Advanced Active Directory Management and Group Policy Implementation

Submitted to:
L&T EduTech

By:
Aabhash Paudel
Chudaraj Kushwaha
Satyam Raut

Sri Venkateshwara College of Engineering And Technology

November 2024

Project Report

Advanced Active Directory Management and Group Policy Implementation

1. Introduction

Active Directory Domain Services (AD DS) is a core part of Windows Server and provides centralised management and authentication for users, computers, etc. on a network. The objective of this project was to implement an Active Directory Domain Services (AD DS) environment, experiment with some of the advanced management features and create Group Policies to deploy security and operating policies.

This document summarises the activities, methodologies, lessons learned and results. This project acts as a simulation to learn enterprise Active Directory

2. Objectives

The primary objectives of this project were:

1. To configure a new Active Directory Forest and promote servers as domain-controllers (DC).
2. To explore advanced Domain-Controller (DC) options such as cloning and read-only Domain-Controllers (RODCs).
3. To implement and manage advanced security configurations like Password Settings Objects (PSOs), Authentication Policies, and Managed Service Accounts (MSA).
4. To configure and manage Group Policy Objects (GPOs) including linking, filtering, and precedence.1. Introduction

Active Directory Domain Services (AD DS) is a core part of Windows Server and provides centralised management and authentication for users, computers, etc. on a network. The objective of this project was to implement an Active Directory Domain Services (AD DS) environment, experiment with some of the advanced management features and create Group Policies to deploy security and operating policies.

This document summarises the activities, methodologies, lessons learned and results. This project acts as a simulation to learn enterprise Active Directory

2. Objectives

The primary objectives of this project were:

1. To configure a new Active Directory Forest and promote servers as domain-controllers (DC).
2. To explore advanced Domain-Controller (DC) options such as cloning and read-only Domain-Controllers (RODCs).
3. To implement and manage advanced security configurations like Password Settings Objects (PSOs), Authentication Policies, and Managed Service Accounts (MSA).
4. To configure and manage Group Policy Objects (GPOs) including linking, filtering, and precedence.
5. To simulate and document recovery procedures for Active Directory Domain Services.

3. Methodology

3.1 Environment Setup

Tools Used:

Oracle VirtualBox: Virtualization platform for creating isolated environments.

Windows Server 2019: Installed as the operating system for Domain Controllers.

Active Directory Domain Services (AD DS): Configured for directory management.

Group Policy Management Console (GPMC): Used for managing Group Policies.

Network Setup:

The virtual machines were connected via the host laptop’s mobile hotspot using a bridged adapter to simulate an enterprise environment with internet connectivity.

3.2 Step-by-Step Implementation

1. Configuring AD DS for a New Forest:

- Installed the AD DS role and promoted the server as a Domain Controller (DC) for a new forest (example.local).

- Configure the Directory Services Restore Mode (DSRM) password.

2. Adding a Secondary Domain Controller:

- Installed a second Windows Server 2019 instance.

- Joined the secondary server to the existing domain and promoted it to a DC.

3. Exploring Advanced DC Options:

- DC Cloning: Tested the process of cloning a domain controller using VM to create a configuration file.

- RODC Setup: Configured a Read-Only Domain Controller to improve security in branch office scenarios.

4. Configuring Security Policies:

- Created Password Settings Objects (PSOs) for enforcing strict password policies.

- Configured Authentication Policies and Silos to restrict access to sensitive resources.

- Set up Managed Service Accounts (MSA) for secure service account management.

5. Group Policy Implementation:

- Created and linked GPOs for domain-wide password policies and user restrictions.

- Configured Administrative Templates to control system settings.

- Used WMI filters to apply GPOs selectively to specific machines or users.

6. Simulating Recovery Procedures:

- Performed a system state backup and restored the AD DS environment in Directory Services Restore Mode (DSRM).

4. Findings

1. AD DS Configurations:

- The new forest and root domain were configured successfully.

- Adding and promoting additional domain controllers enhanced redundancy and load balancing.

2. Advanced DC Features:

- Cloning a DC was effective for rapid deployment but required thorough testing in production scenarios.

- RODCs provided secure access for remote sites but required careful delegation of administrator privileges.

3. Group Policy Management:

- Linking GPOs at the domain and OU levels allowed good control of user and computer settings.

- WMI filters enabled the application of policies to specific subsets of machines, improving efficiency.

4. Recovery Procedures:

- The system state backup and restore process highlighted the importance of scheduled/periodic backups in disaster recovery planning.
  5. To simulate and document recovery procedures for Active Directory Domain Services.

3. Methodology

3.1 Environment Setup

Tools Used:

- *Oracle VirtualBox*: Virtualization platform for creating isolated environments.

- *Windows Server 2019*: Installed as the operating system for Domain Controllers.

- *Active Directory Domain Services (AD DS)*: Configured for directory management.

- *Group Policy Management Console (GPMC)*: Used for managing Group Policies.

Network Setup:

The virtual machines were connected via the host laptop's mobile hotspot using a bridged adapter to simulate an enterprise environment with internet connectivity.

3.2 Step-by-Step Implementation

1. Configuring AD DS for a New Forest:
   - Installed the AD DS role and promoted the server as a Domain Controller (DC) for a new

forest (example.local).
- Configure the Directory Services Restore Mode (DSRM) password.

2. Adding a Secondary Domain Controller:
- Installed a second Windows Server 2019 instance.
- Joined the secondary server to the existing domain and promoted it to a DC.
3. Exploring Advanced DC Options:
- DC Cloning: Tested the process of cloning a domain controller using VM to create a configuration file.
- RODC Setup: Configured a Read-Only Domain Controller to improve security in branch office scenarios.

4. Configuring Security Policies:
- Created Password Settings Objects (PSOs) for enforcing strict password policies.
- Configured Authentication Policies and Silos to restrict access to sensitive resources.
- Set up Managed Service Accounts (MSA) for secure service account management.

5. Group Policy Implementation:
- Created and linked GPOs for domain-wide password policies and user restrictions.
- Configured Administrative Templates to control system settings.
- Used WMI filters to apply GPOs selectively to specific machines or users.

6. Simulating Recovery Procedures:
- Performed a system state backup and restored the AD DS environment in Directory Services Restore Mode (DSRM).

4. Findings

1. AD DS Configurations:
- The new forest and root domain were configured successfully.
- Adding and promoting additional domain controllers enhanced redundancy and load balancing.
2. Advanced DC Features:
- Cloning a DC was effective for rapid deployment but required thorough testing in production scenarios.
- RODCs provided secure access for remote sites but required careful delegation of administrator privileges.

3. Group Policy Management:
- Linking GPOs at the domain and OU levels allowed good control of user and computer settings.
- WMI filters enabled the application of policies to specific subsets of machines, improving efficiency.

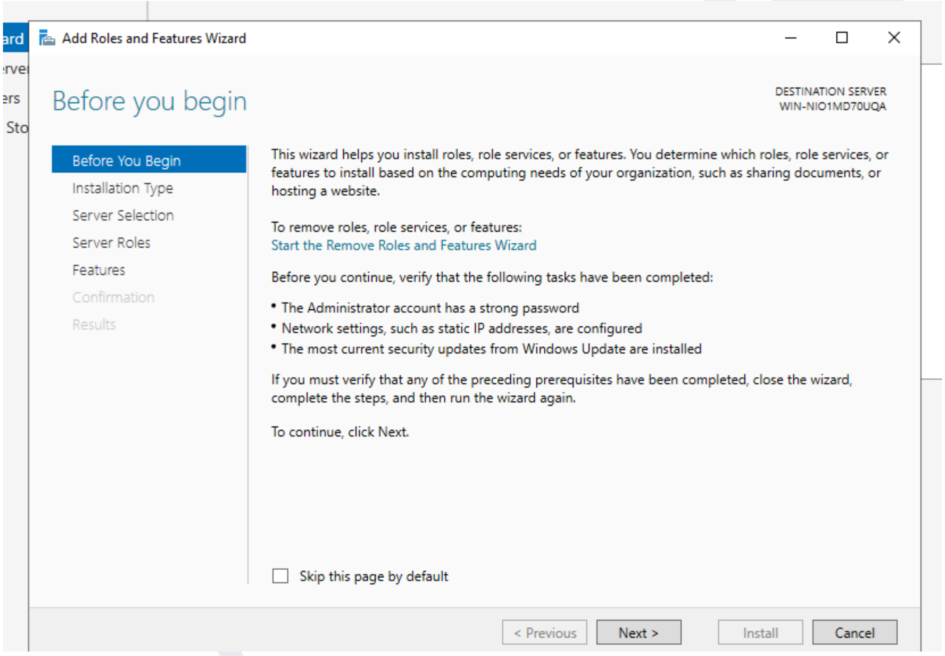
4. Recovery Procedures:
- The system state backup and restore process highlighted the importance of scheduled/periodic backups in disaster recovery planning.

5. Documentation

Key Configuration Screenshots:
- Screenshots captured during the project included AD DS installation and promotion steps, configuration of Password Settings Objects and Authentication Silos, and Group Policy Management Console (GPMC) for GPO linking and editing.

5.1 **Configure Active Directory Domain Services (AD DS)**

1. Install AD DS Role:



Before you begin

DESTINATION SERVER
WIN-NIO1MD70UQA

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

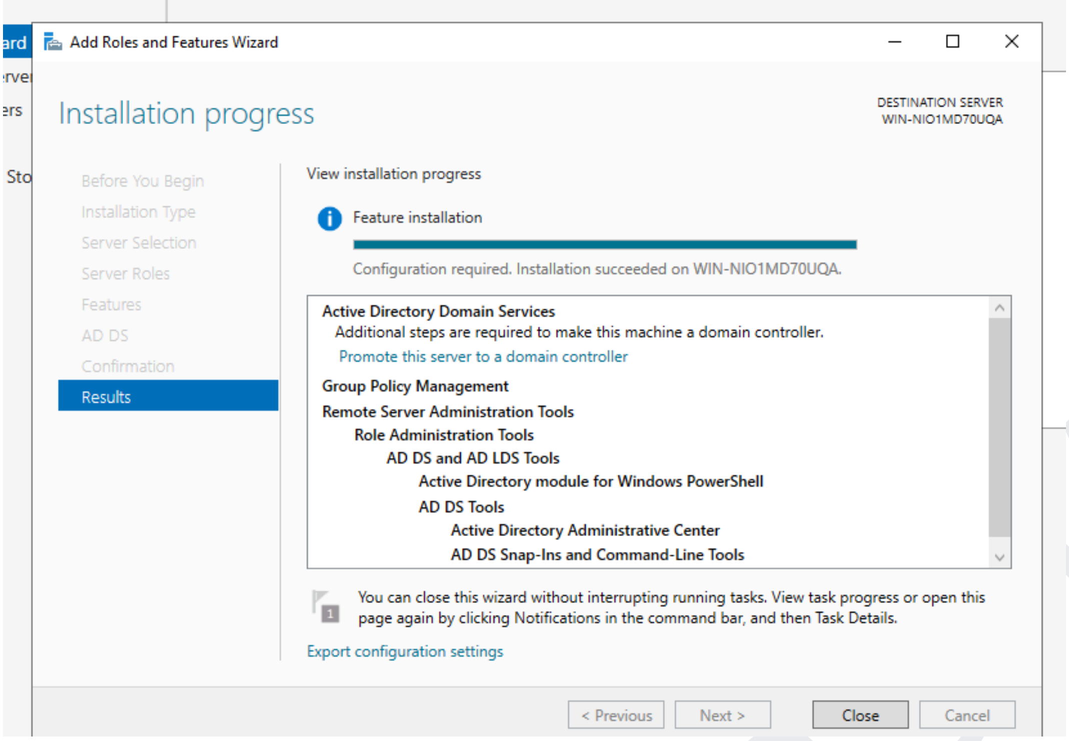
Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default



Installation progress

DESTINATION SERVER
WIN-NIO1MD70UQA

View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-NIO1MD70UQA.

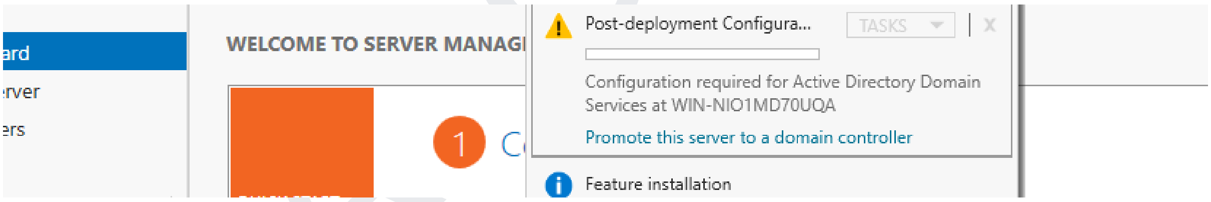
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Promote the Server to a Domain Controller:

After installation, click the **Promote this server to a domain controller** link.



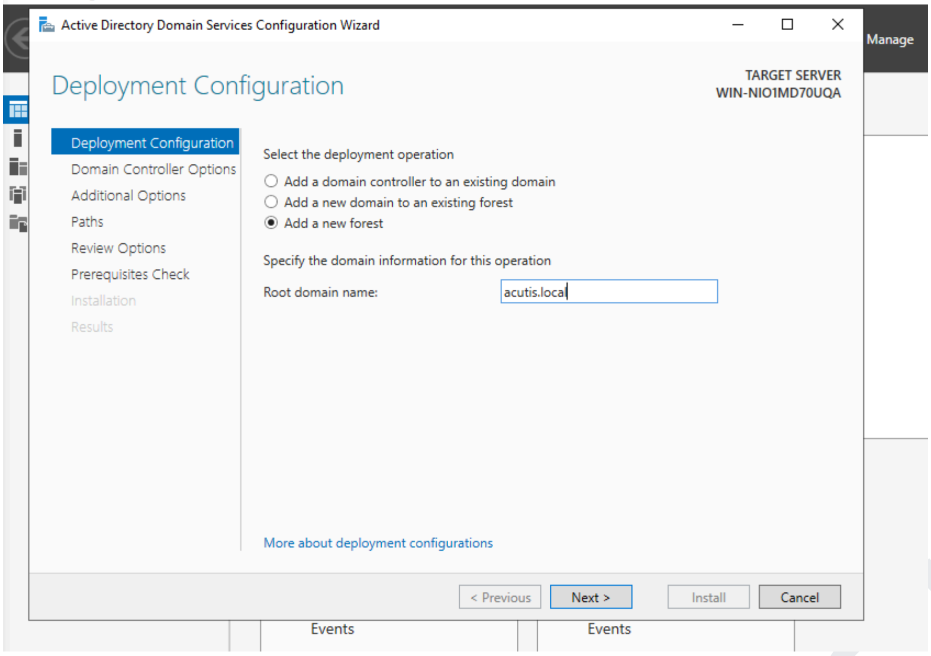
Post-deployment Configura...

Configuration required for Active Directory Domain Services at WIN-NIO1MD70UQA

Promote this server to a domain controller

Feature installation

Root domain name was setup as : **acutis.local**



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WIN-NIO1MD70UQA

Select the deployment operation

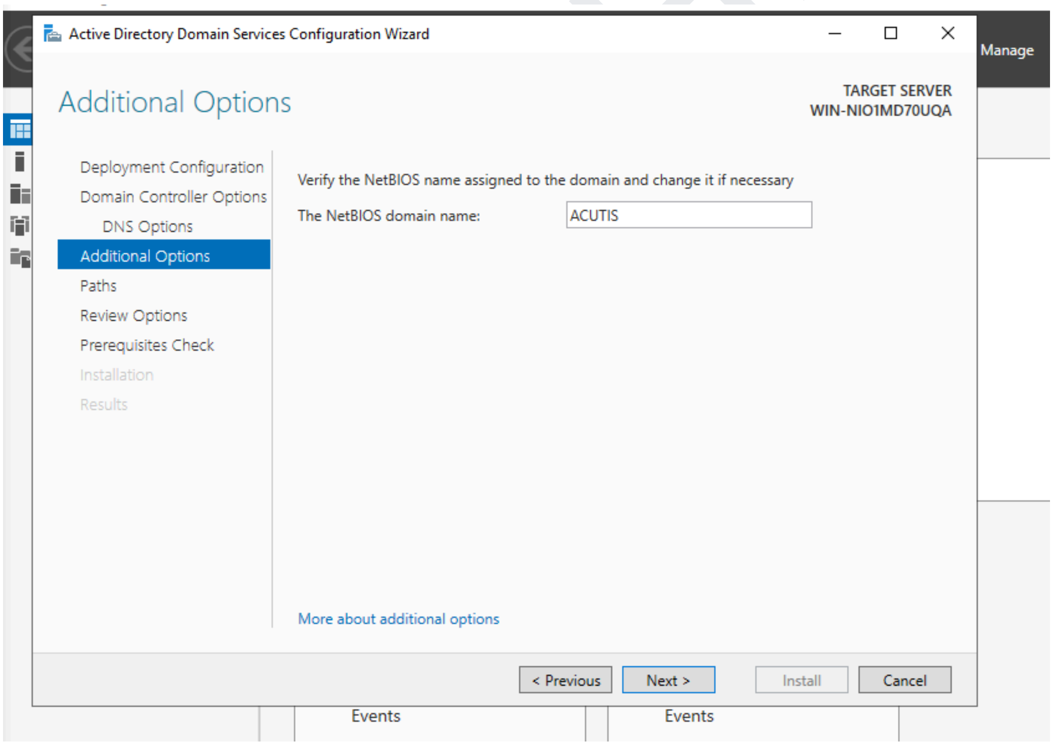
○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: acutis.local

More about deployment configurations

Follow the wizard, setting up the Directory Services Restore Mode (DSRM) password.



Active Directory Domain Services Configuration Wizard

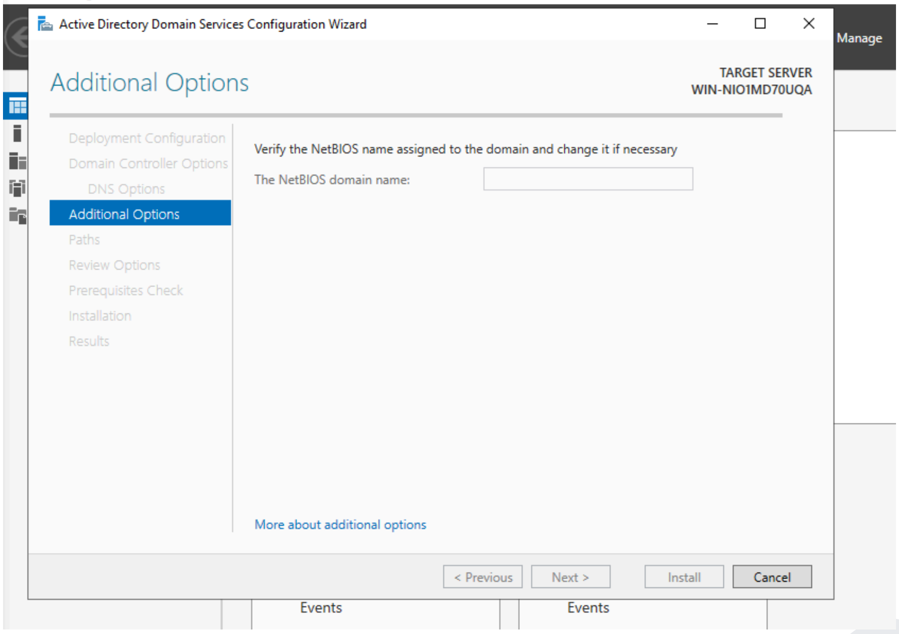
Additional Options

TARGET SERVER
WIN-NIO1MD70UQA

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: ACUTIS

More about additional options



Active Directory Domain Services Configuration Wizard

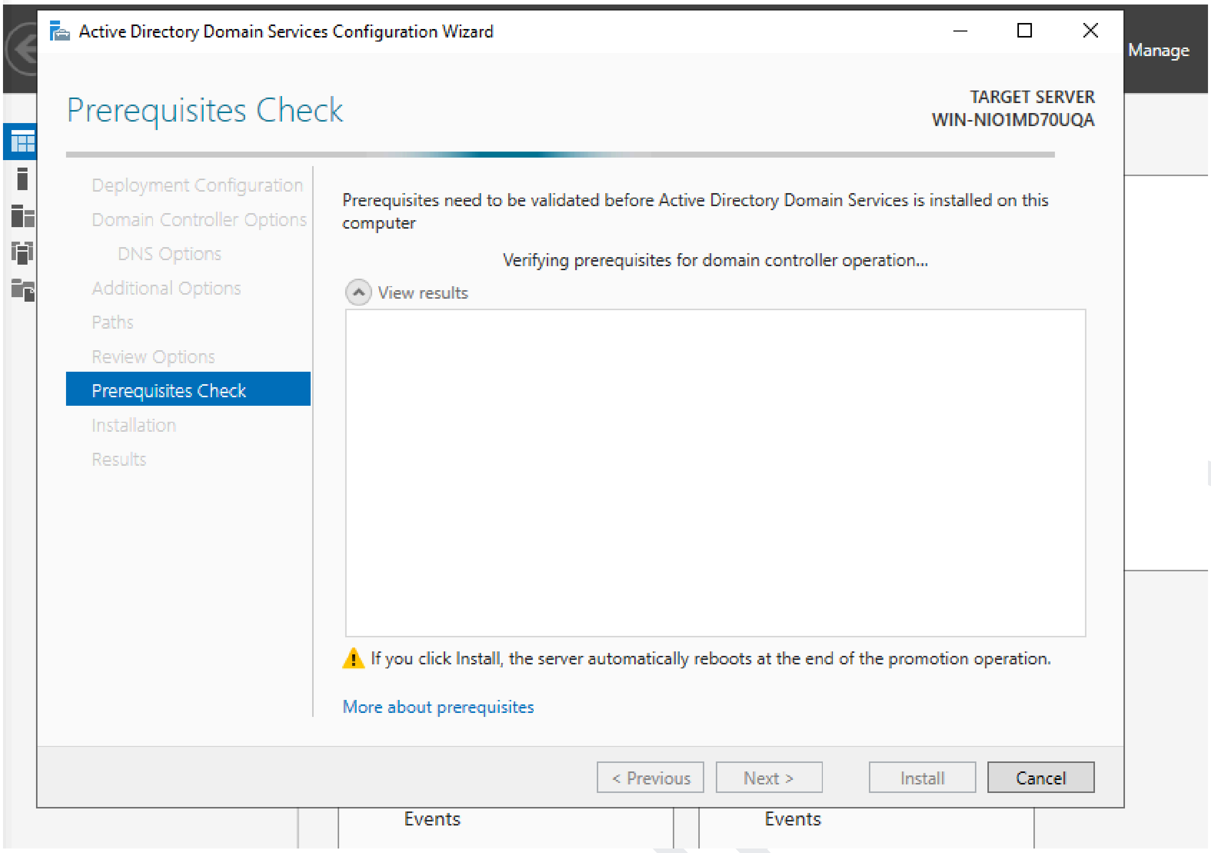
Additional Options

TARGET SERVER
WIN-NIO1MD70UQA

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

More about additional options



Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
WIN-NIO1MD70UQA

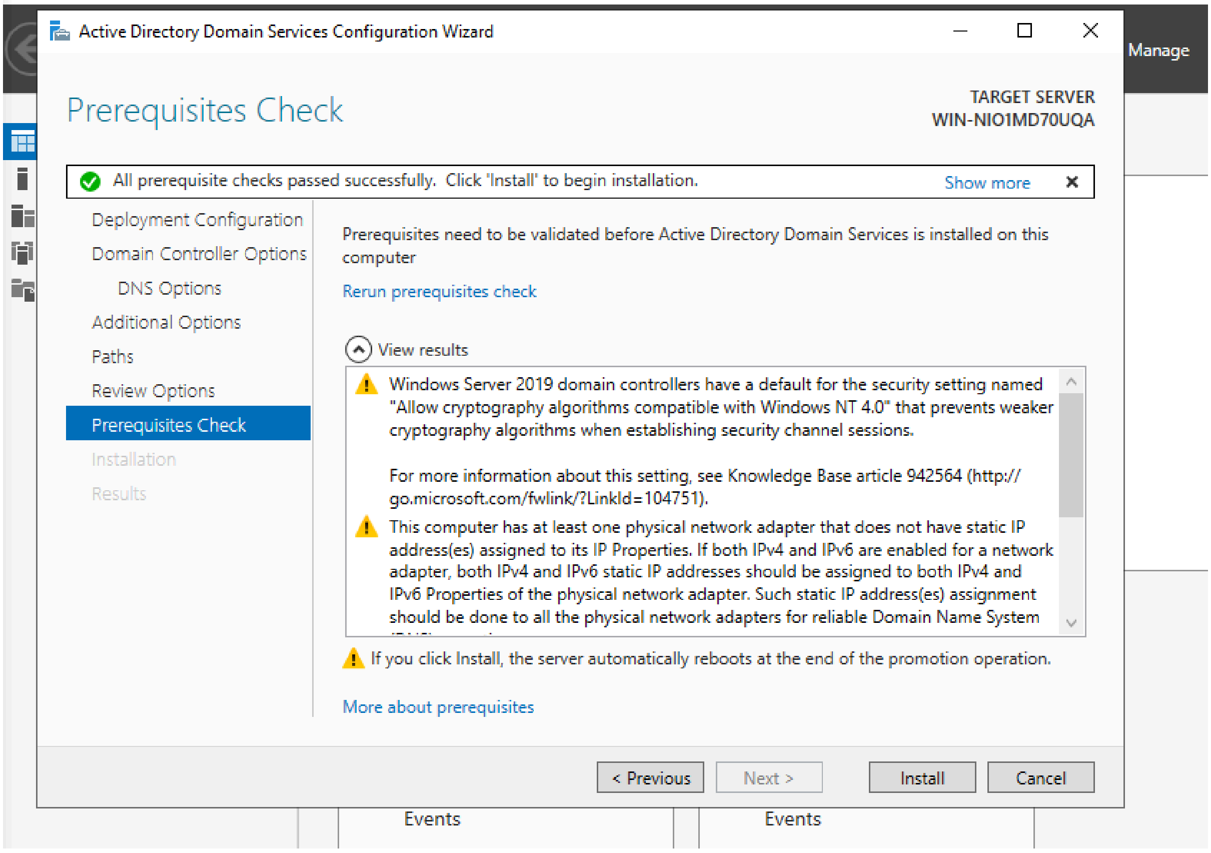
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Verifying prerequisites for domain controller operation...

