for both backup and recovery processes to ensure consistent execution during high-pressure disaster events.

6. Conclusion

This project successfully demonstrated the critical importance of implementing a site-aware Active Directory backup strategy combined with thorough recovery testing. By tailoring backup schedules to specific sites, the organization can optimize resource use and minimize disruptions during backup operations. The lab-based full AD forest recovery validated the reliability of the backups and prepared the team to respond effectively to potential disasters. Additionally, the exercise highlighted the necessity of automating backup processes and maintaining detailed documentation to reduce human error and accelerate recovery times. Proper permissions management was also identified as essential to streamline restoration workflows. Overall, the project underscores that disaster recovery is an ongoing process that requires continuous improvement through regular testing and updates to adapt to evolving infrastructure and technologies.