View results

⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

More about prerequisites



Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
WIN-NIO1MD70UQA

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation. Show more ✕

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Rerun prerequisites check

View results

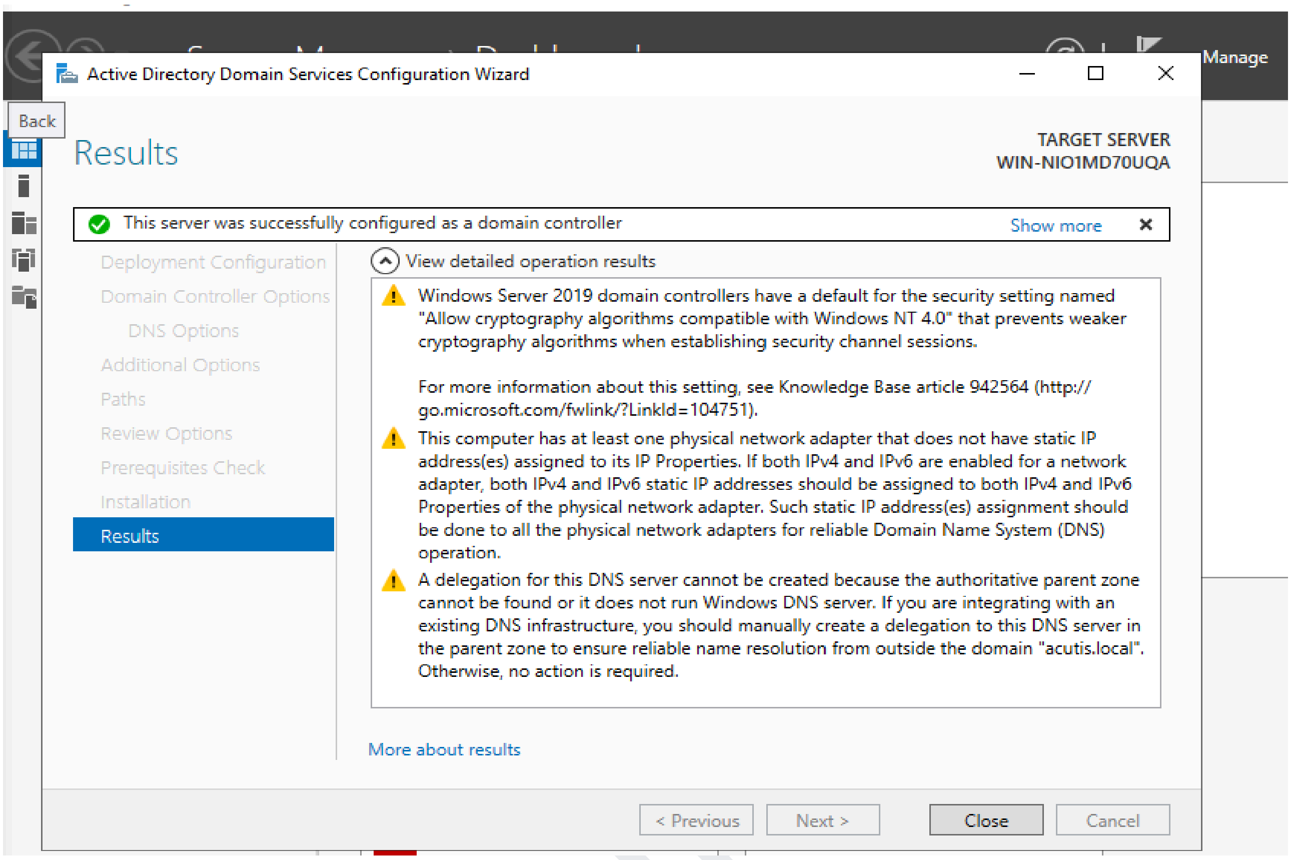
⚠ Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

⚠ This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System

⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

More about prerequisites



Results

TARGET SERVER
WIN-NIO1MD70UQA

This server was successfully configured as a domain controller Show more

View detailed operation results

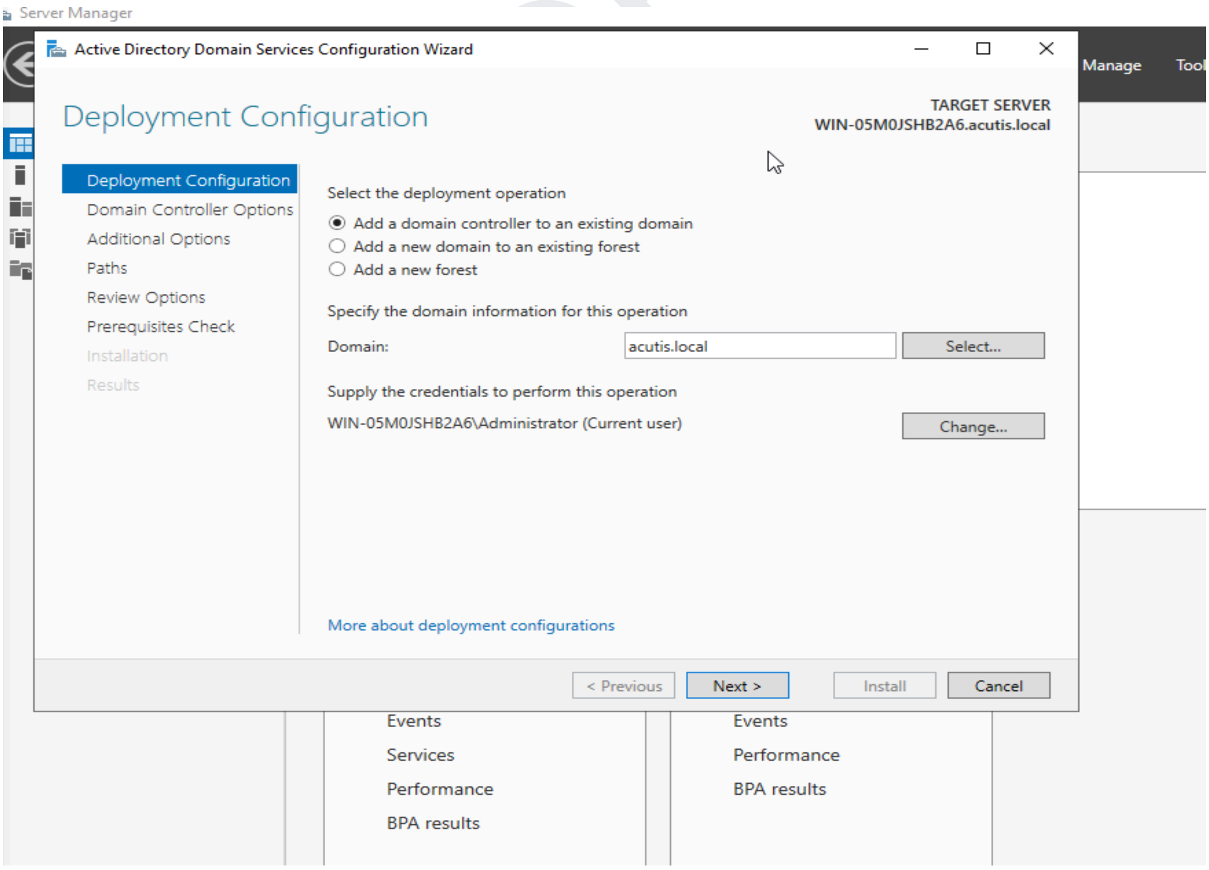
⚠ Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

⚠ This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "acutis.local". Otherwise, no action is required.

More about results



Deployment Configuration

TARGET SERVER
WIN-05M0JSHB2A6.acutis.local

Select the deployment operation

● Add a domain controller to an existing domain
○ Add a new domain to an existing forest
○ Add a new forest

Specify the domain information for this operation

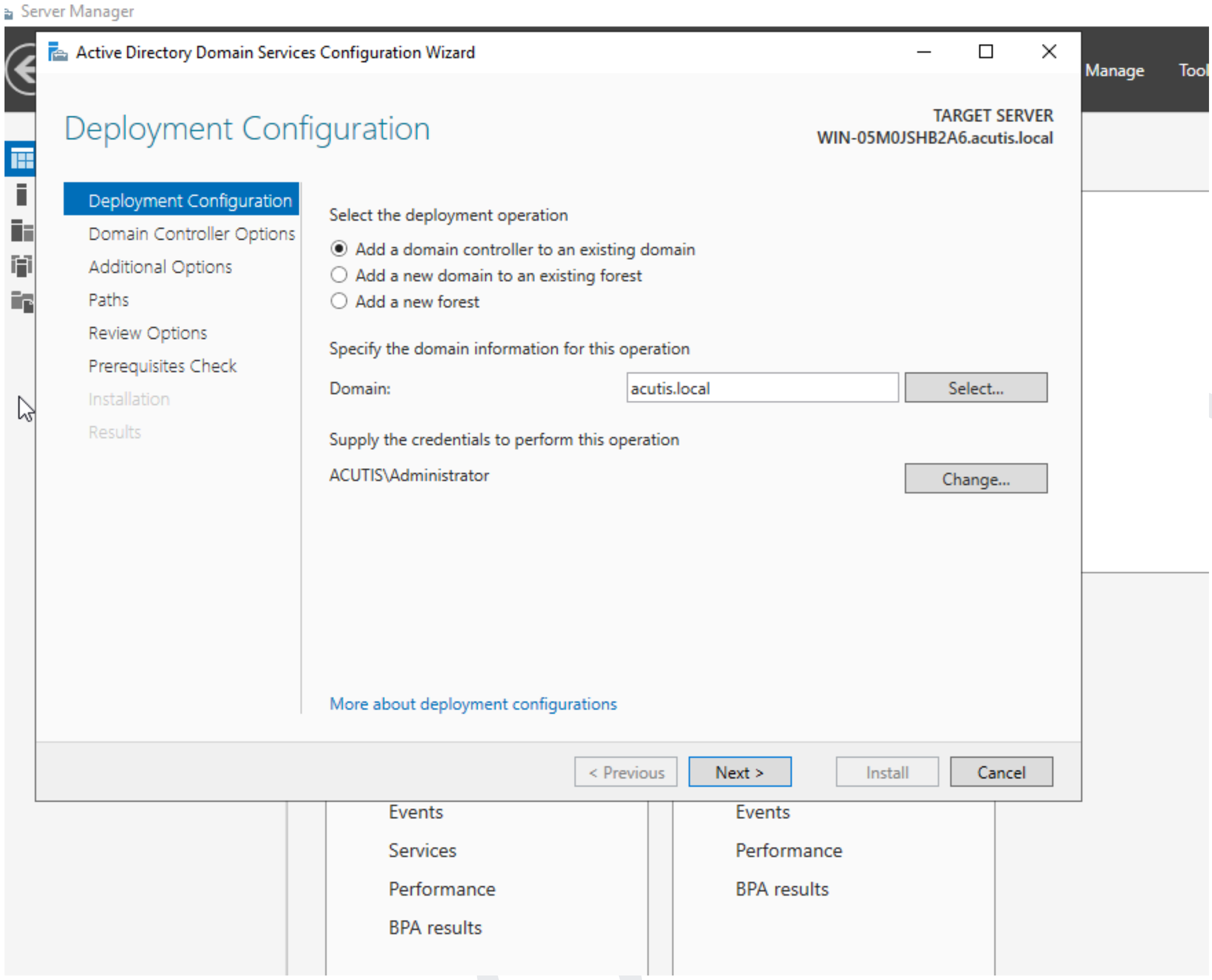
Domain: acutis.local

Supply the credentials to perform this operation

WIN-05M0JSHB2A6\Administrator (Current user)

More about deployment configurations

5.2 Add a Domain Controller to the Existing Forest



Deployment Configuration

TARGET SERVER
WIN-05M0JSHB2A6.acutis.local

Select the deployment operation

● Add a domain controller to an existing domain
○ Add a new domain to an existing forest
○ Add a new forest

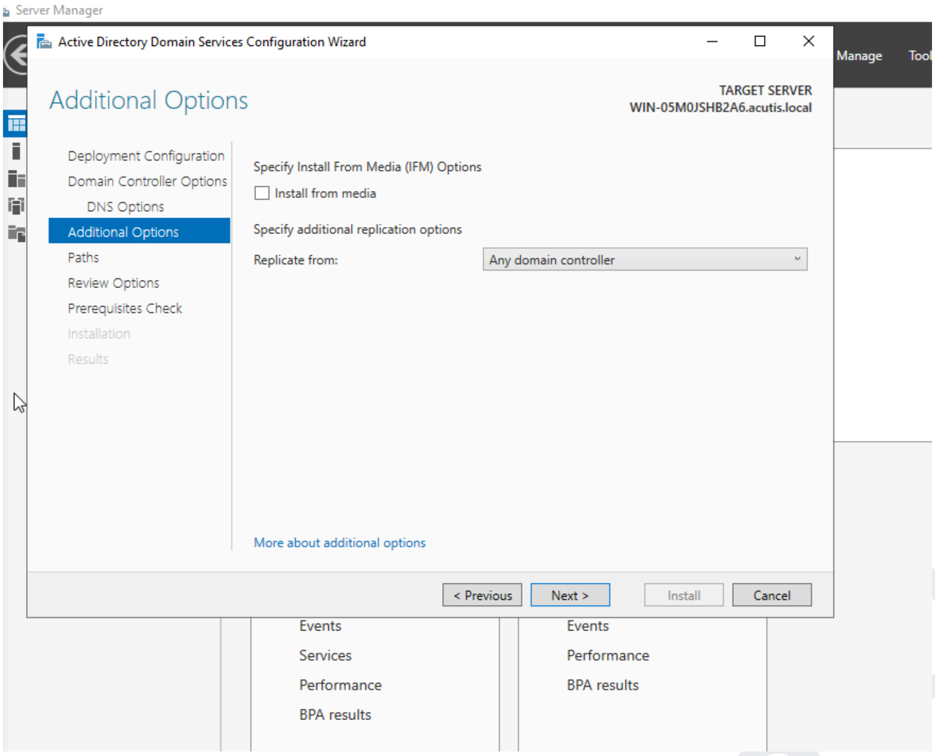
Specify the domain information for this operation

Domain: acutis.local [Select...]

Supply the credentials to perform this operation

ACUTIS\Administrator [Change...]

More about deployment configurations



Additional Options

TARGET SERVER
WIN-05M0JSHB2A6.acutis.local

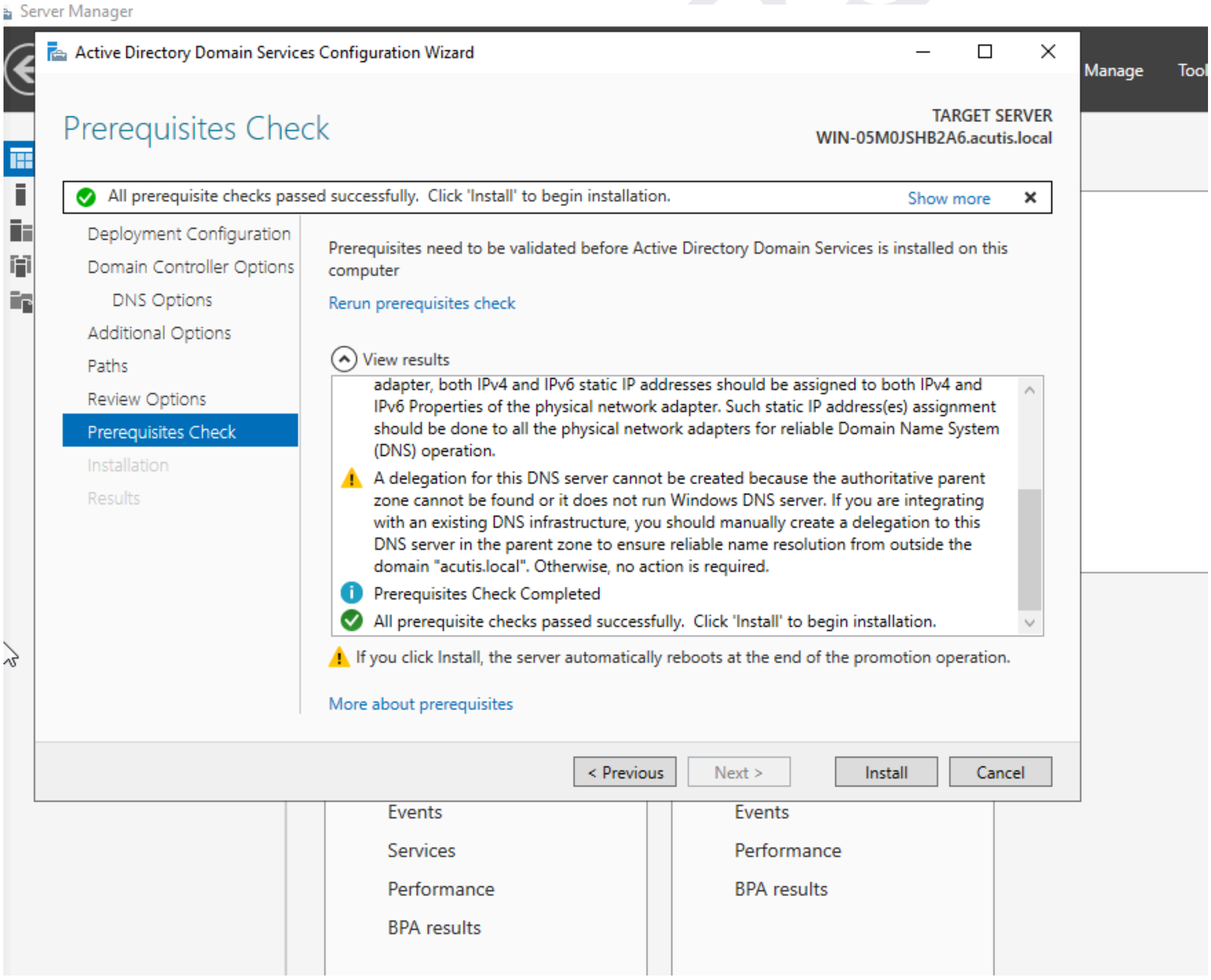
Specify Install From Media (IFM) Options

□ Install from media

Specify additional replication options

Replicate from: Any domain controller

More about additional options



Prerequisites Check

TARGET SERVER
WIN-05M0JSHB2A6.acutis.local

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation. Show more ✕

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Rerun prerequisites check

View results

adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

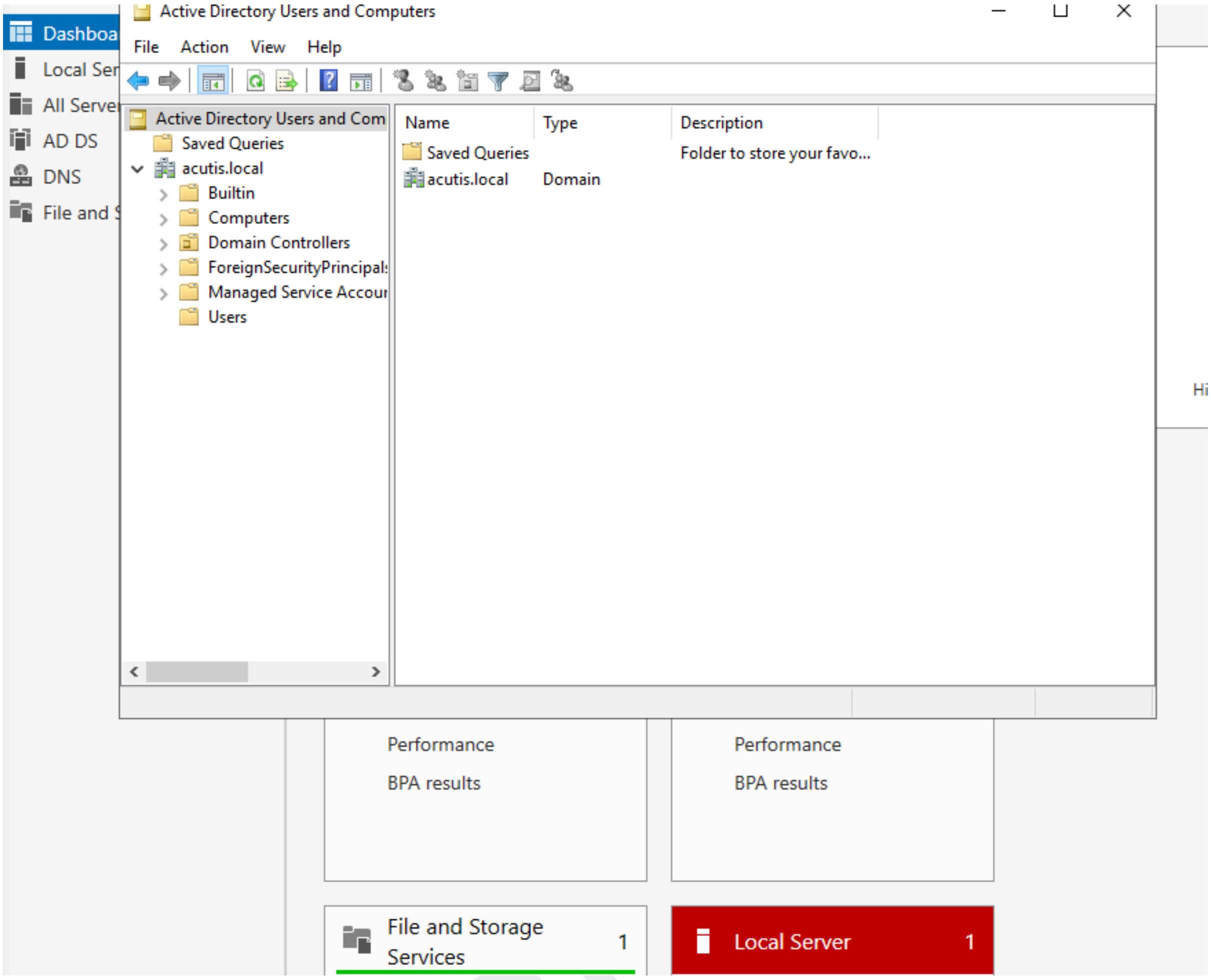
⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "acutis.local". Otherwise, no action is required.

ℹ Prerequisites Check Completed

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation.

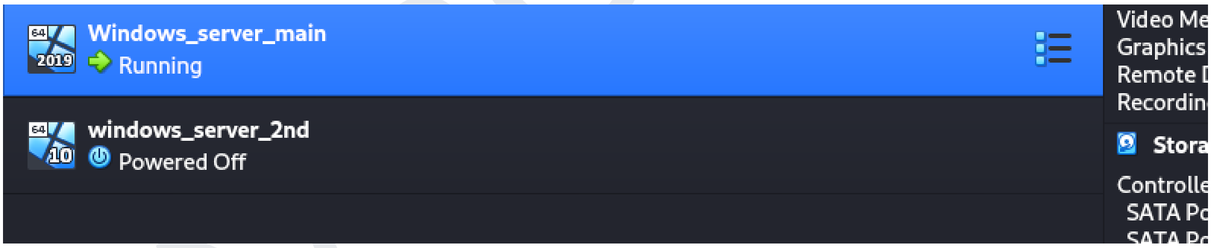
⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

More about prerequisites



Name	Type	Description
Saved Queries		Folder to store your favo...
acutis.local	Domain	

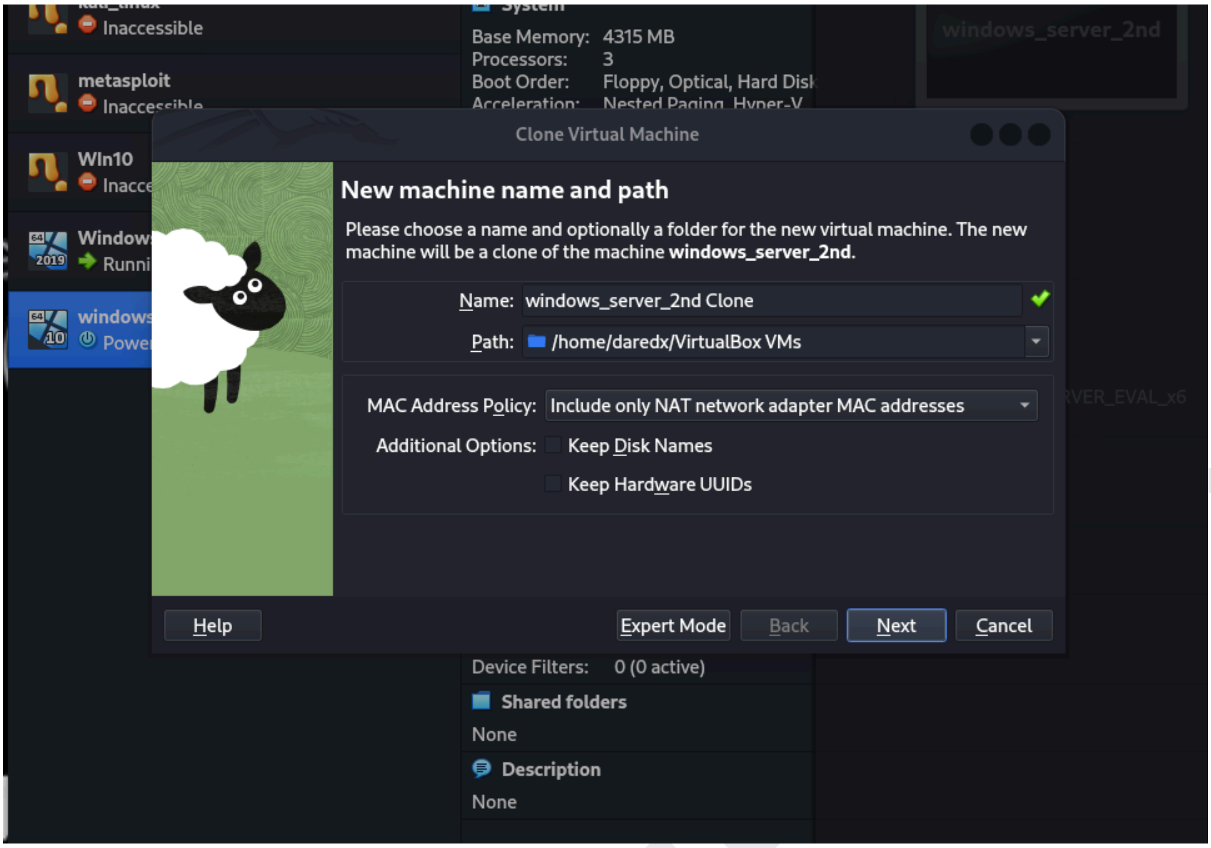
Two system is running in the VM:



5.3 Explore Domain Controller Installation Options

1. **DC cloning:**

VM is cloned and Domain is configured to achieve DC cloning



Clone Virtual Machine

New machine name and path

Please choose a name and optionally a folder for the new virtual machine. The new machine will be a clone of the machine **windows_server_2nd**.

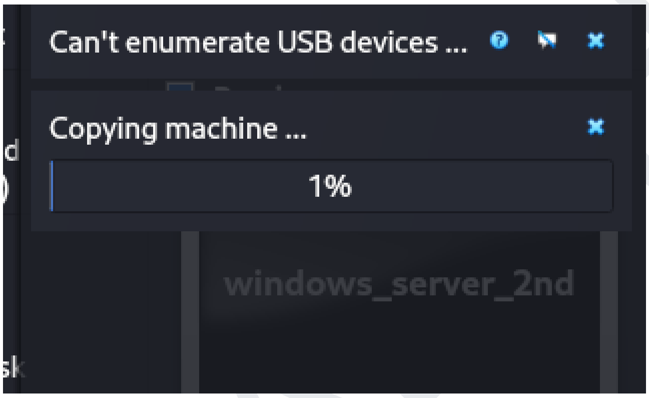
Name: windows_server_2nd Clone

Path: /home/daredx/VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: □ Keep Disk Names

□ Keep Hardware UUIDs

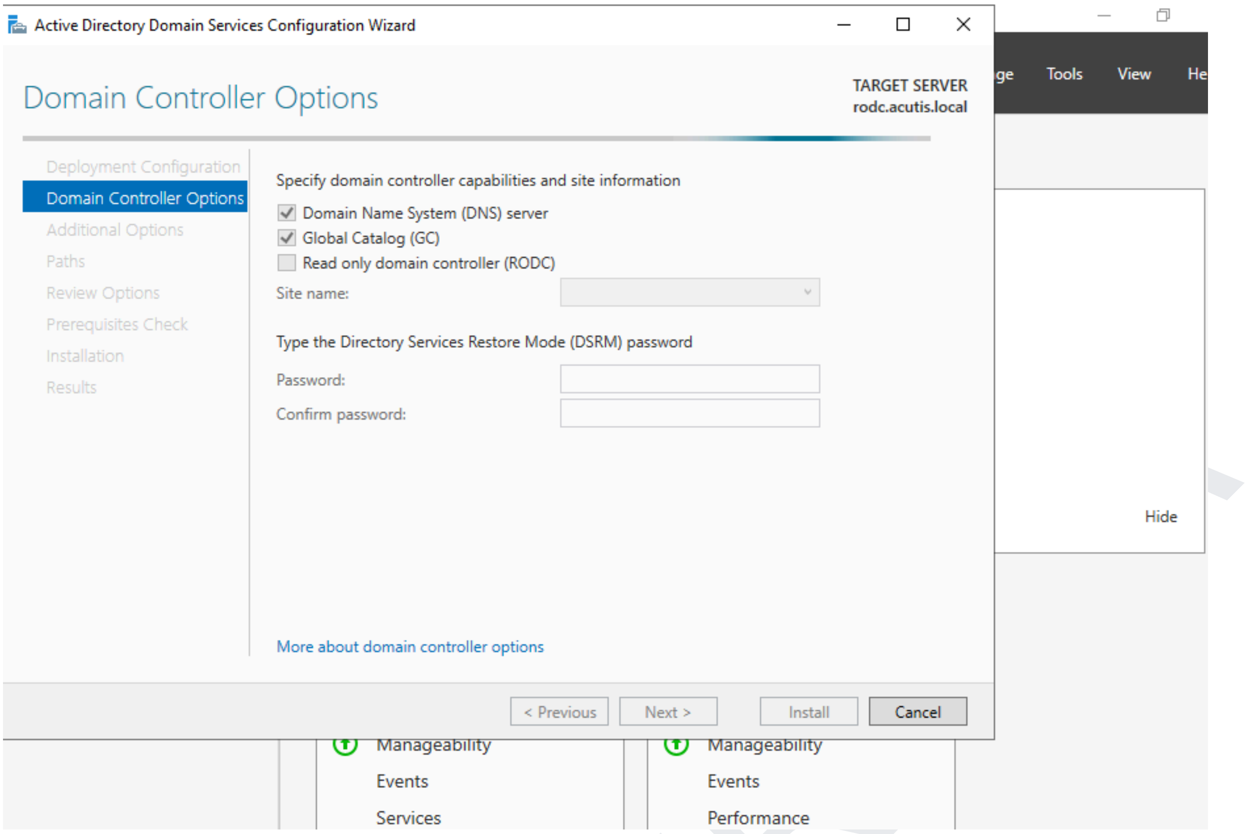


Can't enumerate USB devices ...

Copying machine ...

1%

2. **Read-Only Domain Controllers (RODC)**:
   a. Set up a third server and promote it to an RODC.
   b. During promotion, choose **Read-only domain controller (RODC)** in the wizard.



Domain Controller Options

Specify domain controller capabilities and site information

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

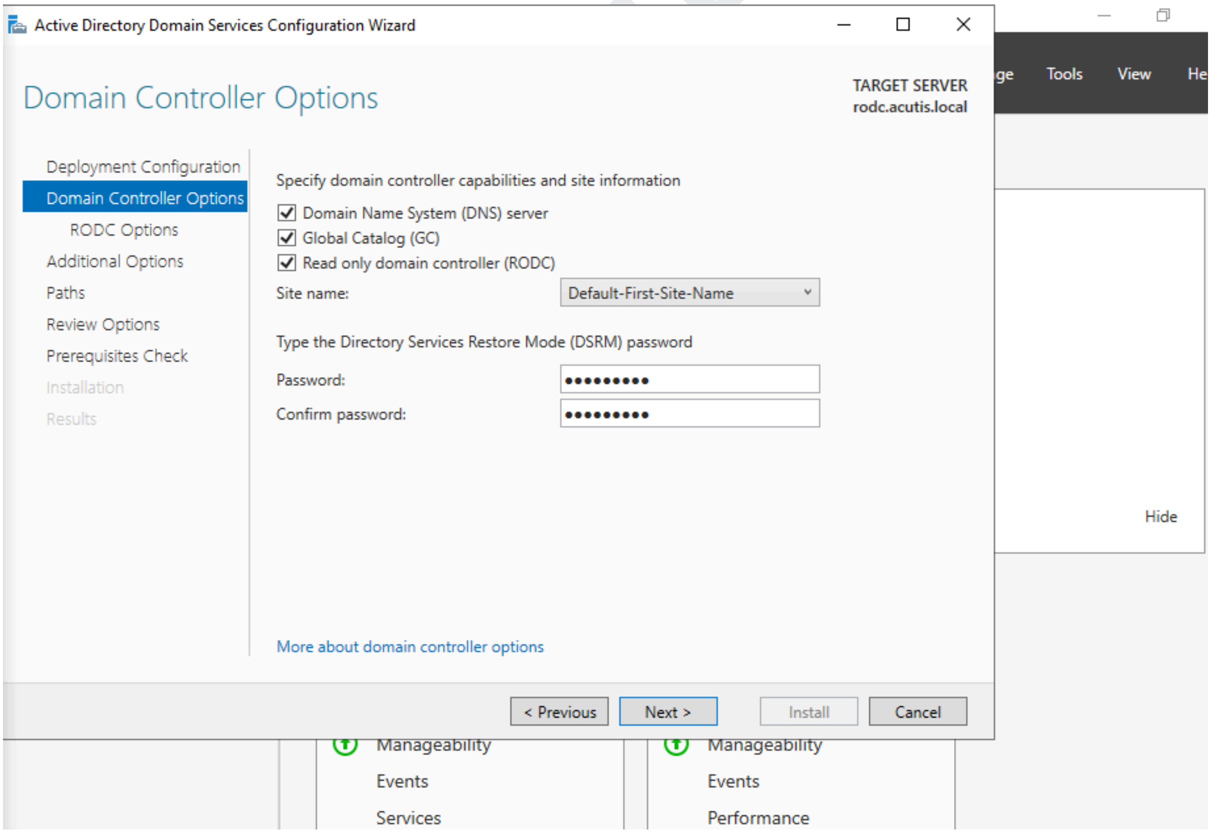
□ Read only domain controller (RODC)

Site name:

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:



Domain Controller Options

Specify domain controller capabilities and site information

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

☑ Read only domain controller (RODC)

Site name: Default-First-Site-Name

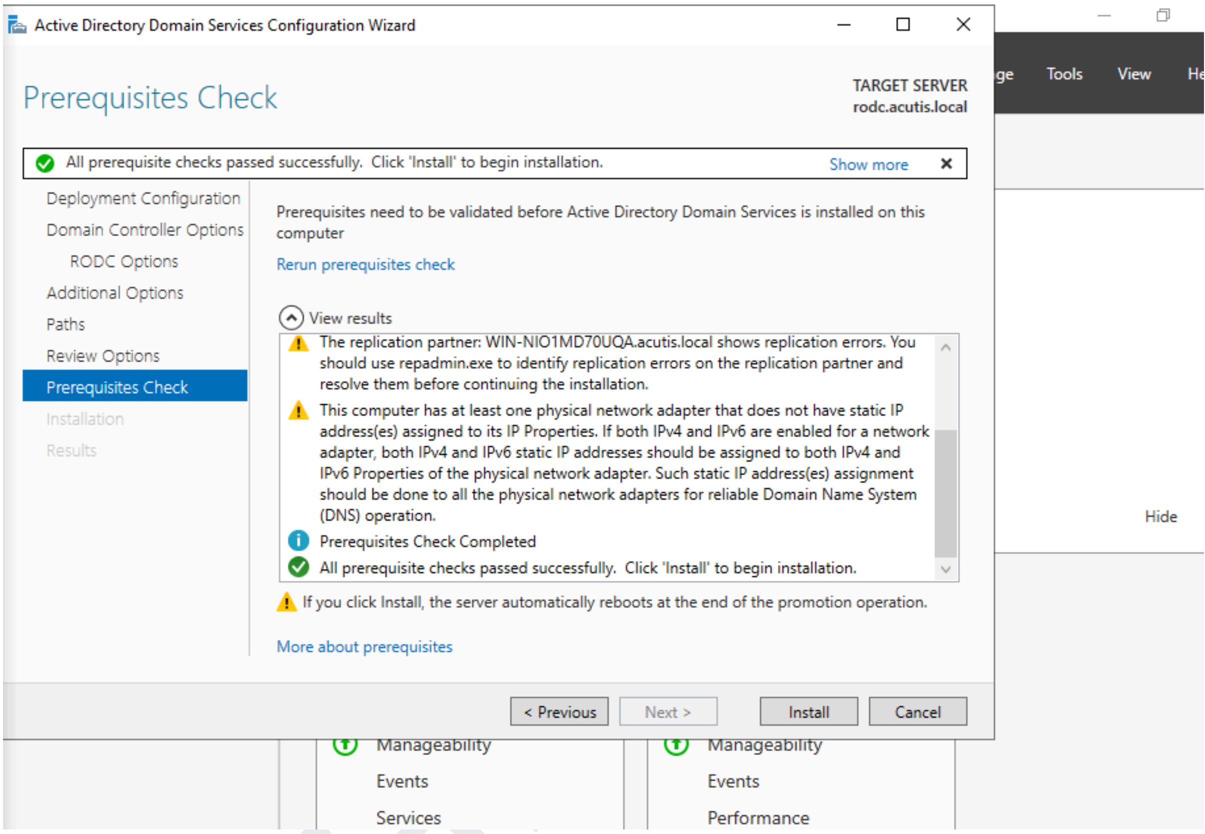
Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

5.4 Configure Security Policies

1. **Account Security and Password Settings:**
   - **Use the Active Directory Administrative Center to create Password Settings Objects (PSOs).**
   - **Apply PSOs to specific users or groups.**



Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
rodc.acutis.local

All prerequisite checks passed successfully. Click 'Install' to begin installation. Show more

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Rerun prerequisites check

View results

The replication partner: WIN-NIO1MD70UQA.acutis.local shows replication errors. You should use repadmin.exe to identify replication errors on the replication partner and resolve them before continuing the installation.

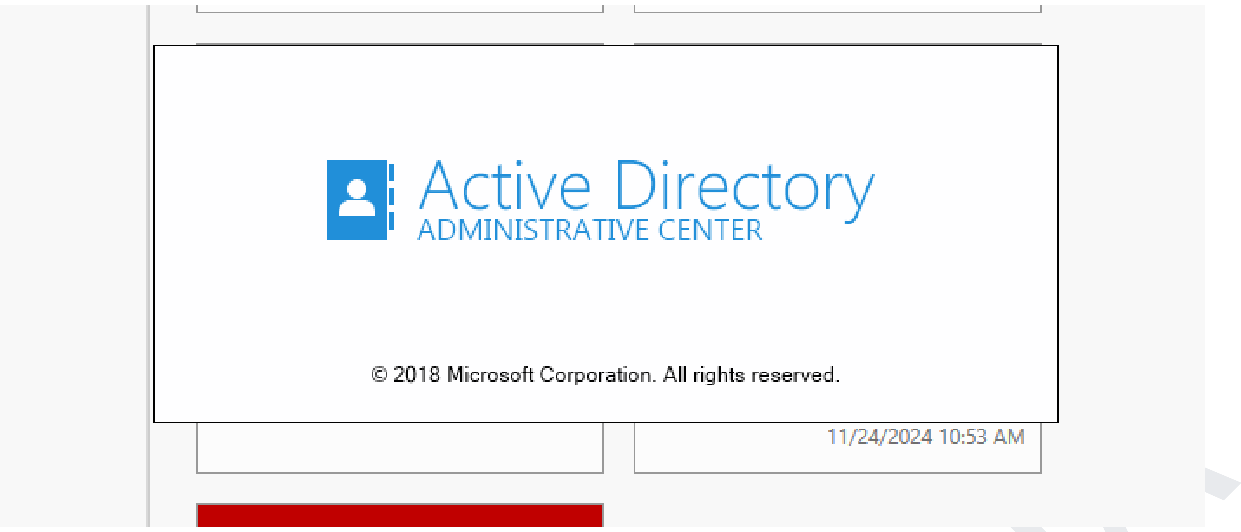
This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

Prerequisites Check Completed

All prerequisite checks passed successfully. Click 'Install' to begin installation.

If you click Install, the server automatically reboots at the end of the promotion operation.

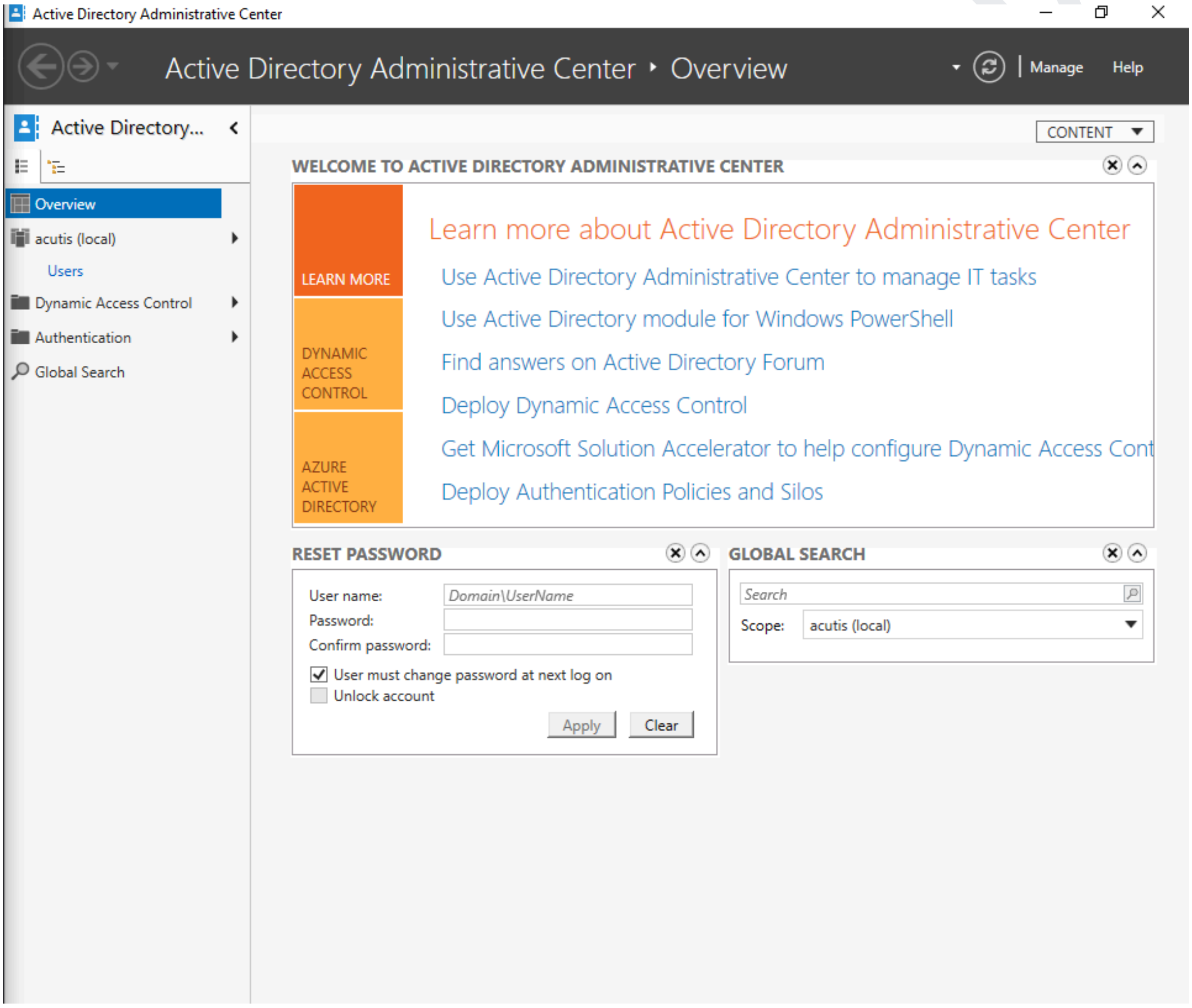
More about prerequisites



Active Directory
ADMINISTRATIVE CENTER

© 2018 Microsoft Corporation. All rights reserved.

11/24/2024 10:53 AM



WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER

Learn more about Active Directory Administrative Center

Use Active Directory Administrative Center to manage IT tasks

Use Active Directory module for Windows PowerShell

Find answers on Active Directory Forum

Deploy Dynamic Access Control

Get Microsoft Solution Accelerator to help configure Dynamic Access Cont

Deploy Authentication Policies and Silos

RESET PASSWORD

User name: Domain\UserName

Password:

Confirm password:

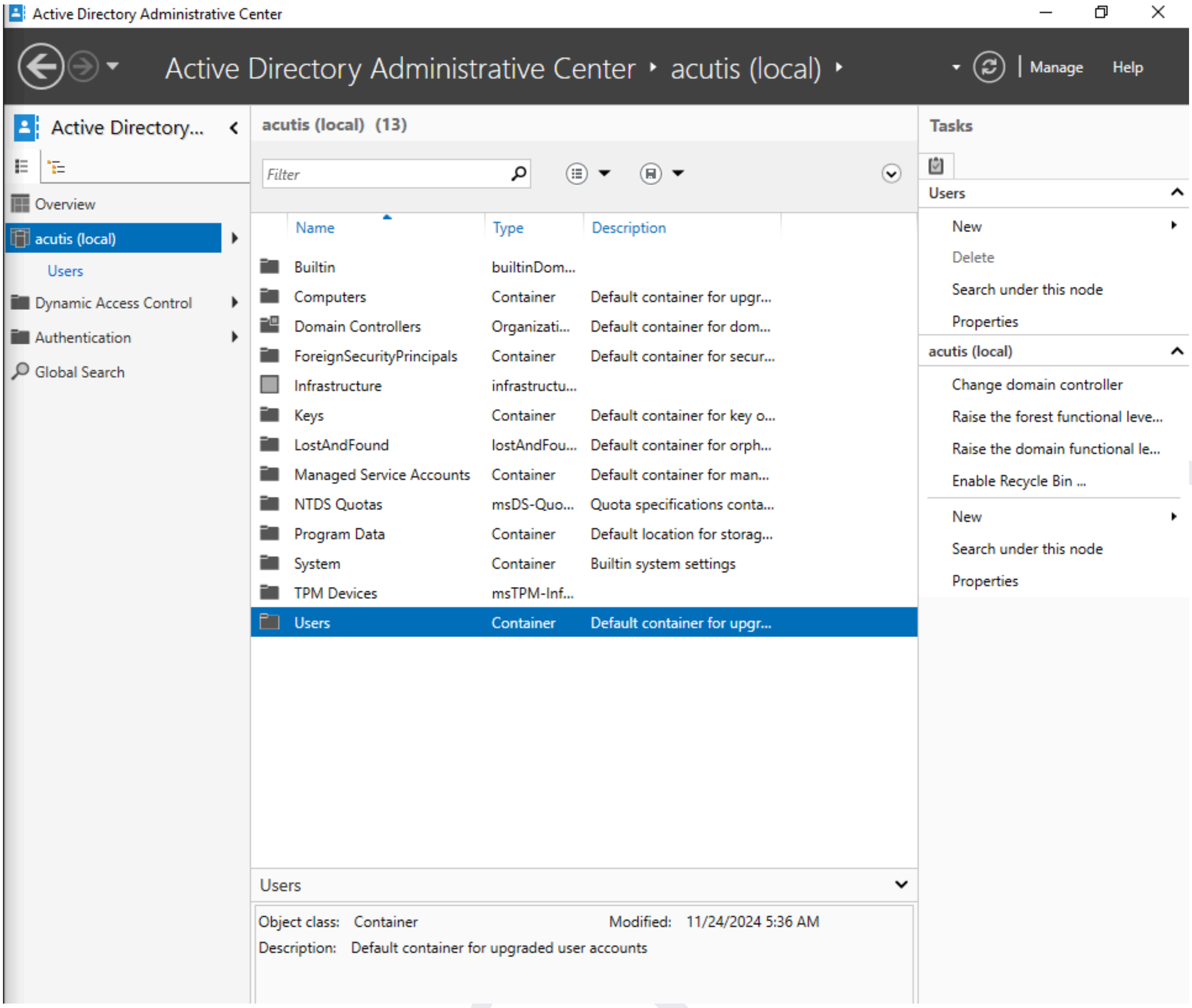
☑ User must change password at next log on

□ Unlock account

GLOBAL SEARCH

Search

Scope: acutis (local)



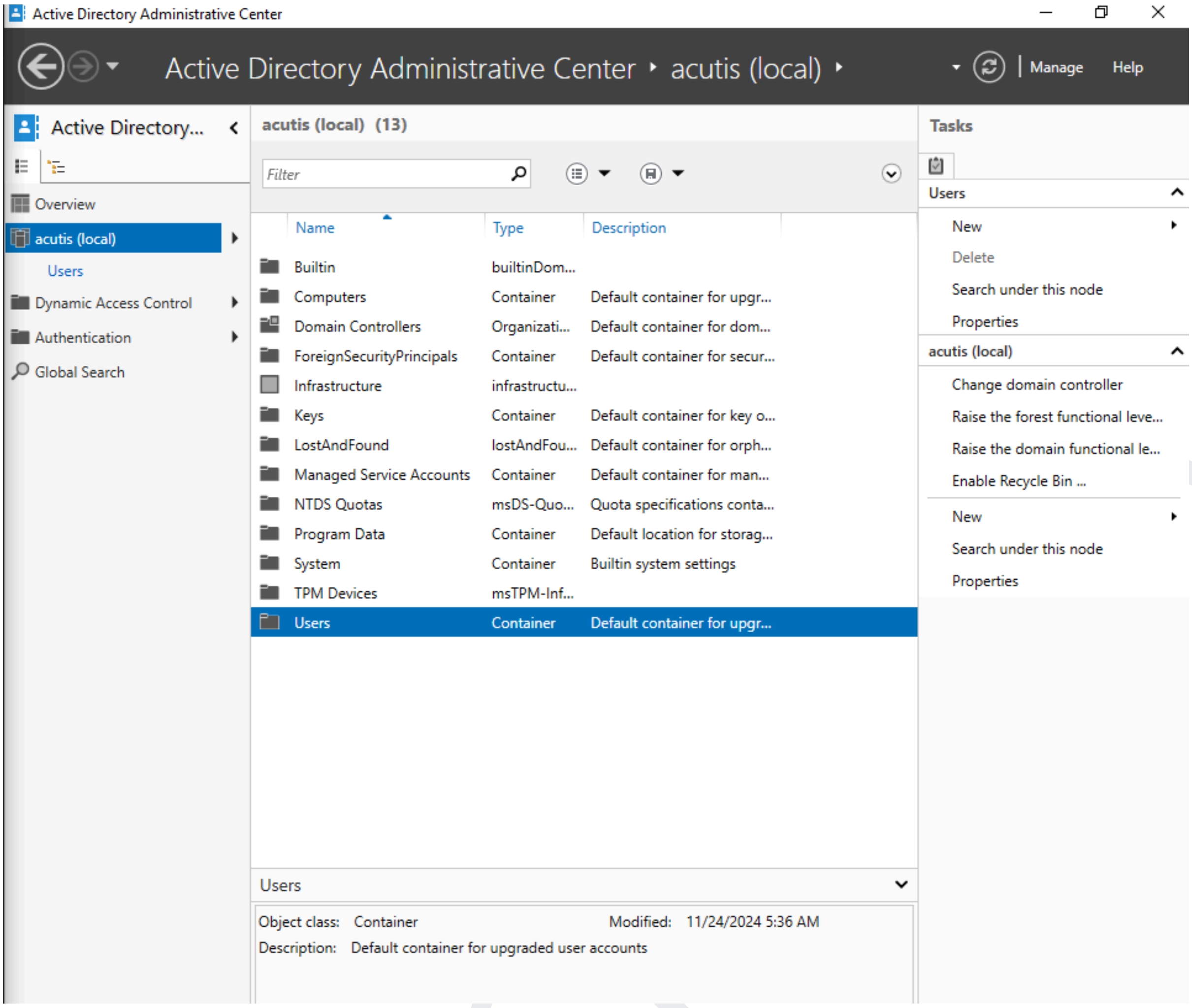
acutis (local) (13)

Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructu...	
Keys	Container	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
TPM Devices	msTPM-Inf...	
Users	Container	Default container for upgr...

Users

Object class: Container   Modified: 11/24/2024 5:36 AM

Description: Default container for upgraded user accounts



acutis (local) (13)

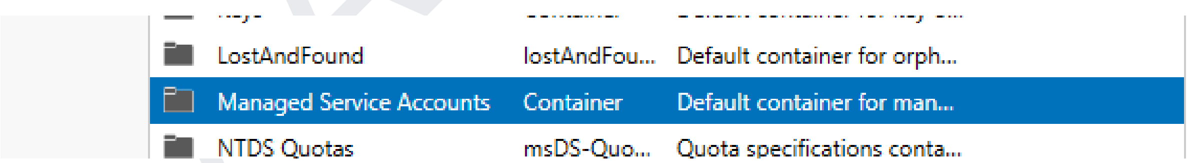
Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructu...	
Keys	Container	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
TPM Devices	msTPM-Inf...	
Users	Container	Default container for upgr...

Users

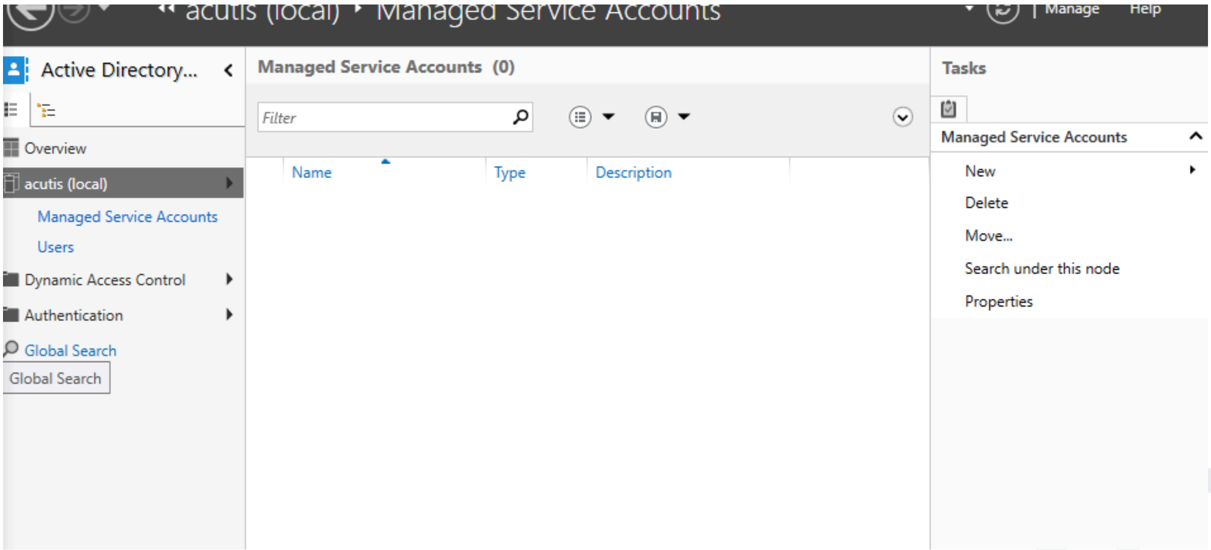
Object class: Container Modified: 11/24/2024 5:36 AM

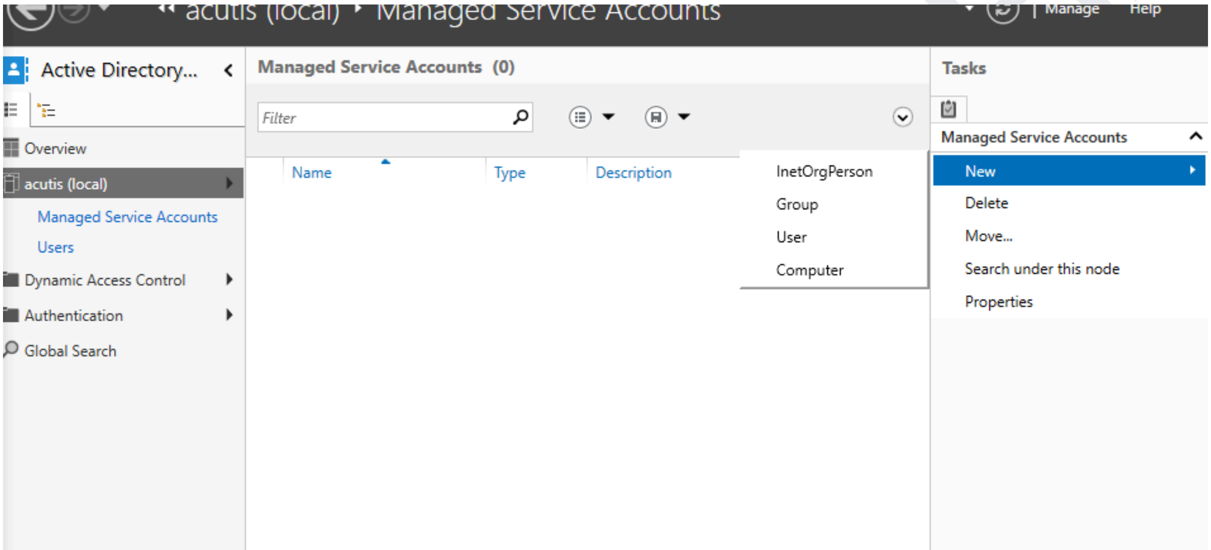
Description: Default container for upgraded user accounts

a. **Managed Service Accounts (MSAs)**:



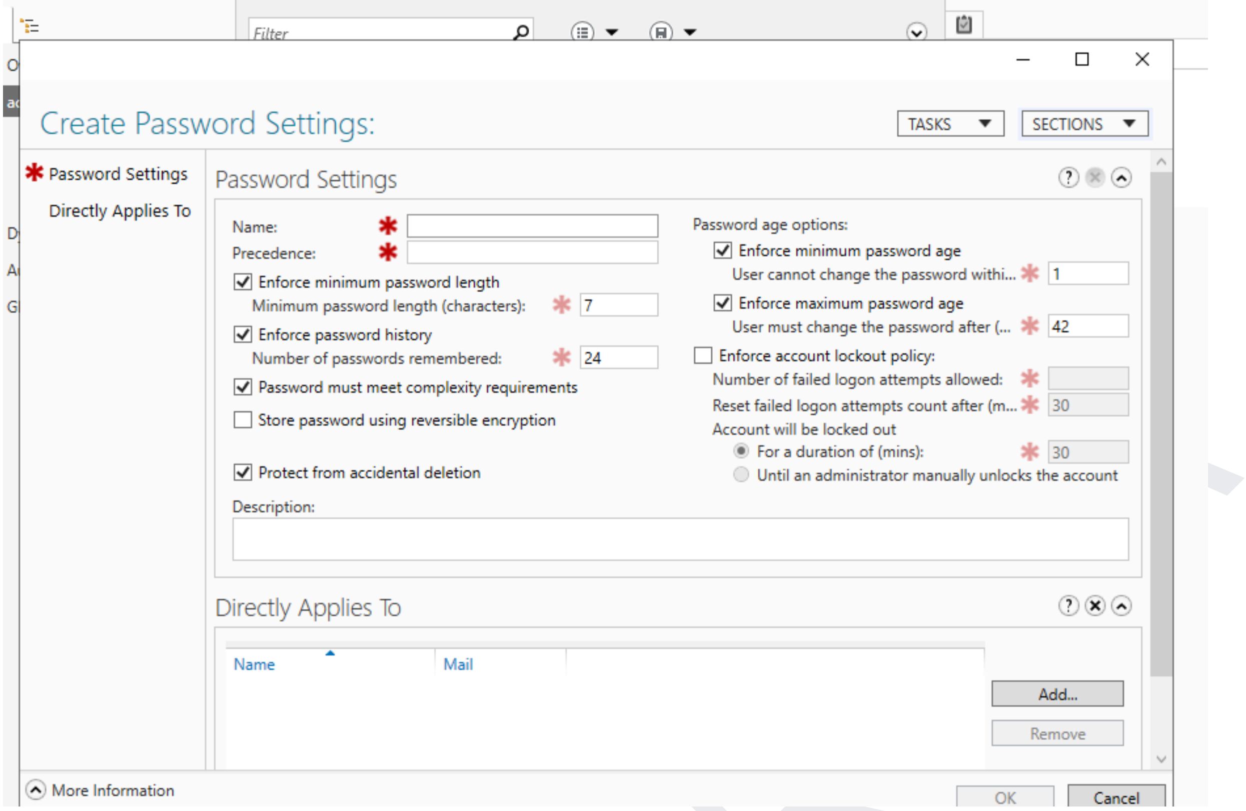
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...





Create a New PSO:

- Right-click **Password Settings Container** > **New** > **Password Settings**.
- Configure the following:
  - **Name**: Provide a name for the PSO (e.g., `STRICT_PASSWORD_POLICY`).
  - **Precedence**: Lower numbers take priority if a user is linked to multiple PSOs.
  - **Password Complexity**: Enforce strong passwords.
  - **Maximum/Minimum Password Age**: Define how long passwords are valid.
  - **Minimum Password Length**: Set the minimum length for passwords.
  - **Lockout Threshold and Duration**: Configure account lockout settings.



Create Password Settings:

Password Settings

Directly Applies To

Password Settings

Name: *	
Precedence: *	
☑ Enforce minimum password length	
Minimum password length (characters): *	7
☑ Enforce password history	
Number of passwords remembered: *	24
☑ Password must meet complexity requirements	
□ Store password using reversible encryption	
☑ Protect from accidental deletion	

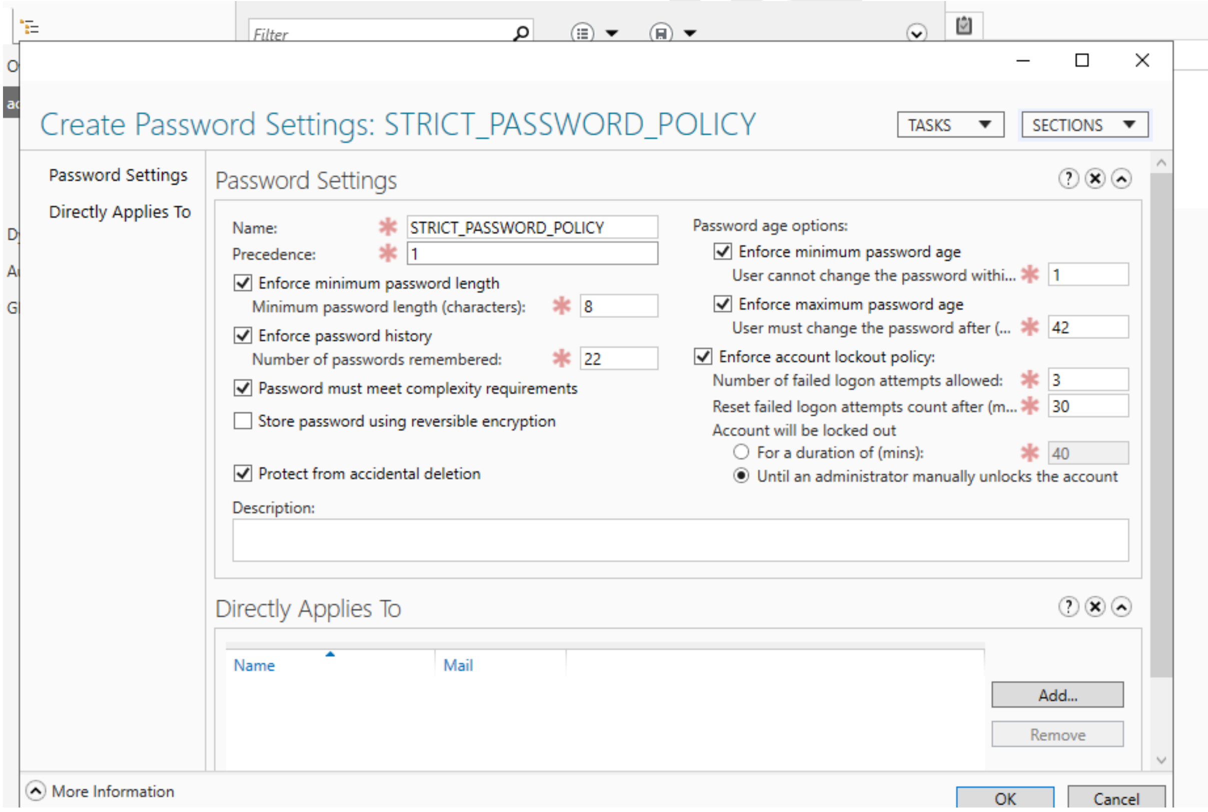
Password age options:

☑ Enforce minimum password age	
User cannot change the password withi... *	1
☑ Enforce maximum password age	
User must change the password after (... *	42
□ Enforce account lockout policy:	
Number of failed logon attempts allowed: *	
Reset failed logon attempts count after (m... *	30
Account will be locked out	
● For a duration of (mins): *	30
○ Until an administrator manually unlocks the account	

Description:

Directly Applies To

Name	Mail



Create Password Settings: STRICT_PASSWORD_POLICY

Password Settings

Directly Applies To

Password Settings

Name: *	STRICT_PASSWORD_POLICY
Precedence: *	1
☑ Enforce minimum password length	
Minimum password length (characters): *	8
☑ Enforce password history	
Number of passwords remembered: *	22
☑ Password must meet complexity requirements	
□ Store password using reversible encryption	
☑ Protect from accidental deletion	

Password age options:

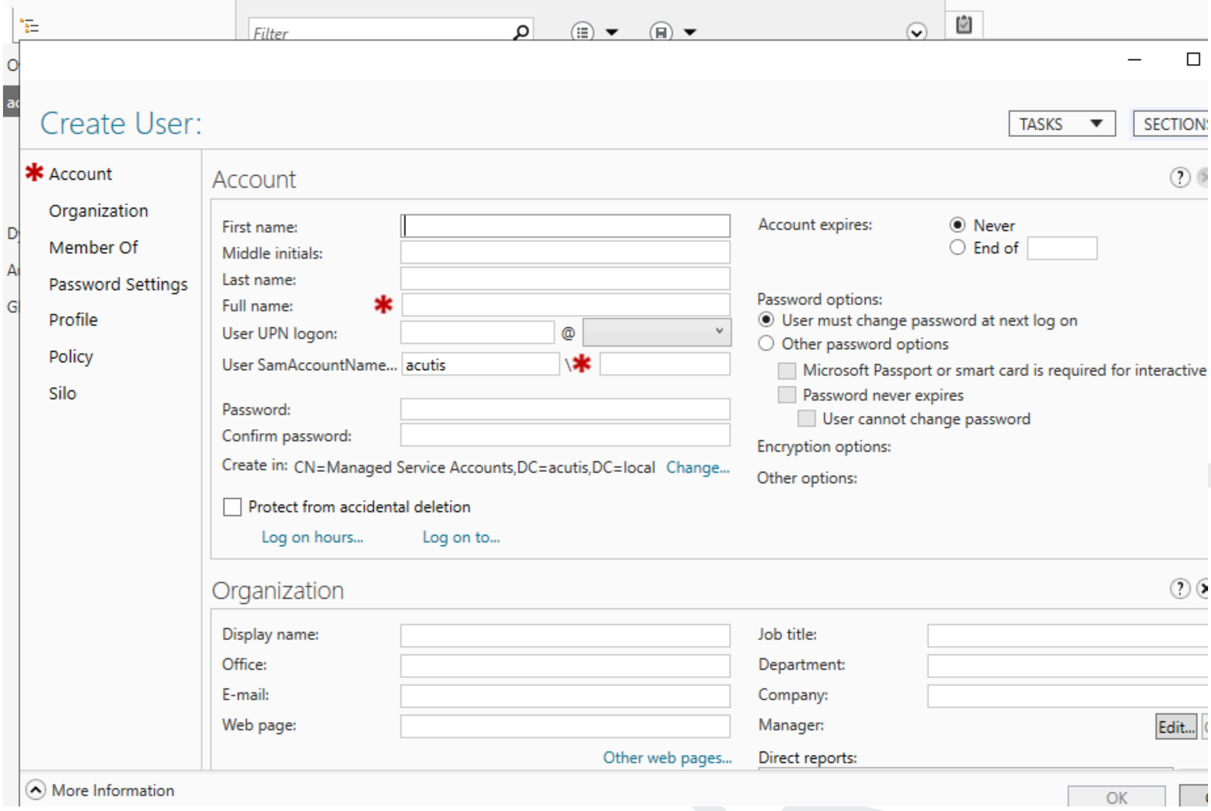
☑ Enforce minimum password age	
User cannot change the password withi... *	1
☑ Enforce maximum password age	
User must change the password after (... *	42
☑ Enforce account lockout policy:	
Number of failed logon attempts allowed: *	3
Reset failed logon attempts count after (m... *	30
Account will be locked out	
○ For a duration of (mins): *	40
● Until an administrator manually unlocks the account	

Description:

Directly Applies To

Name	Mail

Apply the PSO to Users or Groups:



Account

First name:
Middle initials:
Last name:
Full name:
User UPN logon: @
User SamAccountName... acutis \
Password:
Confirm password:
Create in: CN=Managed Service Accounts,DC=acutis,DC=local Change...

□ Protect from accidental deletion

Log on hours... Log on to...

Account expires: ● Never ○ End of

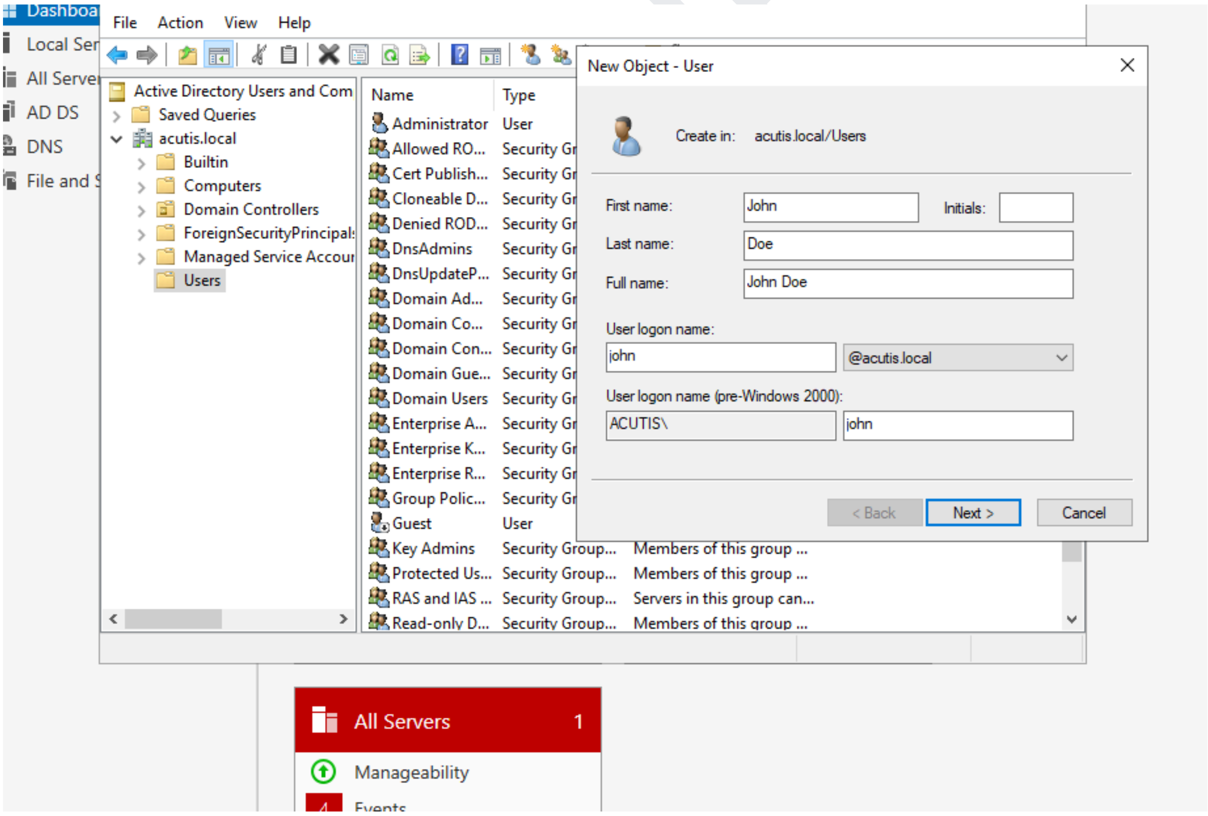
Password options:
● User must change password at next log on
○ Other password options
□ Microsoft Passport or smart card is required for interactive
□ Password never expires
□ User cannot change password

Encryption options:

Other options:

Organization

Display name:
Office:
E-mail:
Web page:
Other web pages...
Job title:
Department:
Company:
Manager: Edit...
Direct reports:



Active Directory Users and Com
- Saved Queries
- acutis.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Users

Name	Type	
Administrator	User	
Allowed RO...	Security Gr	
Cert Publish...	Security Gr	
Cloneable D...	Security Gr	
Denied ROD...	Security Gr	
DnsAdmins	Security Gr	
DnsUpdateP...	Security Gr	
Domain Ad...	Security Gr	
Domain Co...	Security Gr	
Domain Con...	Security Gr	
Domain Gue...	Security Gr	
Domain Users	Security Gr	
Enterprise A...	Security Gr	
Enterprise K...	Security Gr	
Enterprise R...	Security Gr	
Group Polic...	Security Gr	
Guest	User	
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...

New Object - User

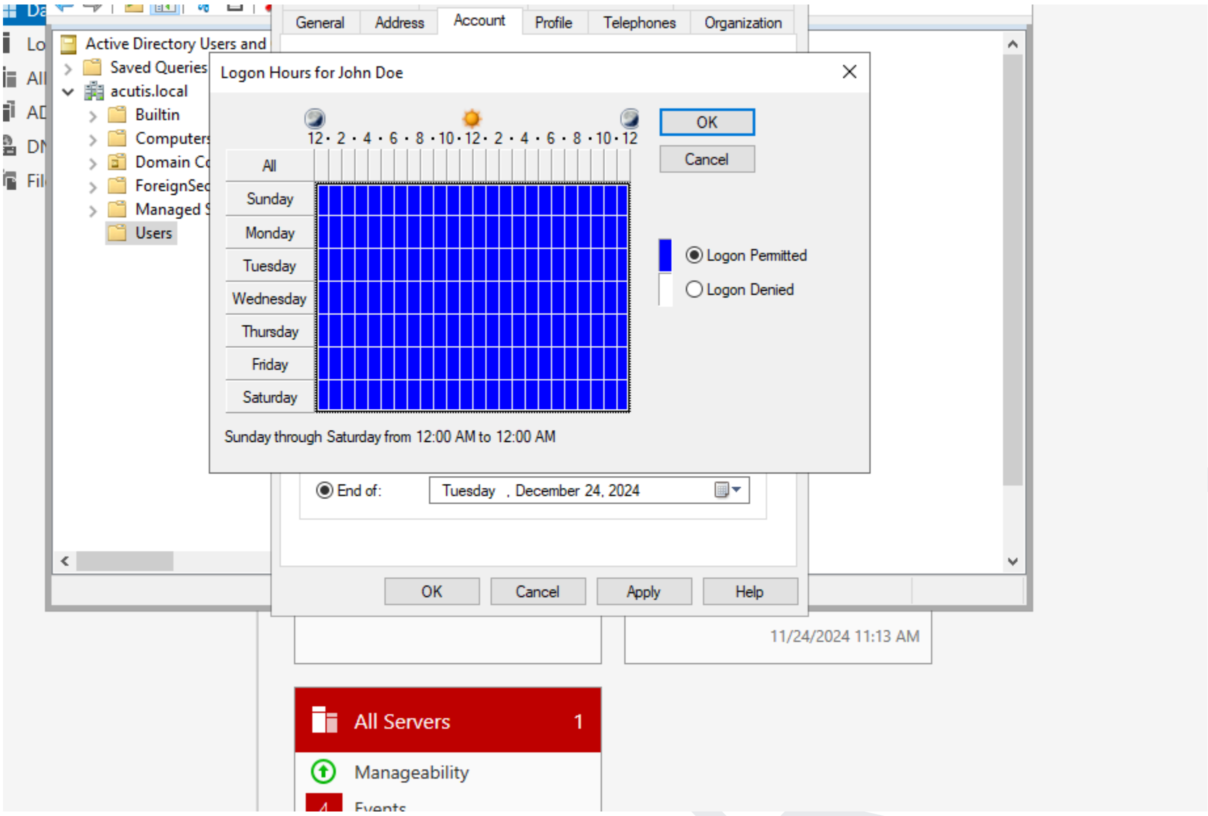
Create in: acutis.local/Users

First name: John Initials:
Last name: Doe
Full name: John Doe

User logon name:
john @acutis.local

User logon name (pre-Windows 2000):
ACUTIS\ john

We can add multiple policies for users and groups



Logon Hours for John Doe

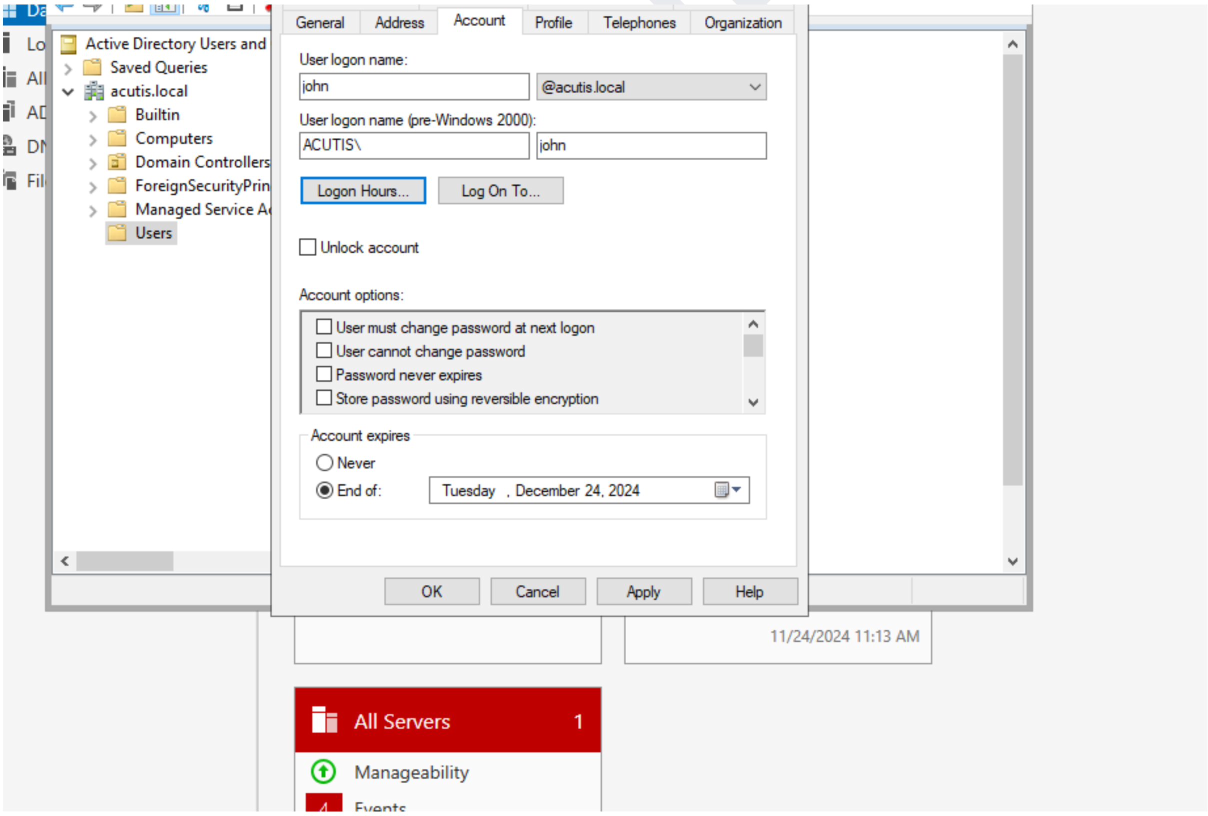
● Logon Permitted

○ Logon Denied

Sunday through Saturday from 12:00 AM to 12:00 AM

● End of: Tuesday , December 24, 2024

11/24/2024 11:13 AM



User logon name:

john @acutis.local

User logon name (pre-Windows 2000):

ACUTIS\ john

□ Unlock account

Account options:

□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Store password using reversible encryption

Account expires

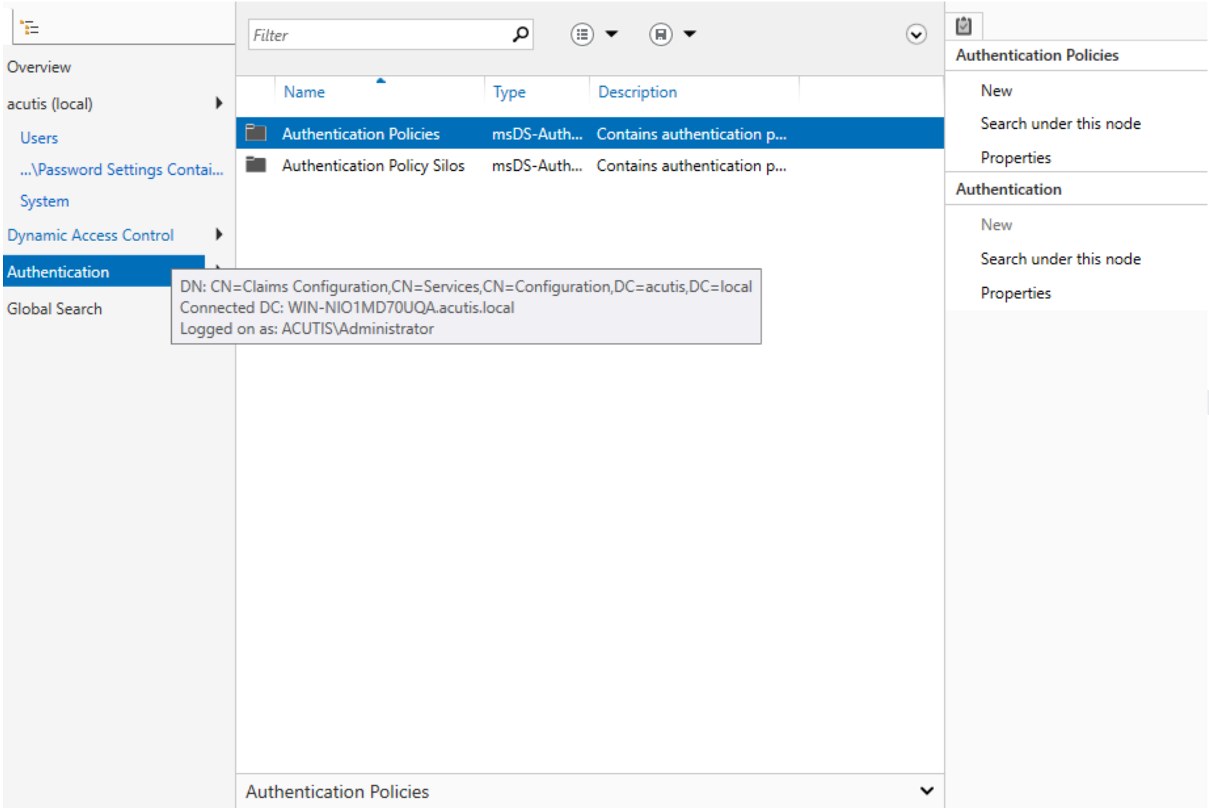
○ Never

● End of: Tuesday , December 24, 2024

11/24/2024 11:13 AM

a. **Configure Authentication Policies and Silos:**

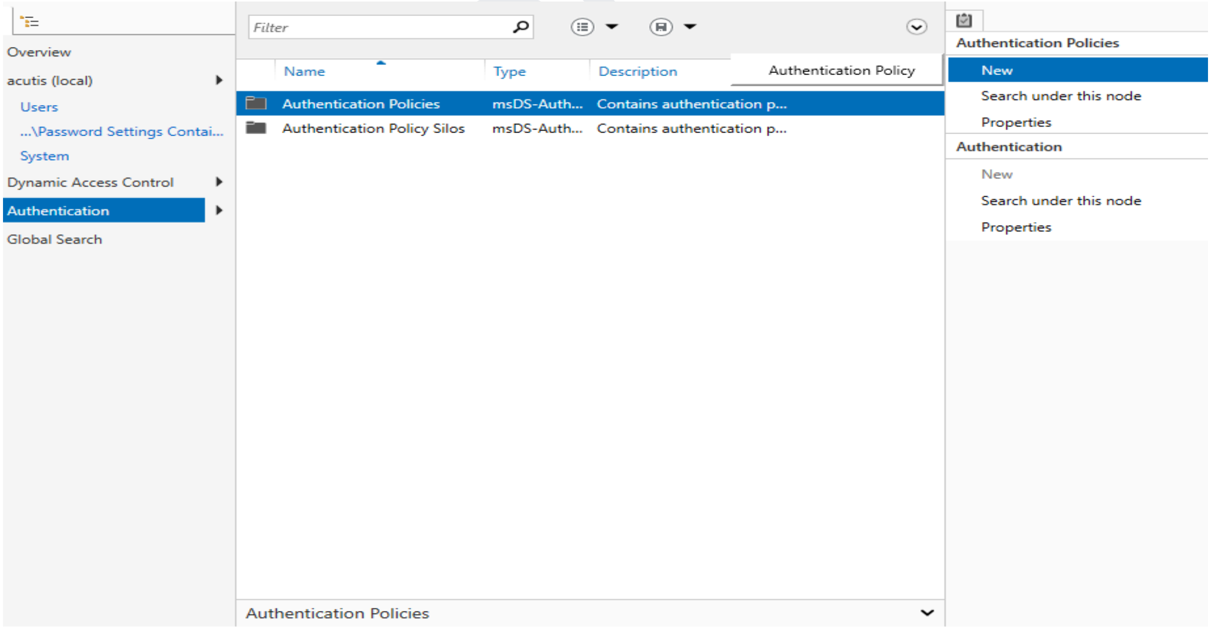
- Restrict access to sensitive accounts and ensure secure authentication processes.



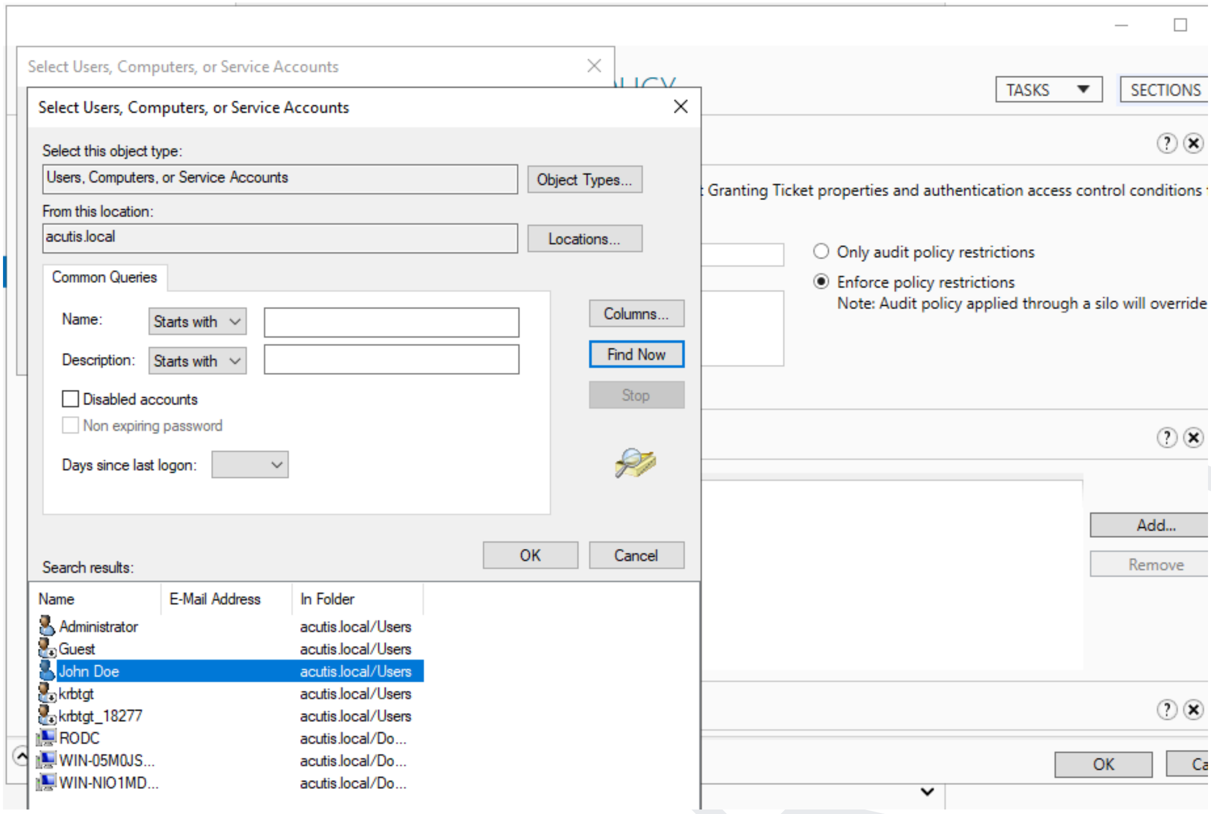
Name	Type	Description
Authentication Policies	msDS-Auth...	Contains authentication p...
Authentication Policy Silos	msDS-Auth...	Contains authentication p...

DN: CN=Claims Configuration,CN=Services,CN=Configuration,DC=acutis,DC=local
Connected DC: WIN-NIO1MD70UQA.acutis.local
Logged on as: ACUTIS\Administrator

Create an Authentication Policy Silo



Name	Type	Description
Authentication Policies	msDS-Auth...	Contains authentication p...
Authentication Policy Silos	msDS-Auth...	Contains authentication p...



Select Users, Computers, or Service Accounts

Select this object type:
Users, Computers, or Service Accounts

From this location:
acutis.local

Common Queries

Name: Starts with
Description: Starts with
□ Disabled accounts
□ Non expiring password
Days since last logon:

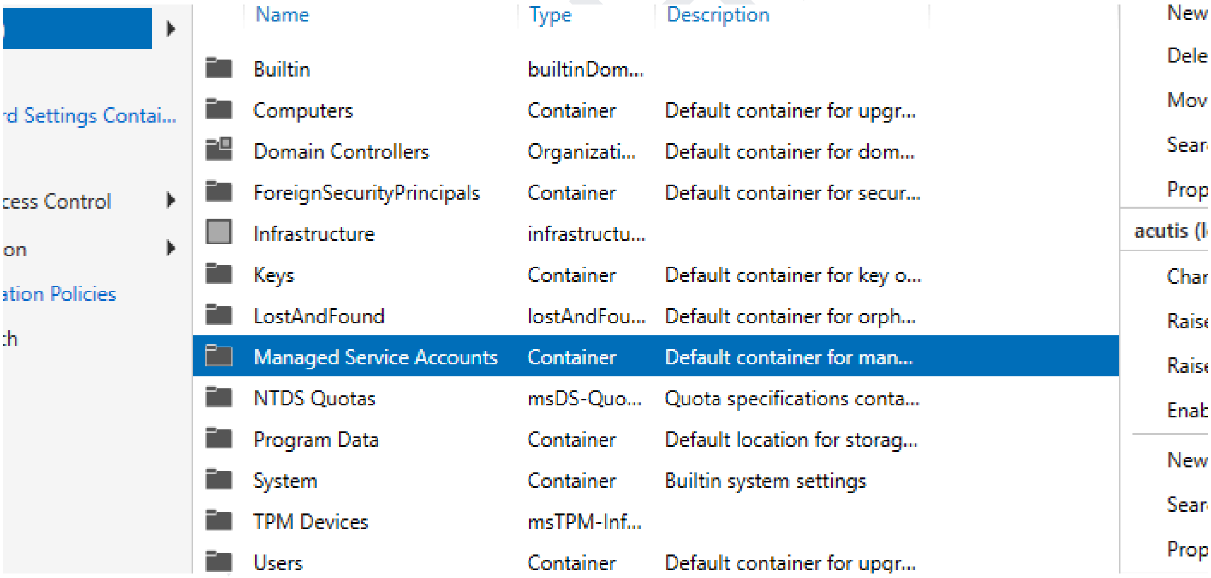
Granting Ticket properties and authentication access control conditions

○ Only audit policy restrictions
● Enforce policy restrictions
Note: Audit policy applied through a silo will override

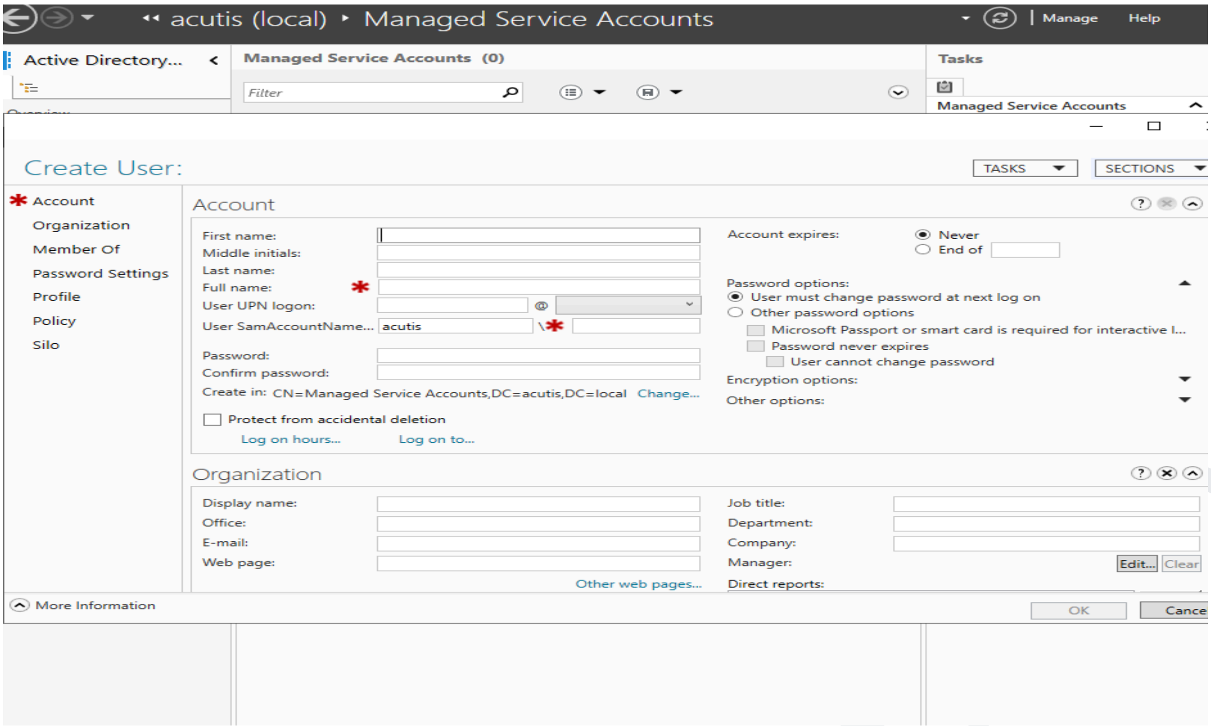
Search results:

Name	E-Mail Address	In Folder
Administrator		acutis.local/Users
Guest		acutis.local/Users
John Doe		acutis.local/Users
krbtgt		acutis.local/Users
krbtgt_18277		acutis.local/Users
RODC		acutis.local/Do...
WIN-05M0JS...		acutis.local/Do...
WIN-NIO1MD...		acutis.local/Do...

Configure Managed Service Accounts (MSAs)



Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructu...	
Keys	Container	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
TPM Devices	msTPM-Inf...	
Users	Container	Default container for upgr...



acutis (local) ▸ Managed Service Accounts

Managed Service Accounts (0)

Create User:

Account

First name:	
Middle initials:	
Last name:	
Full name: *	
User UPN logon:	@
User SamAccountName...	acutis \ *
Password:	
Confirm password:	

Create in: CN=Managed Service Accounts,DC=acutis,DC=local Change...

□ Protect from accidental deletion

Log on hours... Log on to...

Account expires: ● Never ○ End of

Password options:
● User must change password at next log on
○ Other password options
□ Microsoft Passport or smart card is required for interactive l...
□ Password never expires
□ User cannot change password

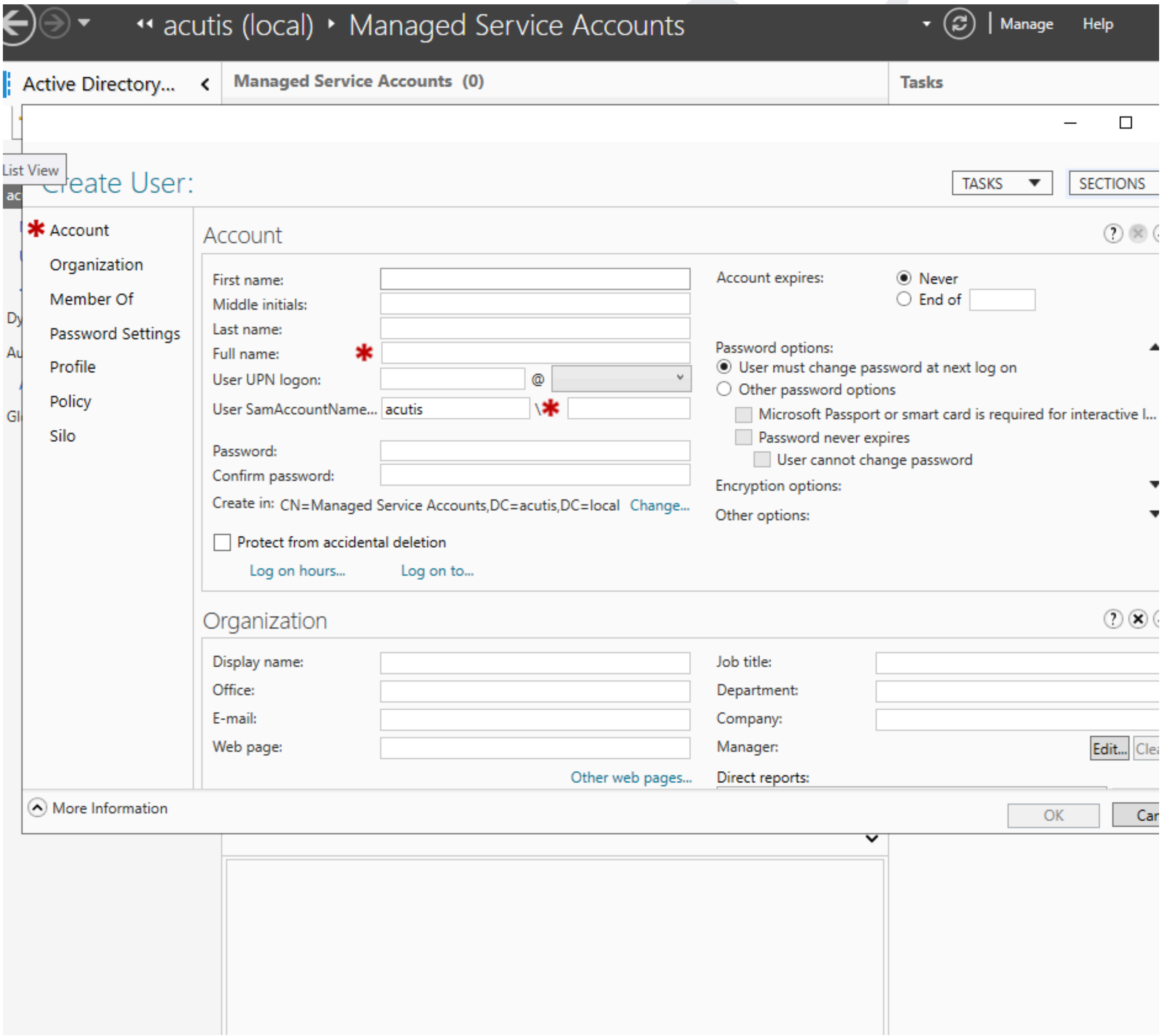
Encryption options:

Other options:

Organization

Display name:		Job title:	
Office:		Department:	
E-mail:		Company:	
Web page:		Manager:	

Other web pages... Direct reports:



acutis (local) ▸ Managed Service Accounts

Managed Service Accounts (0)

Create User:

Account

First name:	
Middle initials:	
Last name:	
Full name: *	
User UPN logon:	@
User SamAccountName...	acutis \ *
Password:	
Confirm password:	

Create in: CN=Managed Service Accounts,DC=acutis,DC=local Change...

□ Protect from accidental deletion

Log on hours... Log on to...

Account expires: ● Never ○ End of

Password options:
● User must change password at next log on
○ Other password options
□ Microsoft Passport or smart card is required for interactive l...
□ Password never expires
□ User cannot change password

Encryption options:

Other options:

Organization

Display name:		Job title:	
Office:		Department:	
E-mail:		Company:	
Web page:		Manager:	

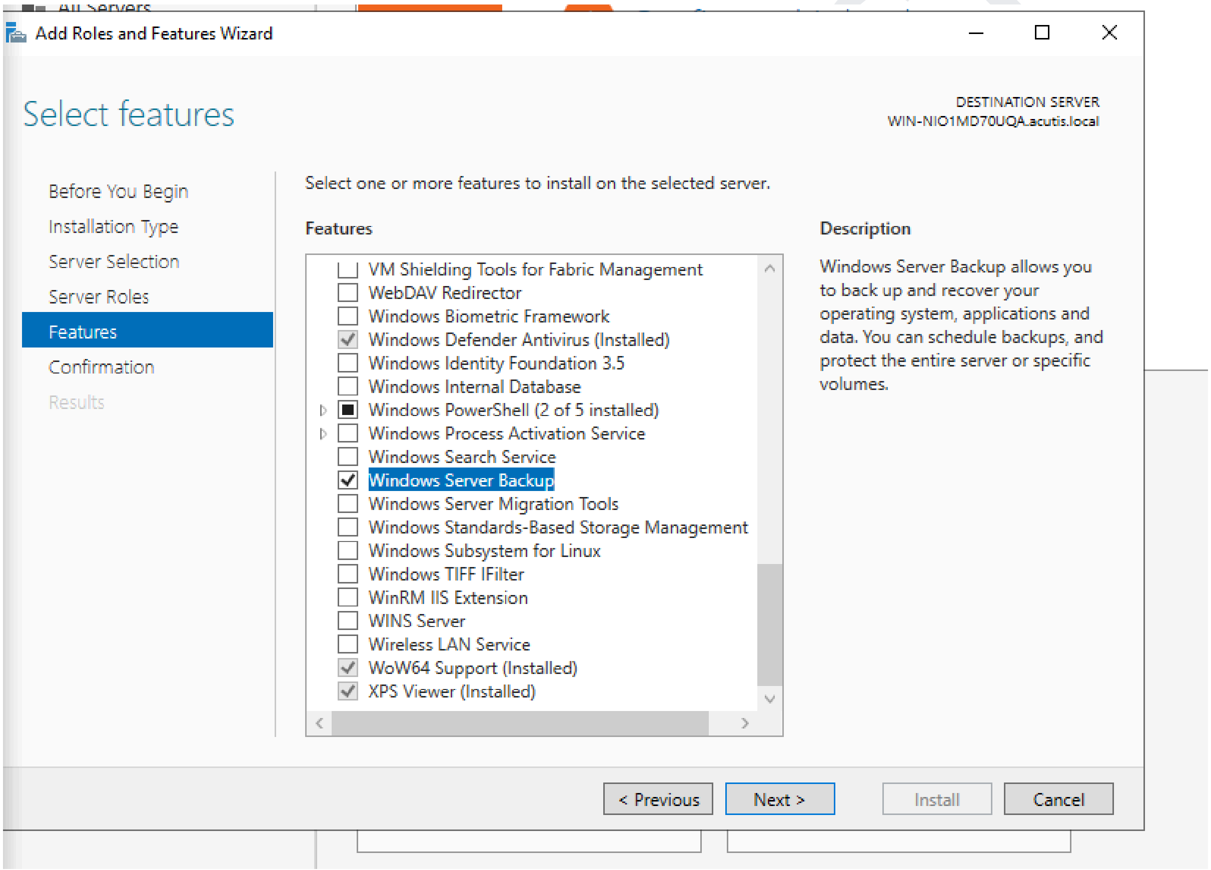
Other web pages... Direct reports:

5.5 Implement Recovery Procedures for Active Directory Domain Services (AD DS)

- Backing up the **system state** is essential for AD DS recovery because it includes critical data such as the Active Directory database, SYSVOL, and the registry.

1. Backup Active Directory Domain Services (System State Backup)

- **Install Windows Server Backup Feature (if not already installed)**:



DESTINATION SERVER
WIN-NIO1MD70UQA.acutis.local

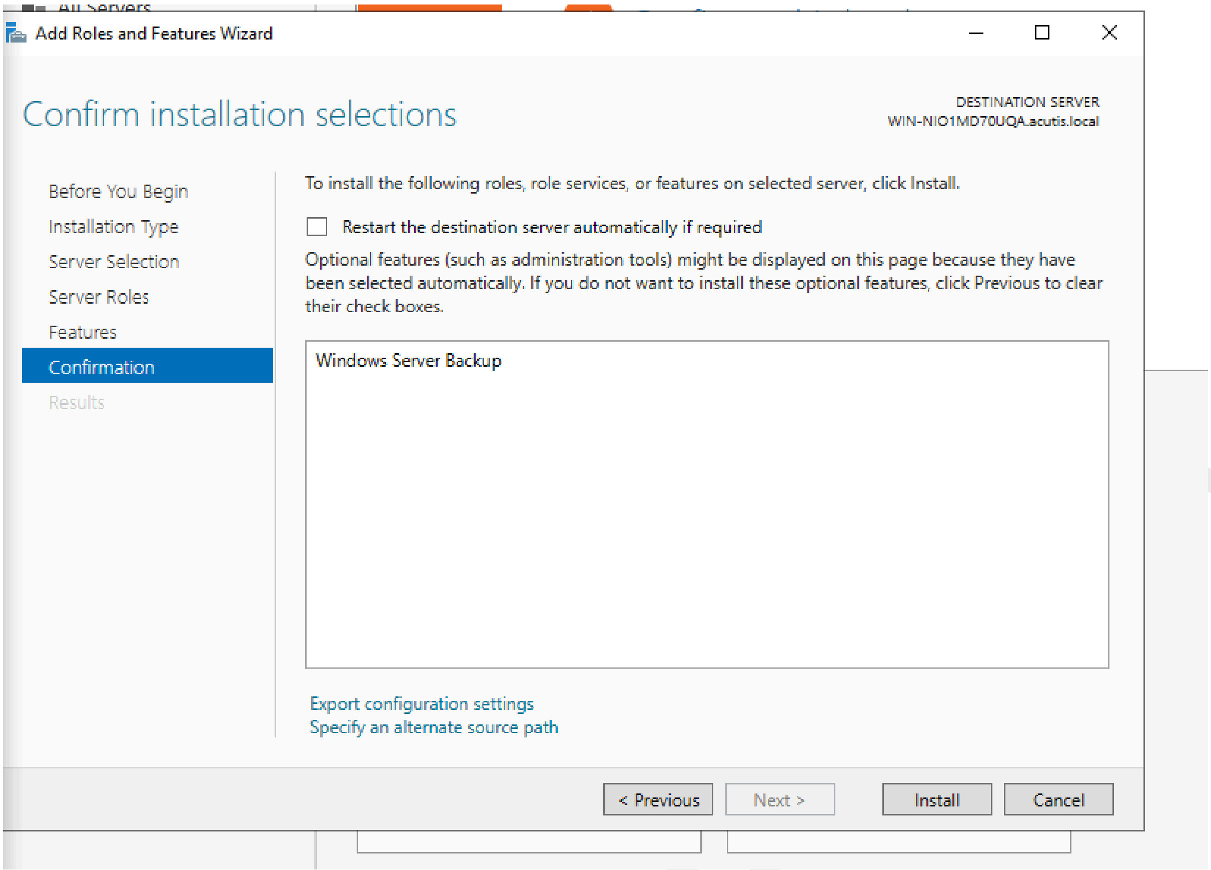
Select one or more features to install on the selected server.

Features

- □ VM Shielding Tools for Fabric Management
- □ WebDAV Redirector
- □ Windows Biometric Framework
- ☑ Windows Defender Antivirus (Installed)
- □ Windows Identity Foundation 3.5
- □ Windows Internal Database
- ■ Windows PowerShell (2 of 5 installed)
- □ Windows Process Activation Service
- □ Windows Search Service
- ☑ Windows Server Backup
- □ Windows Server Migration Tools
- □ Windows Standards-Based Storage Management
- □ Windows Subsystem for Linux
- □ Windows TIFF IFilter
- □ WinRM IIS Extension
- □ WINS Server
- □ Wireless LAN Service
- ☑ WoW64 Support (Installed)
- ☑ XPS Viewer (Installed)

Description

Windows Server Backup allows you to back up and recover your operating system, applications and data. You can schedule backups, and protect the entire server or specific volumes.



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
WIN-NIO1MD70UQA.acutis.local

To install the following roles, role services, or features on selected server, click Install.

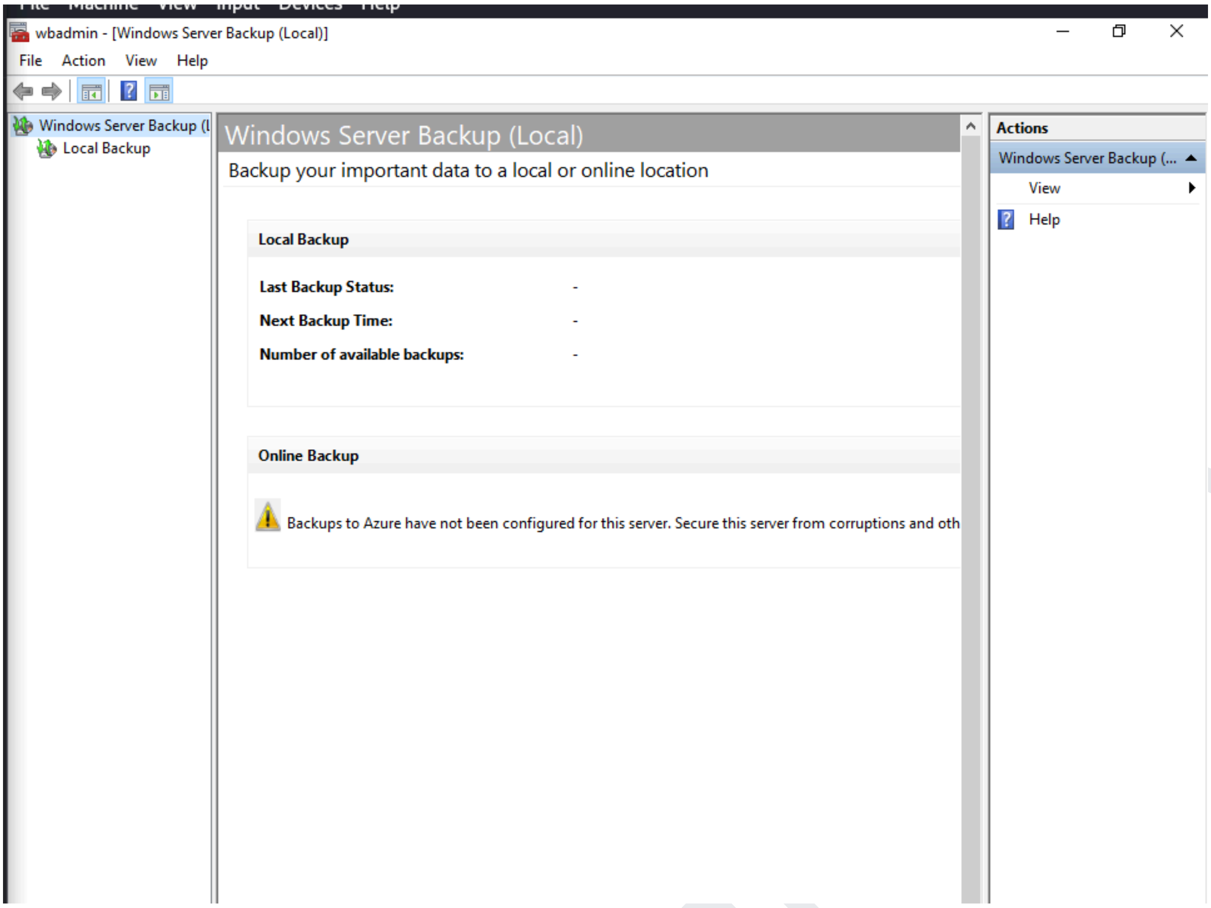
□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Windows Server Backup

Export configuration settings
Specify an alternate source path

2. **Perform the Backup:**


File Machine View Input Devices Help
wbadmin - [Windows Server Backup (Local)]
File Action View Help
Windows Server Backup (L
Local Backup
Actions
Windows Server Backup (...
View
Help

Windows Server Backup (Local)

Backup your important data to a local or online location

Local Backup

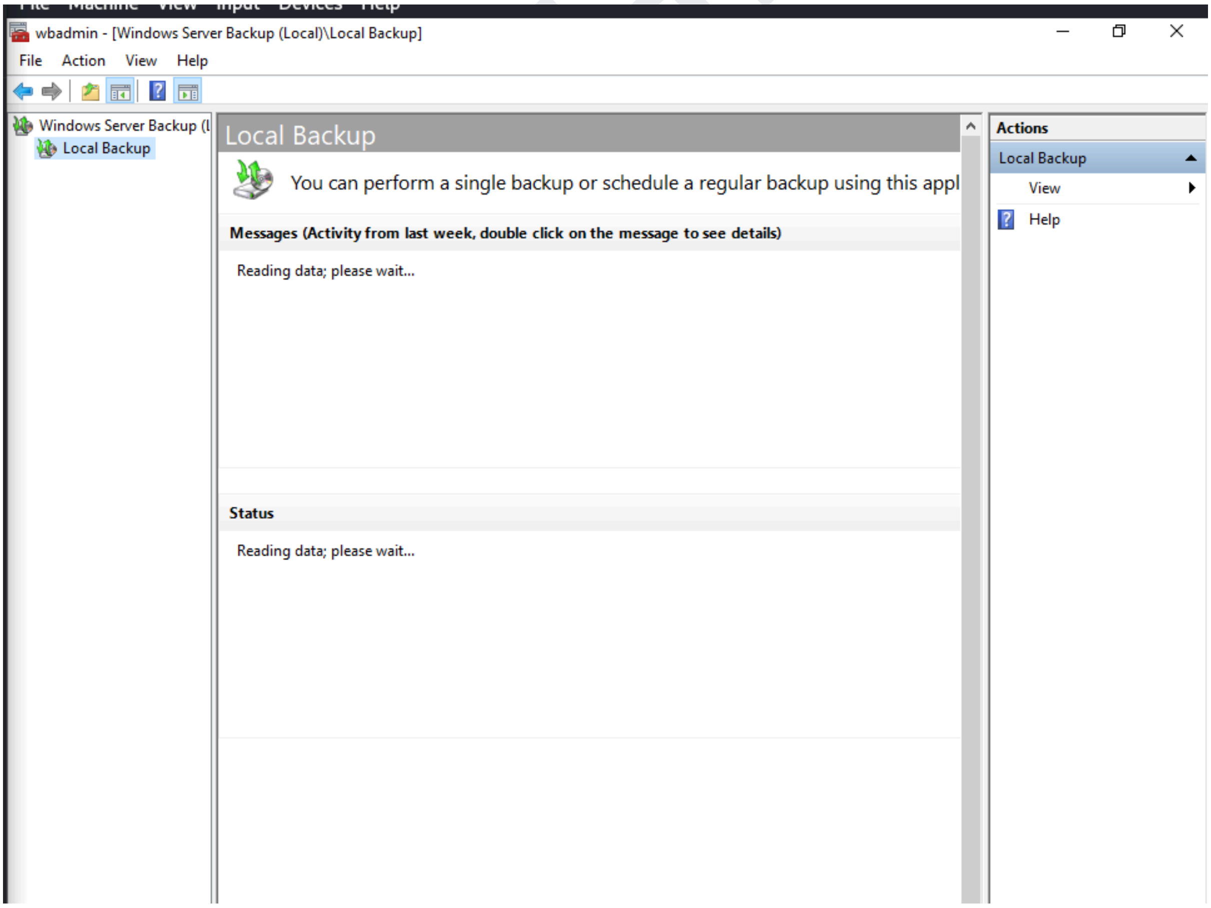
Last Backup Status: -

Next Backup Time: -

Number of available backups: -

Online Backup

⚠ Backups to Azure have not been configured for this server. Secure this server from corruptions and oth


File Machine View Input Devices Help
wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Windows Server Backup (L
Local Backup
Actions
Local Backup
View
Help

Local Backup

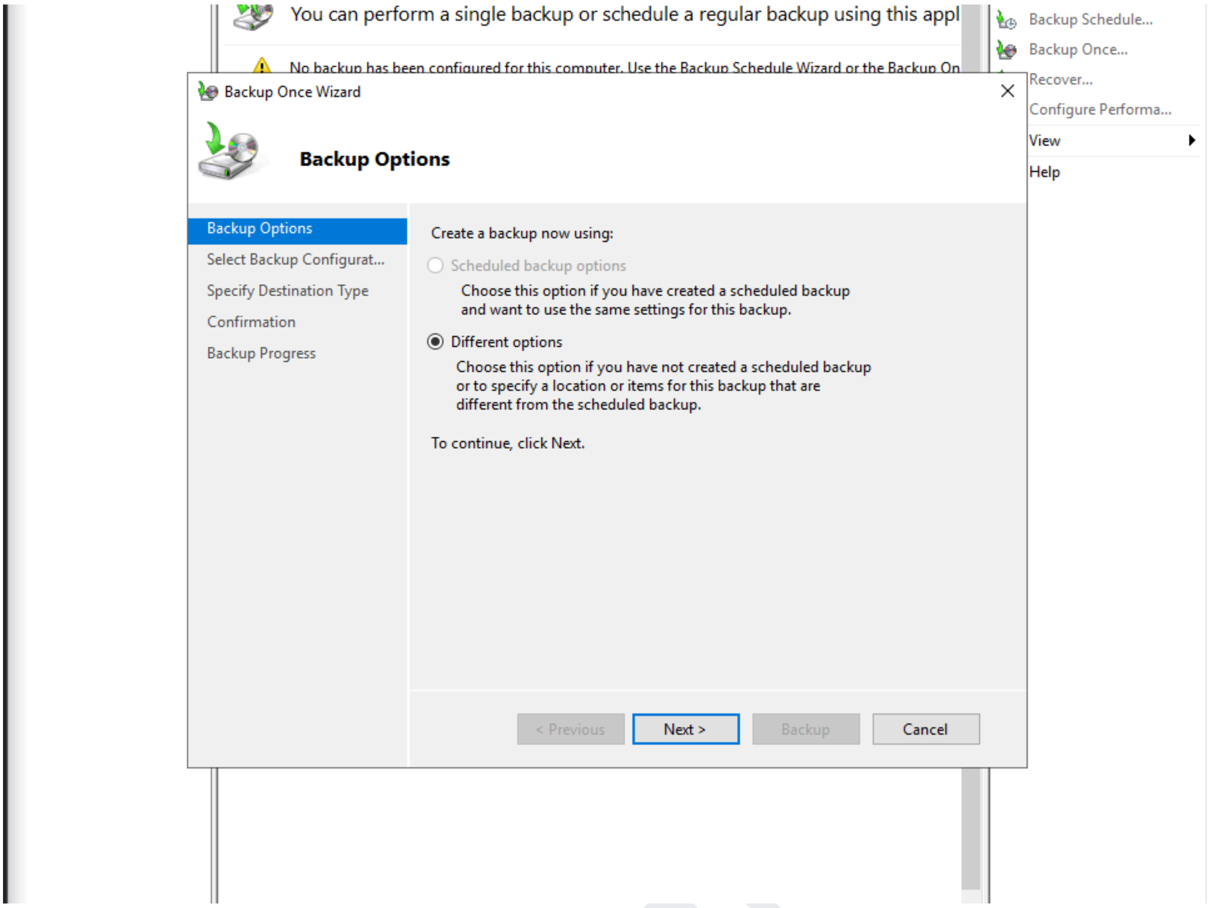
You can perform a single backup or schedule a regular backup using this appl

Messages (Activity from last week, double click on the message to see details)

Reading data; please wait...

Status

Reading data; please wait...



You can perform a single backup or schedule a regular backup using this appl

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup On

Backup Once Wizard

Backup Options

Create a backup now using:

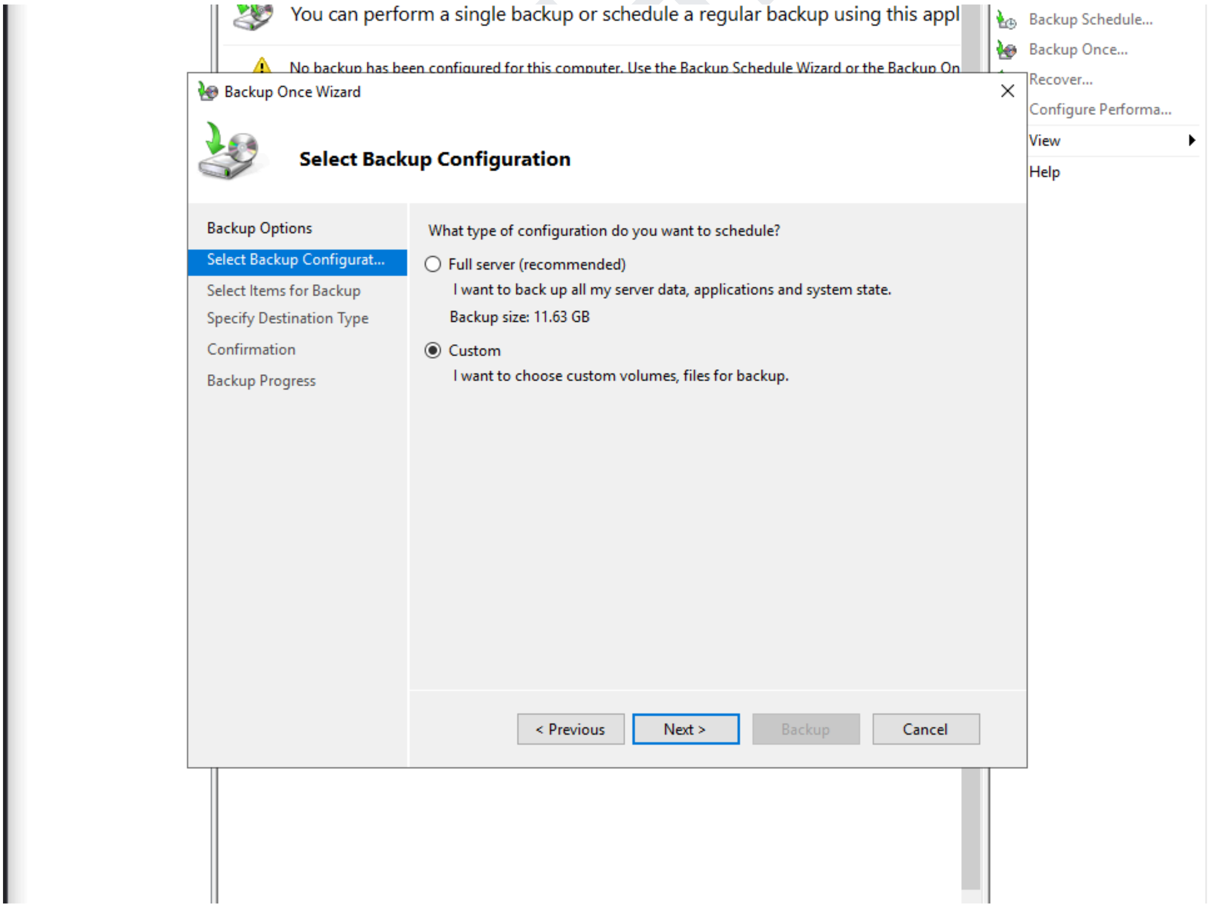
○ Scheduled backup options

Choose this option if you have created a scheduled backup and want to use the same settings for this backup.

● Different options

Choose this option if you have not created a scheduled backup or to specify a location or items for this backup that are different from the scheduled backup.

To continue, click Next.



You can perform a single backup or schedule a regular backup using this appl

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup On

Backup Once Wizard

Select Backup Configuration

What type of configuration do you want to schedule?

○ Full server (recommended)

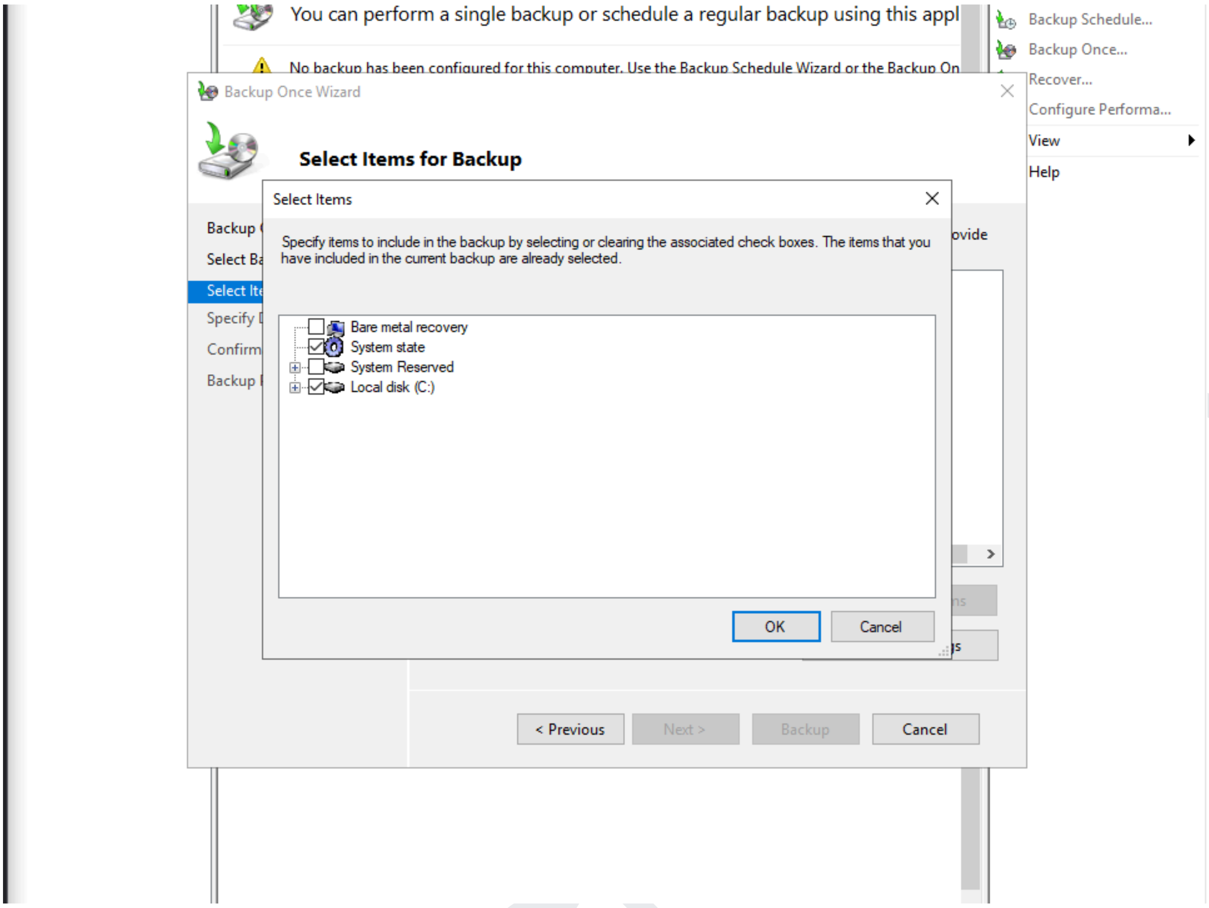
I want to back up all my server data, applications and system state.

Backup size: 11.63 GB

● Custom

I want to choose custom volumes, files for backup.

Select what to backup:



You can perform a single backup or schedule a regular backup using this appl

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup On

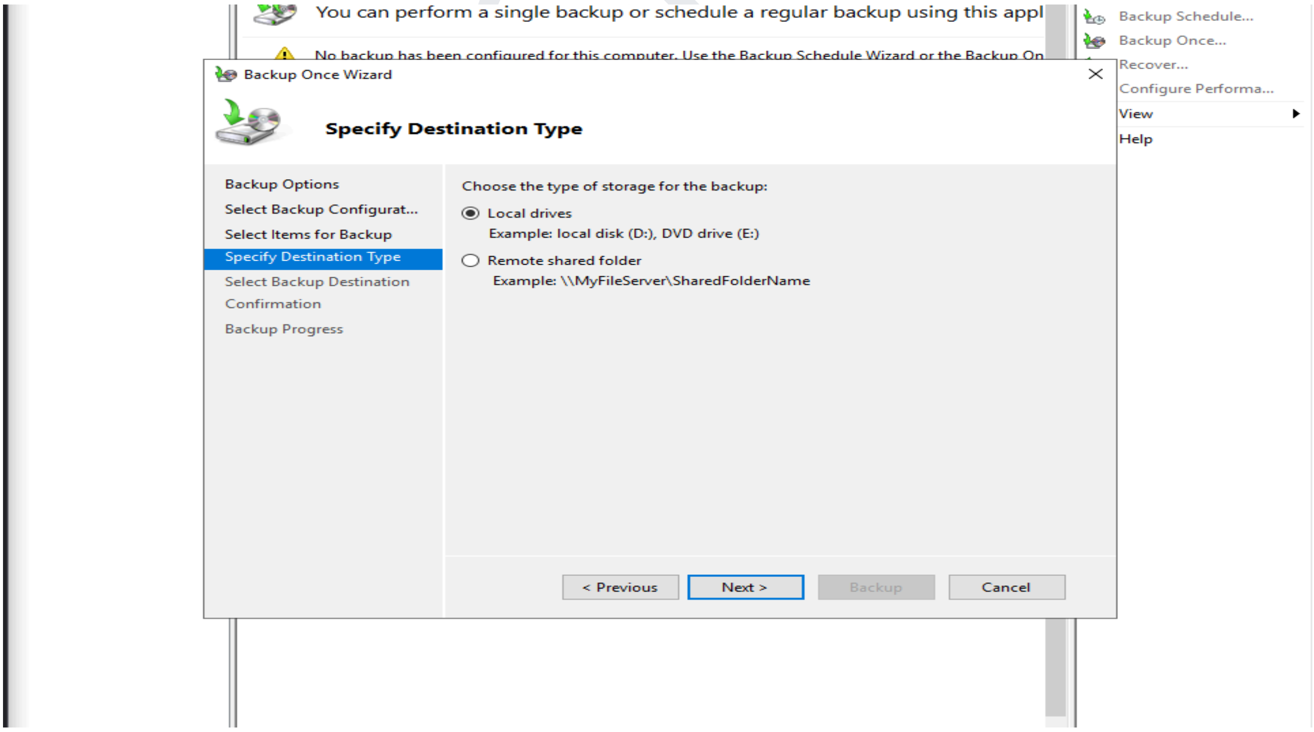
Backup Once Wizard

Select Items for Backup

Select Items

Specify items to include in the backup by selecting or clearing the associated check boxes. The items that you have included in the current backup are already selected.

- □ Bare metal recovery
- ☑ System state
- □ System Reserved
- ☑ Local disk (C:)



You can perform a single backup or schedule a regular backup using this appl

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup On

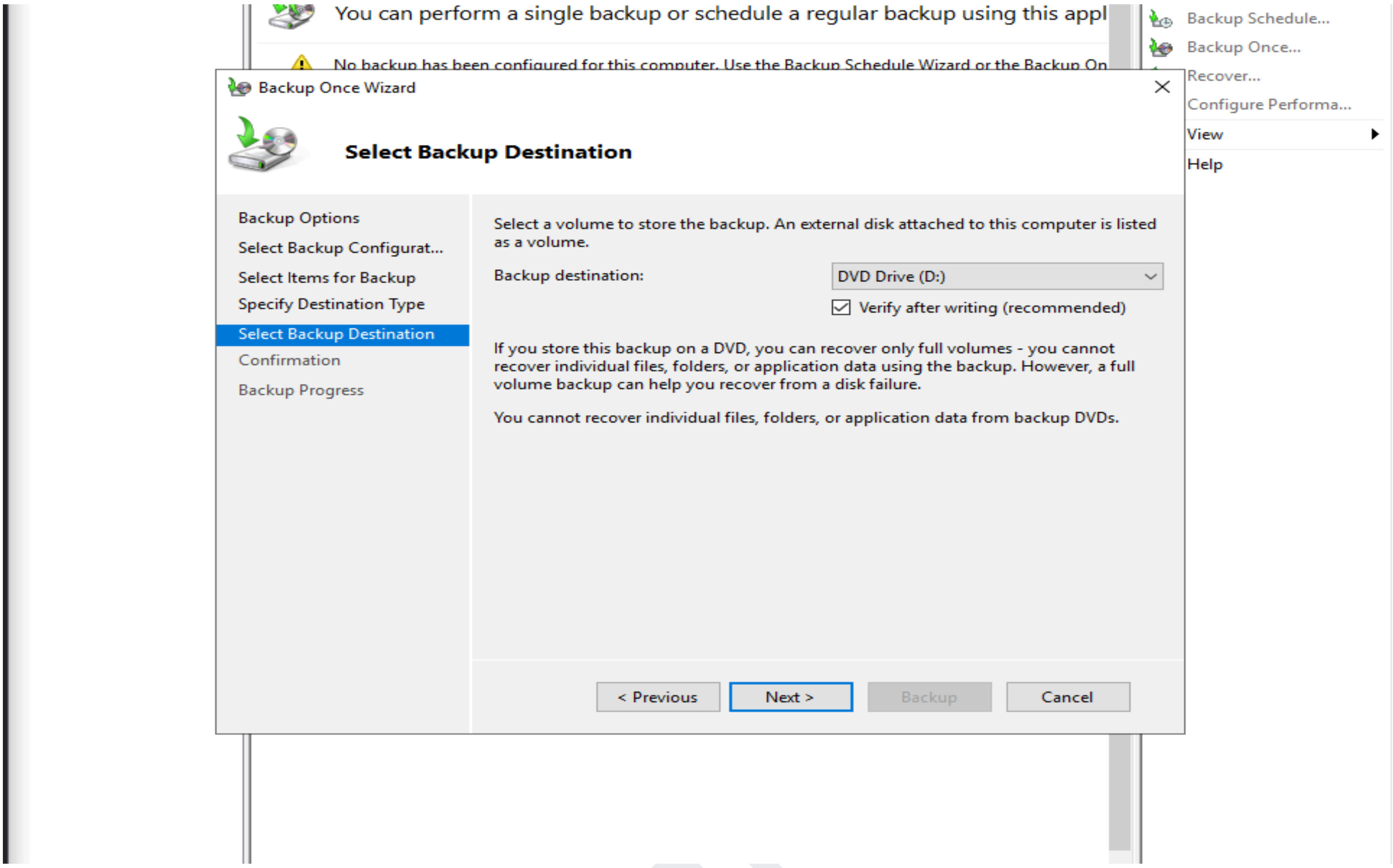
Backup Once Wizard

Specify Destination Type

Choose the type of storage for the backup:

● Local drives
Example: local disk (D:), DVD drive (E:)

○ Remote shared folder
Example: \\MyFileServer\SharedFolderName



You can perform a single backup or schedule a regular backup using this appl

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup On

Backup Once Wizard

Select Backup Destination

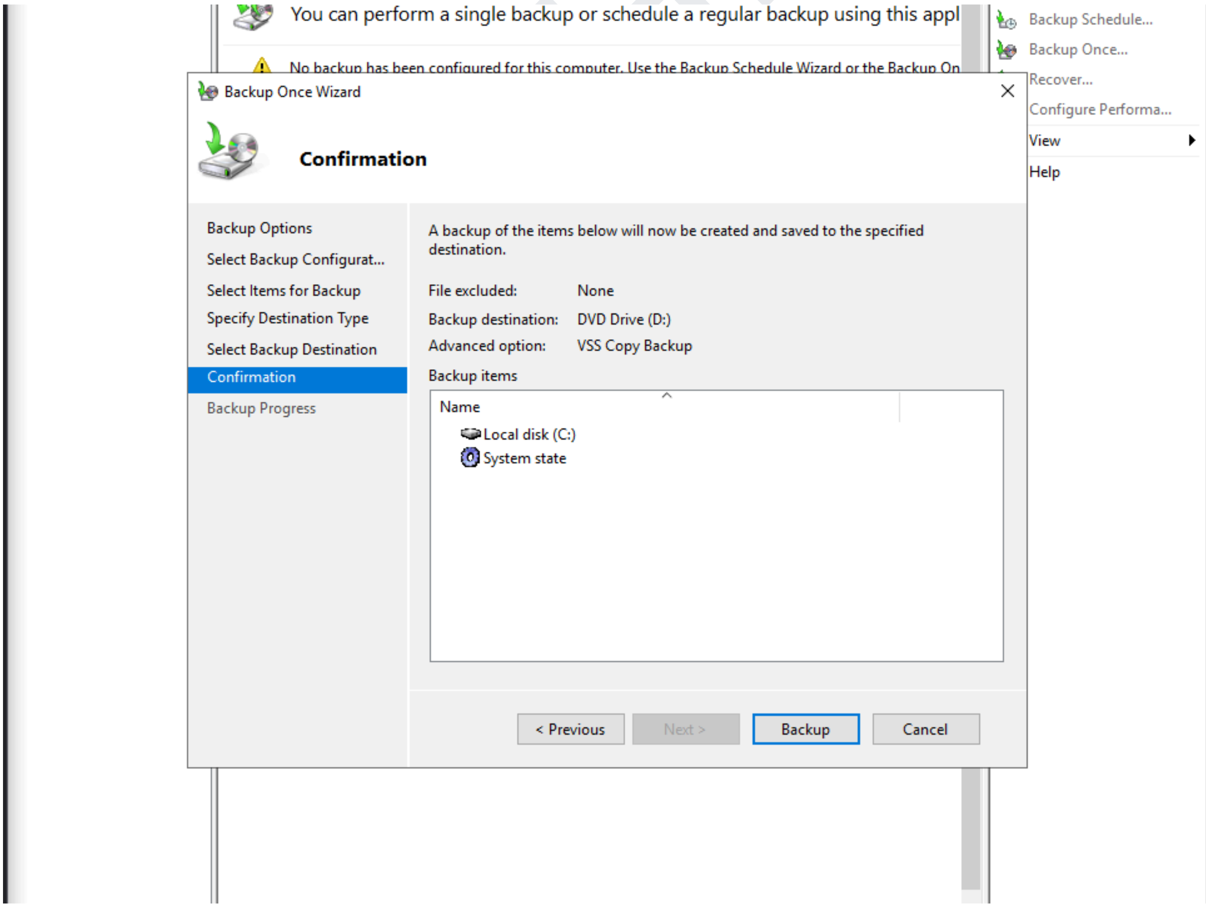
Select a volume to store the backup. An external disk attached to this computer is listed as a volume.

Backup destination: DVD Drive (D:)

☑ Verify after writing (recommended)

If you store this backup on a DVD, you can recover only full volumes - you cannot recover individual files, folders, or application data using the backup. However, a full volume backup can help you recover from a disk failure.

You cannot recover individual files, folders, or application data from backup DVDs.



You can perform a single backup or schedule a regular backup using this appl

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup On

Backup Once Wizard

Confirmation

A backup of the items below will now be created and saved to the specified destination.

File excluded: None

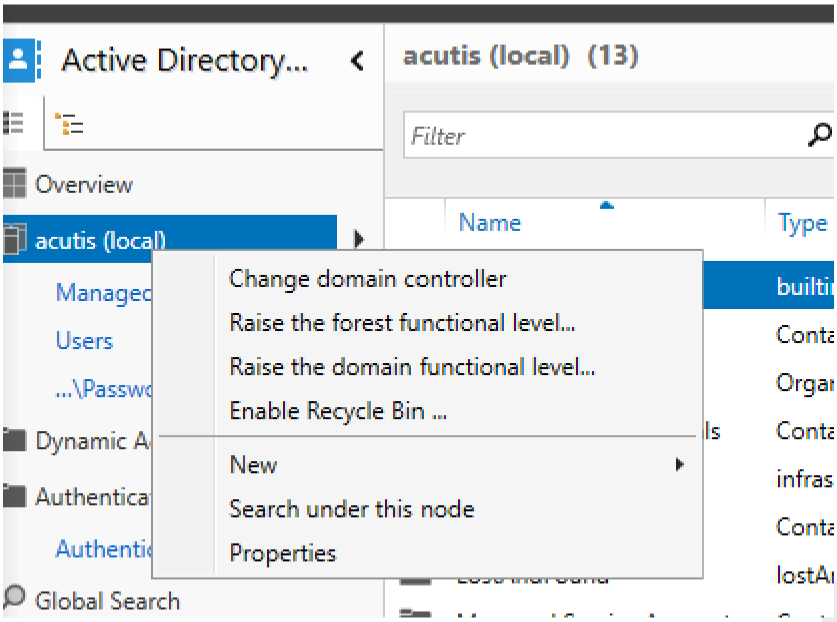
Backup destination: DVD Drive (D:)

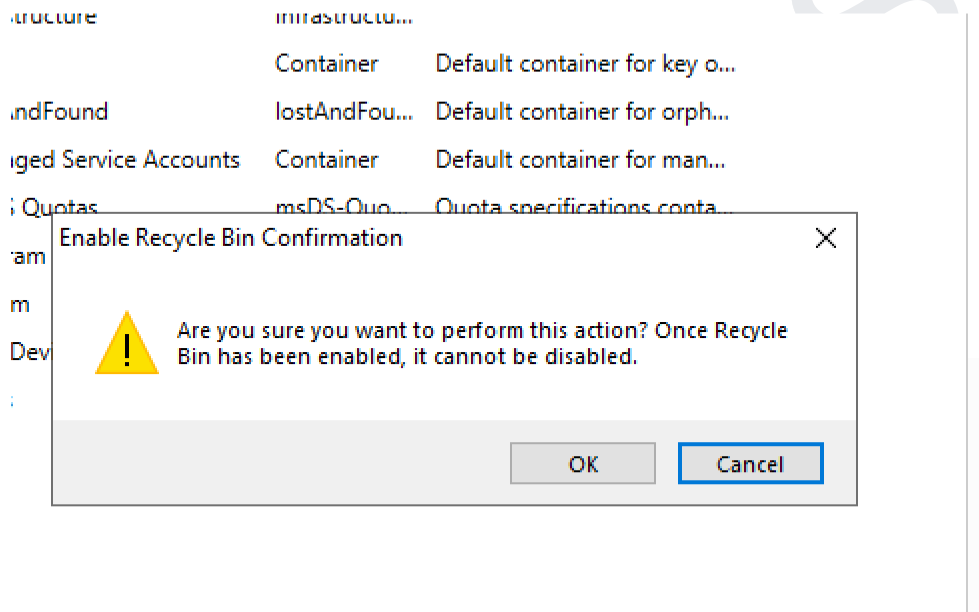
Advanced option: VSS Copy Backup

Backup items

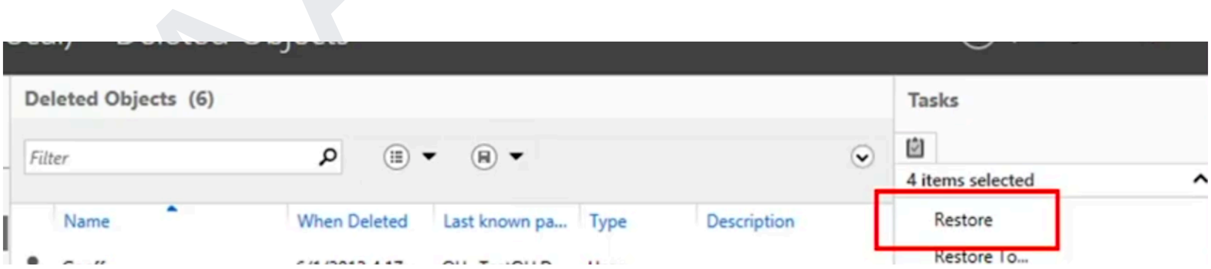
Name
Local disk (C:)
System state

Another option for backing up or recovering is “**Enabling Recycle Bin” from Active directory**




ıtructure
infrastructu...
Container
Default container for key o...
ındFound
lostAndFou...
Default container for orph...
ıged Service Accounts
Container
Default container for man...
; Quotas
msDS-Quo...
Quota specifications conta...
am
m
Dev
Enable Recycle Bin Confirmation

Are you sure you want to perform this action? Once Recycle Bin has been enabled, it cannot be disabled.



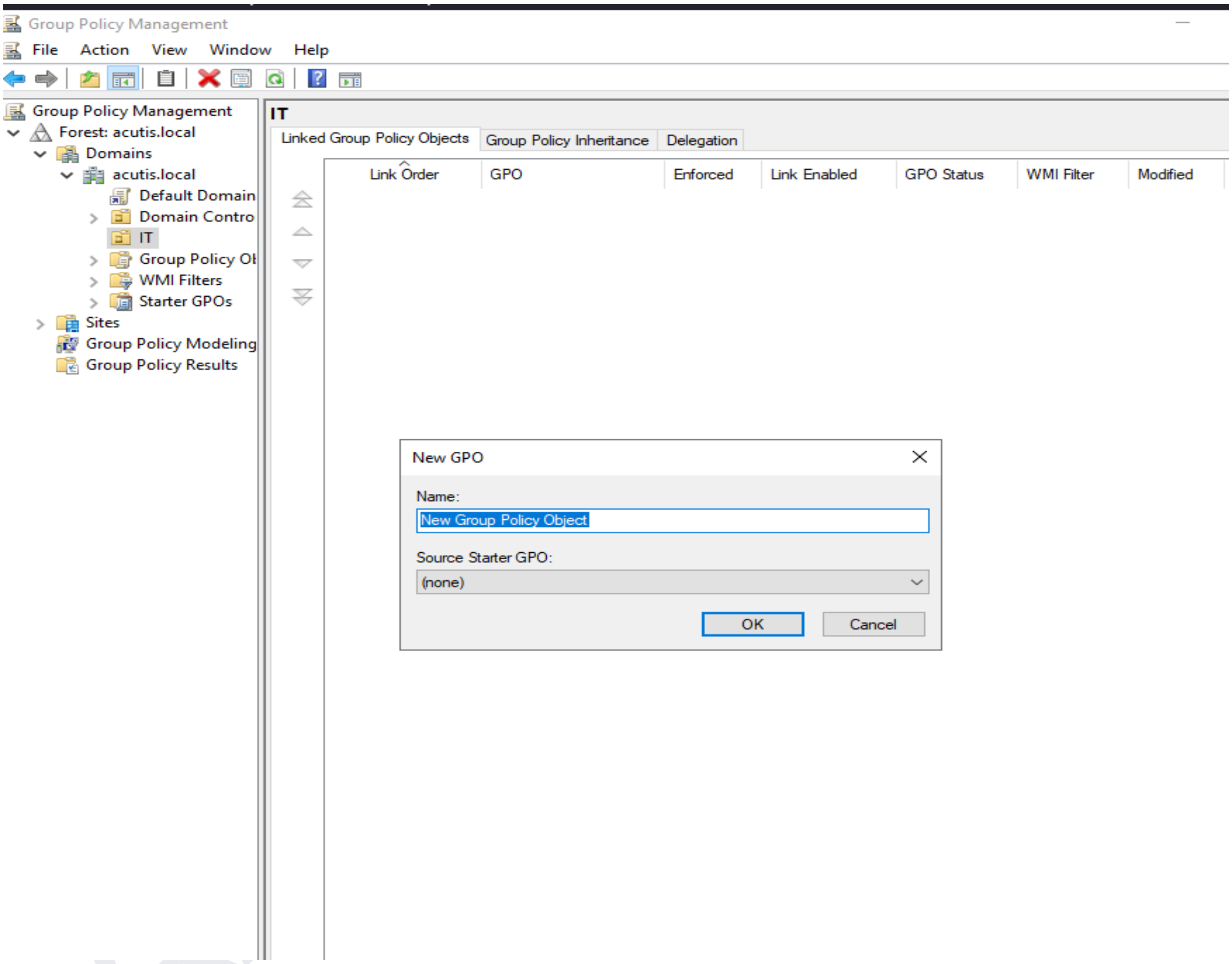
5.6 Implement and Manage Group Policies

1. Create and Link GPOs

Group Policy Objects (GPOs) are used to enforce settings for users and computers in Active Directory. You can create new GPOs and link them to domains, organizational units (OUs), or sites.

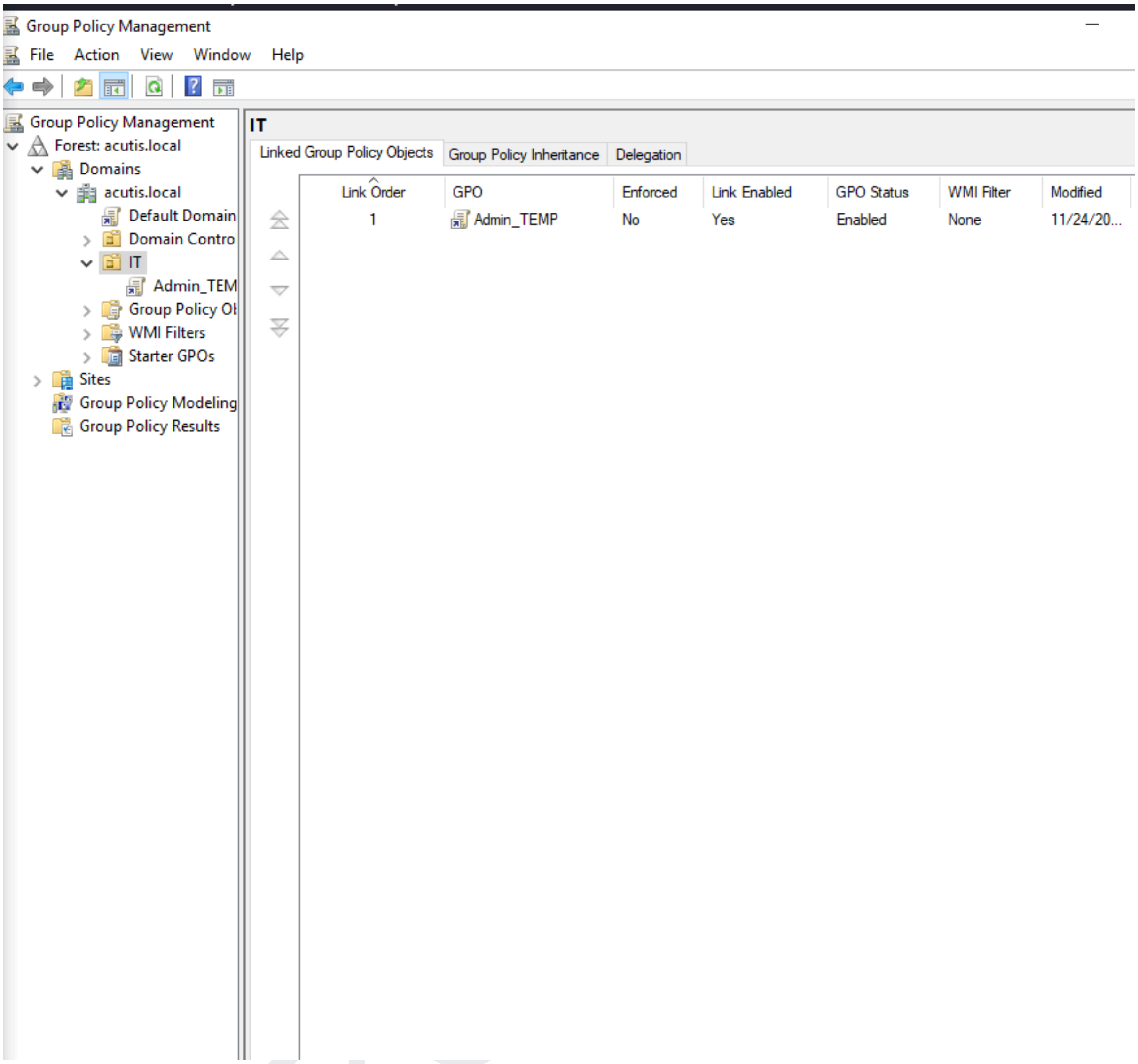
a. Open Group Policy Management Console (GPMC):

Create new GPO:



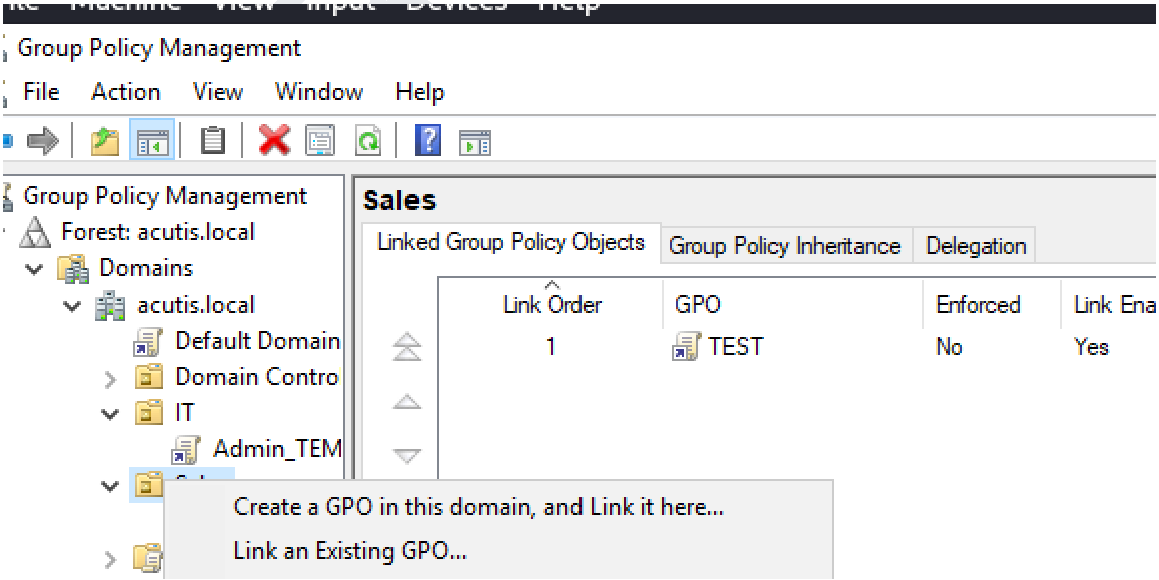
Name:
New Group Policy Object

Source Starter GPO:
(none)



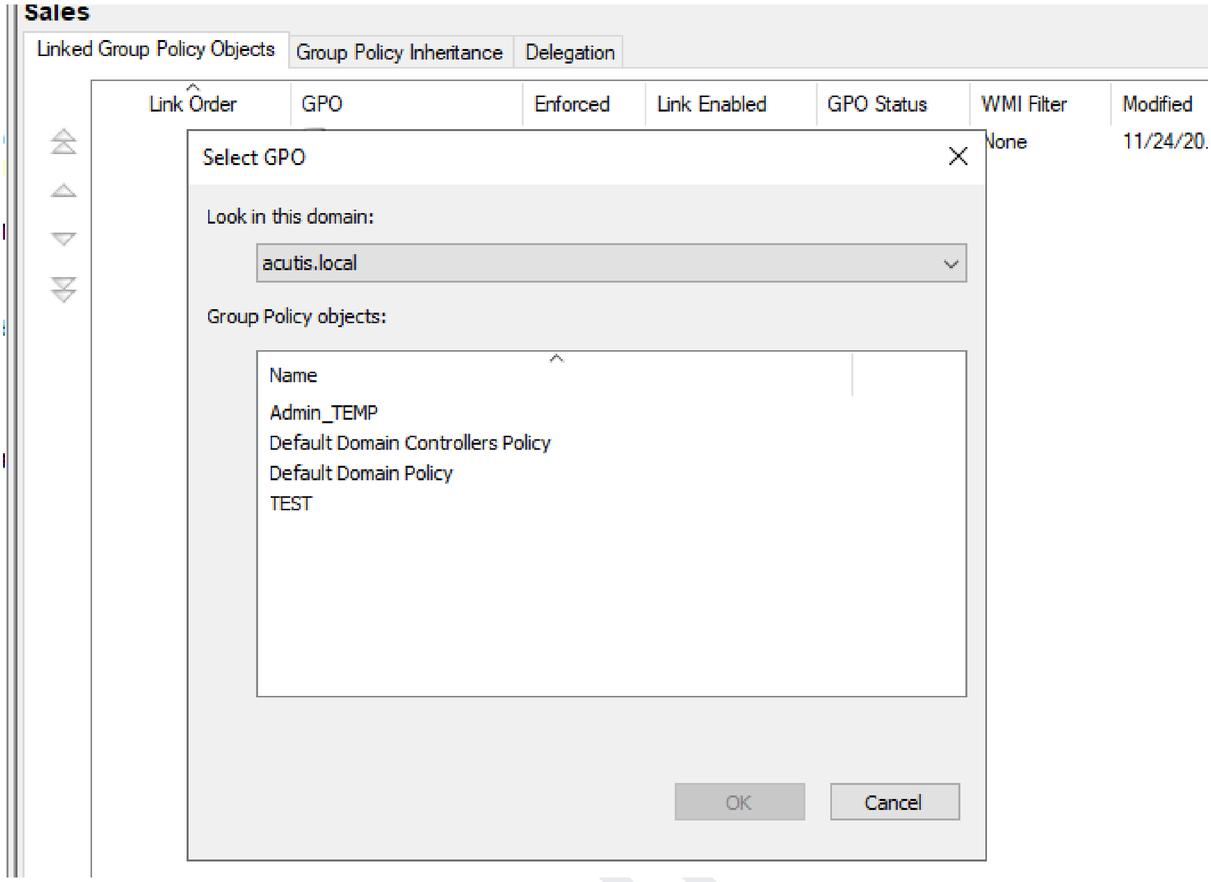
IT

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified
1	Admin_TEMP	No	Yes	Enabled	None	11/24/20...



Sales

Link Order	GPO	Enforced	Link Ena
1	TEST	No	Yes



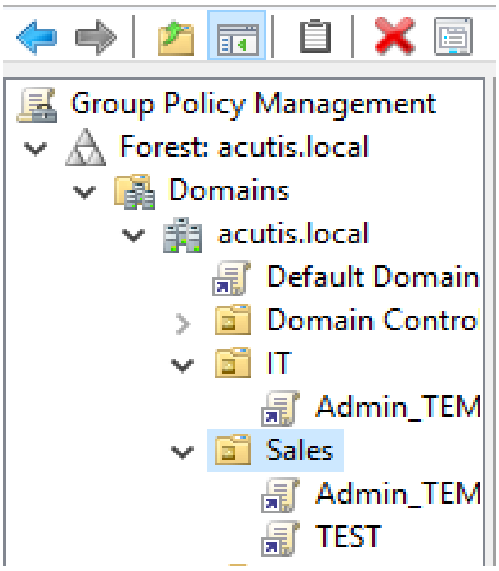
Look in this domain:

acutis.local

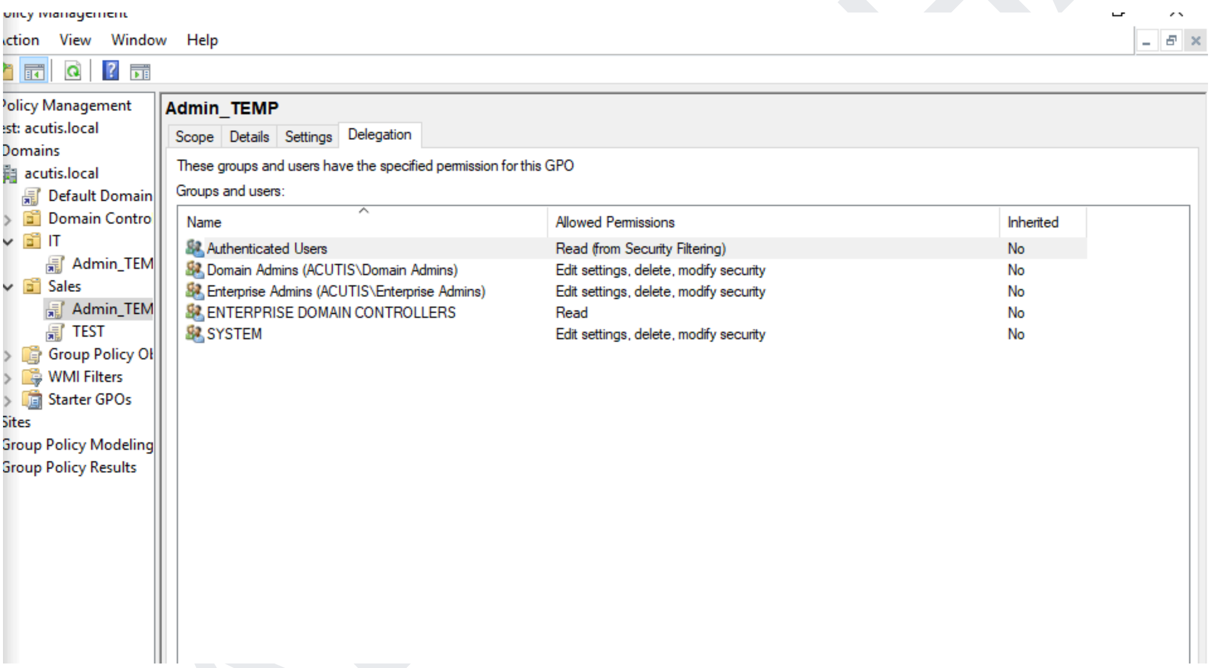
Group Policy objects:

Name
Admin_TEMP
Default Domain Controllers Policy
Default Domain Policy
TEST

Can link GPO with other units:



- Group Policy Management
  - Forest: acutis.local
    - Domains
      - acutis.local
        - Default Domain
        - Domain Contro
        - IT
          - Admin_TEM
        - Sales
          - Admin_TEM
          - TEST



- 'olicy Management
  - st: acutis.local
    - Domains
      - acutis.local
        - Default Domain
        - Domain Contro
        - IT
          - Admin_TEM
        - Sales
          - Admin_TEM
          - TEST
        - Group Policy Ol
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

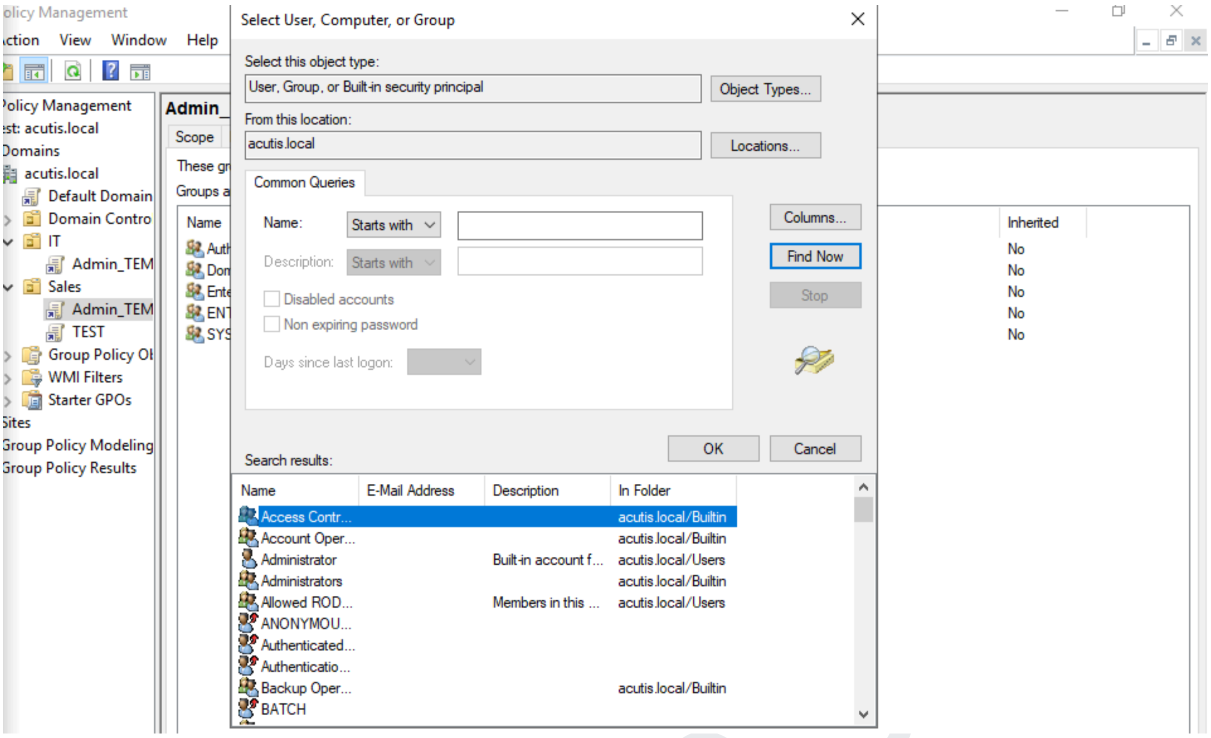
Admin_TEMP

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (ACUTIS\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (ACUTIS\Enterprise Admins)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
SYSTEM	Edit settings, delete, modify security	No

Can restrict units and provide additional permissiins



Select User, Computer, or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
acutis.local

Name: Starts with

Description: Starts with

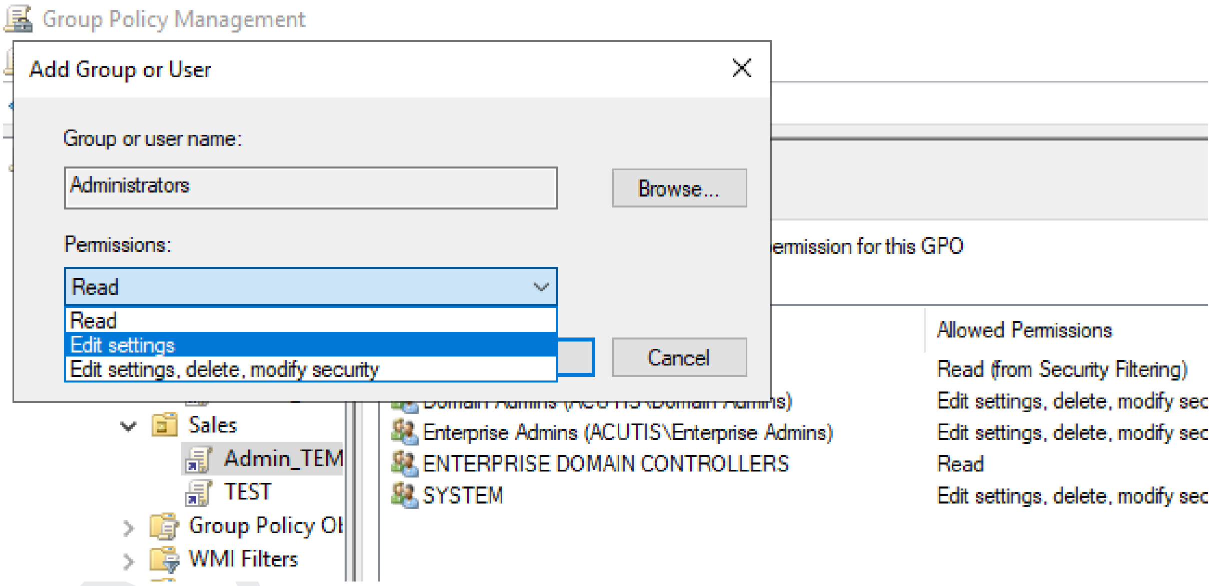
□ Disabled accounts

□ Non expiring password

Days since last logon:

Search results:

Name	E-Mail Address	Description	In Folder
Access Contr...			acutis.local/Builtin
Account Oper...			acutis.local/Builtin
Administrator		Built-in account f...	acutis.local/Users
Administrators			acutis.local/Builtin
Allowed ROD...		Members in this ...	acutis.local/Users
ANONYMOU...			
Authenticated...			
Authenticatio...			
Backup Oper...			acutis.local/Builtin
BATCH			



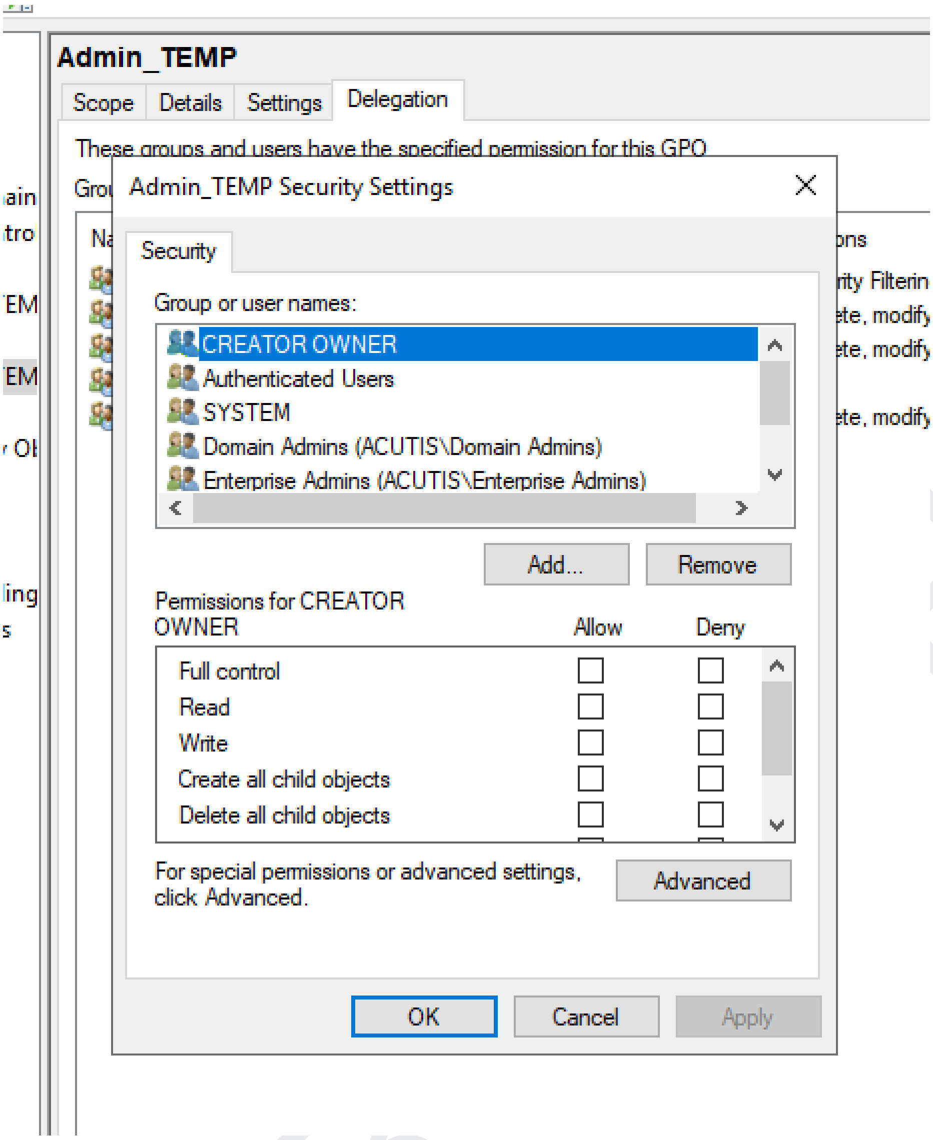
Add Group or User

Group or user name:
Administrators

Permissions:
Read

Read
Edit settings
Edit settings, delete, modify security

	Allowed Permissions
Domain Admins (ACUTIS\Domain Admins)	Read (from Security Filtering)
	Edit settings, delete, modify sec
Enterprise Admins (ACUTIS\Enterprise Admins)	Edit settings, delete, modify sec
ENTERPRISE DOMAIN CONTROLLERS	Read
SYSTEM	Edit settings, delete, modify sec



Admin_TEMP

These groups and users have the specified permission for this GPO

Admin_TEMP Security Settings

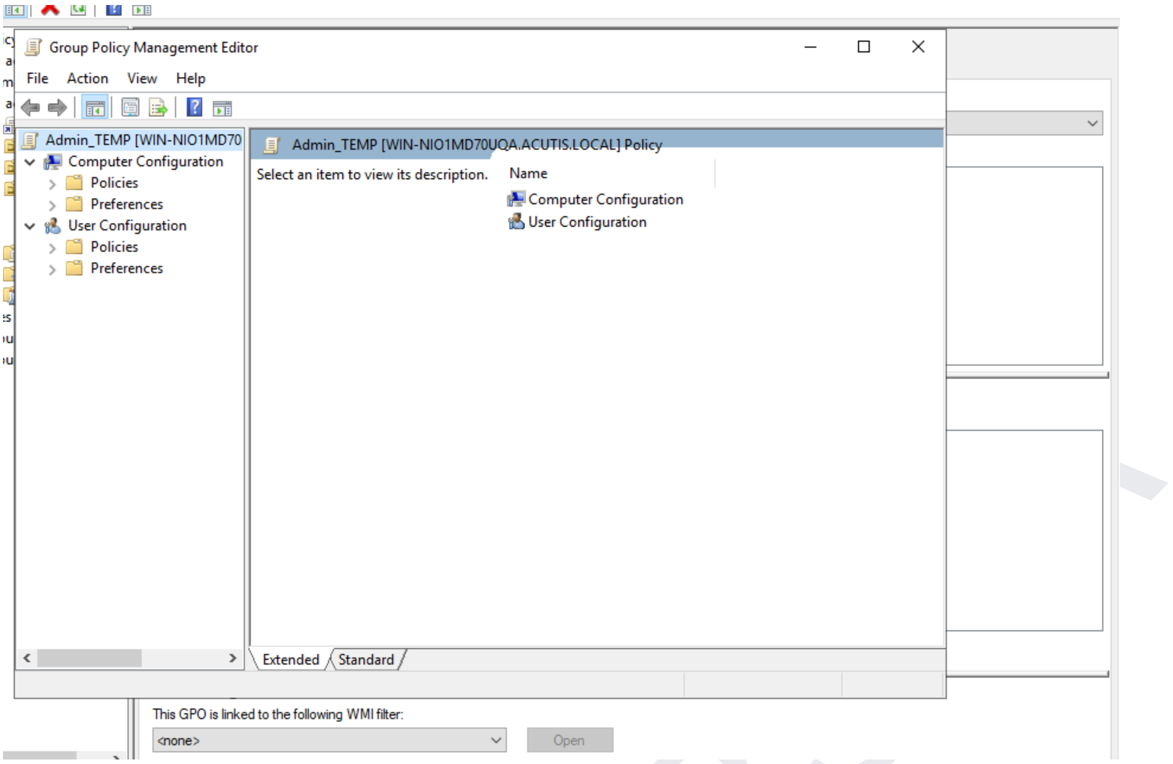
Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Domain Admins (ACUTIS\Domain Admins)
- Enterprise Admins (ACUTIS\Enterprise Admins)

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□

For special permissions or advanced settings, click Advanced.

5.7 Administration Templates:



Admin_TEMP [WIN-NIO1MD70
- Computer Configuration
  - Policies
  - Preferences
- User Configuration
  - Policies
  - Preferences

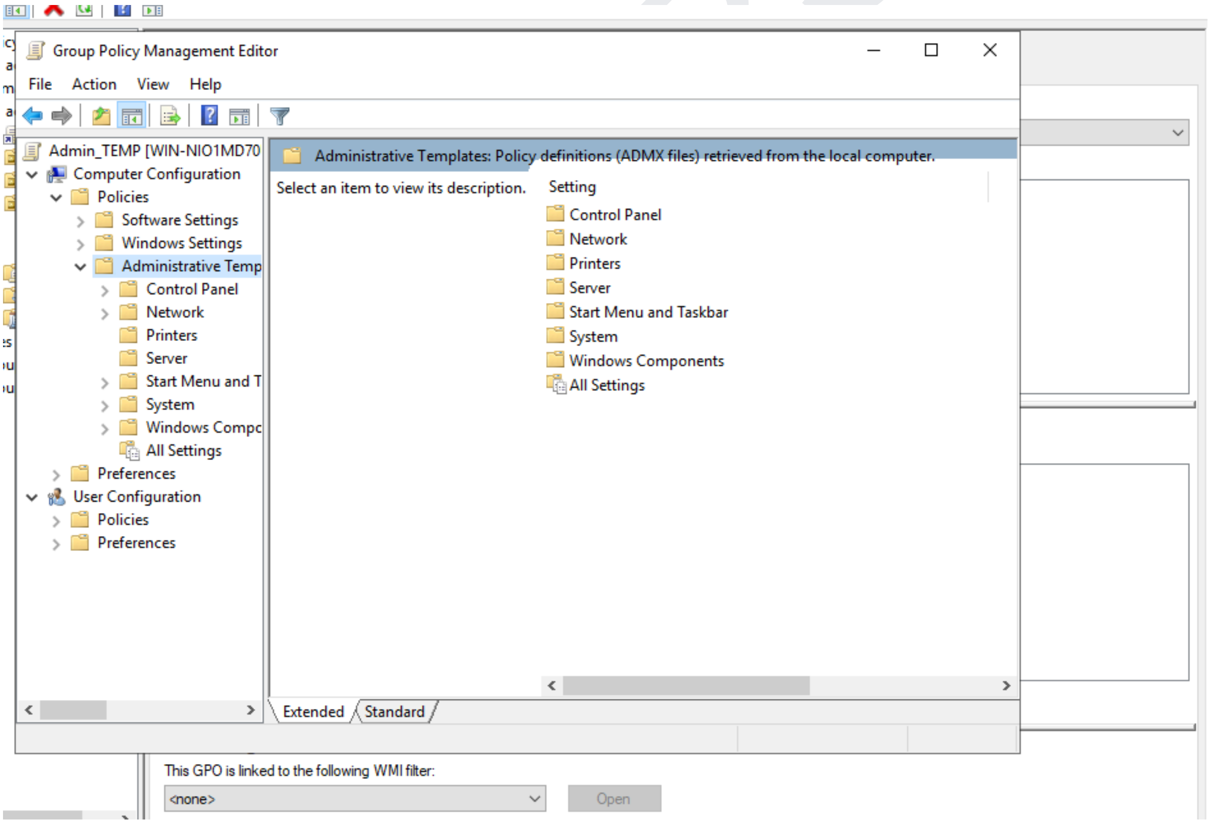
Admin_TEMP [WIN-NIO1MD70UQA.ACUTIS.LOCAL] Policy

Select an item to view its description.

Name
Computer Configuration
User Configuration

This GPO is linked to the following WMI filter:

<none>



Admin_TEMP [WIN-NIO1MD70
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Temp
      - Control Panel
      - Network
      - Printers
      - Server
      - Start Menu and T
      - System
      - Windows Compc
      - All Settings
  - Preferences
- User Configuration
  - Policies
  - Preferences

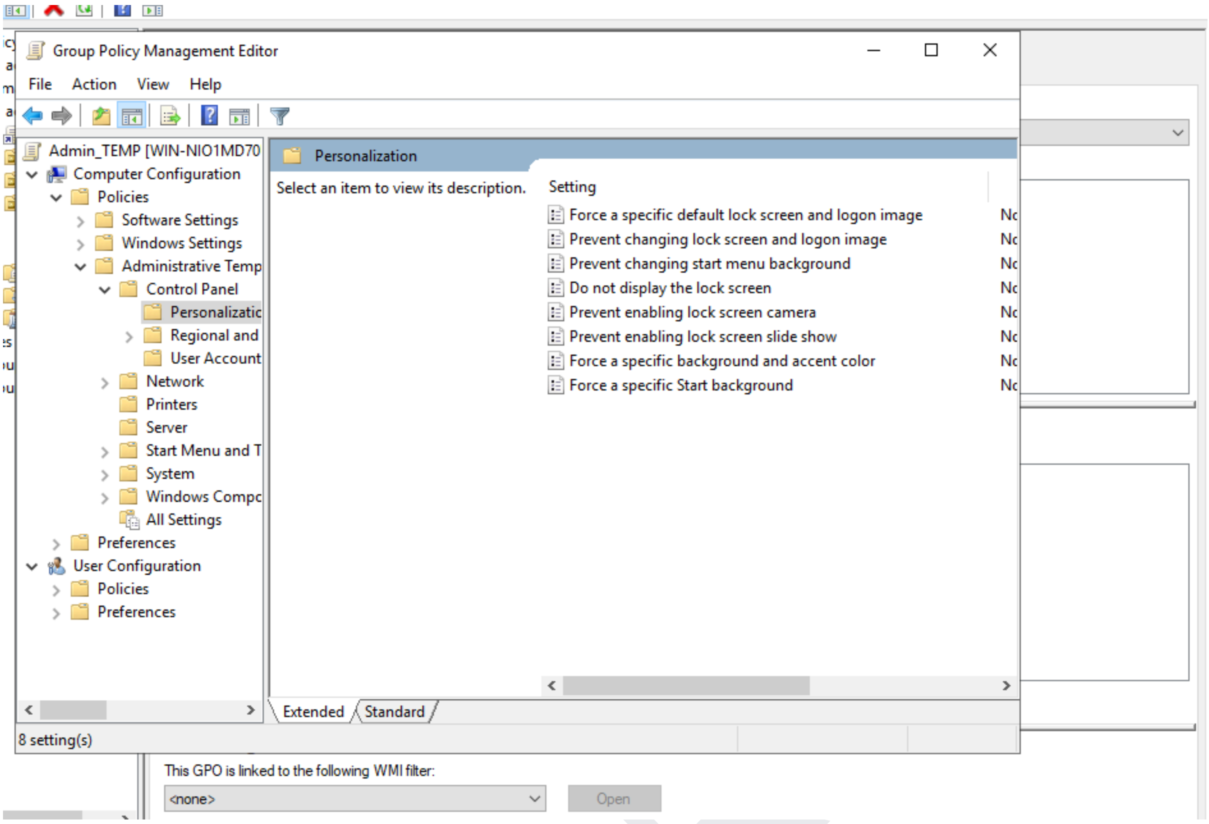
Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.

Select an item to view its description.

Setting
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
Windows Components
All Settings

This GPO is linked to the following WMI filter:

<none>



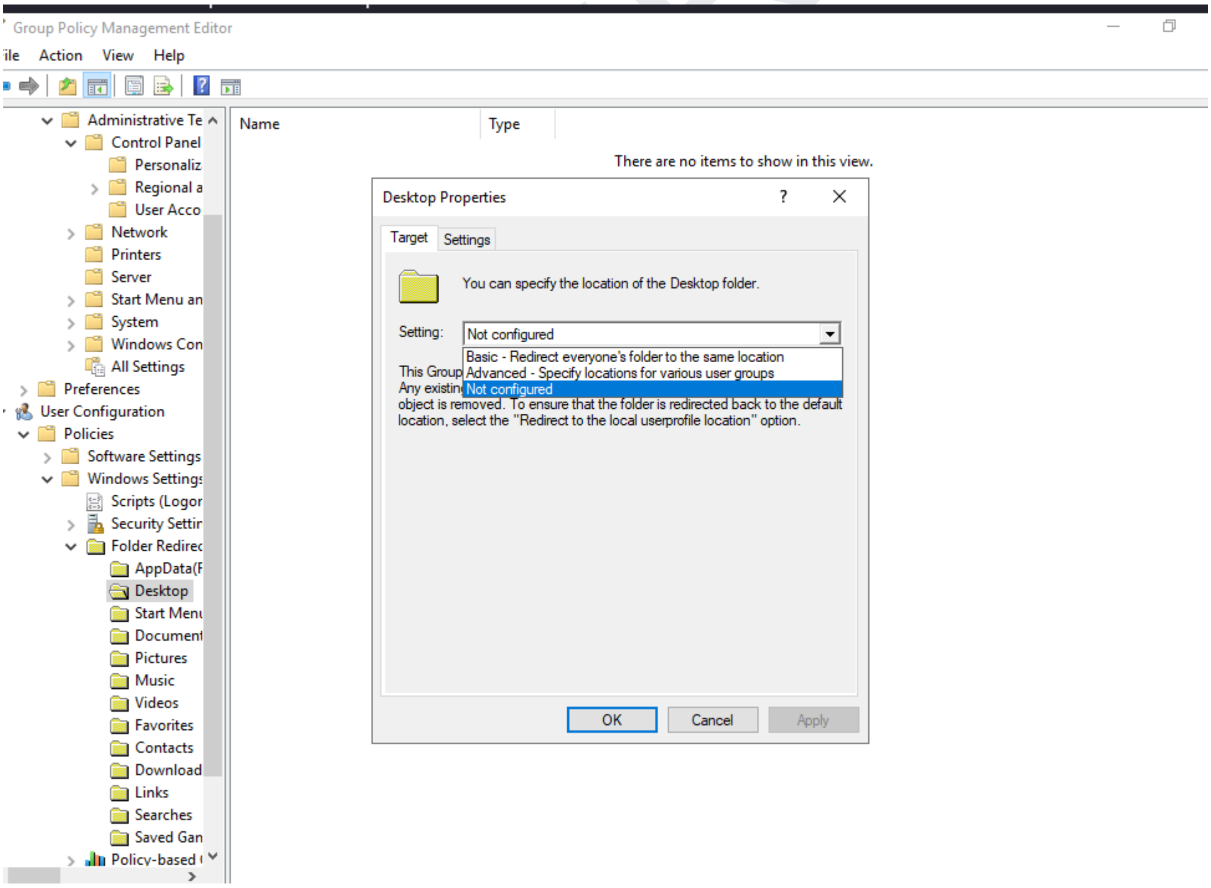
Select an item to view its description.

Setting	
Force a specific default lock screen and logon image	Nc
Prevent changing lock screen and logon image	Nc
Prevent changing start menu background	Nc
Do not display the lock screen	Nc
Prevent enabling lock screen camera	Nc
Prevent enabling lock screen slide show	Nc
Force a specific background and accent color	Nc
Force a specific Start background	Nc

8 setting(s)

This GPO is linked to the following WMI filter:

<none>



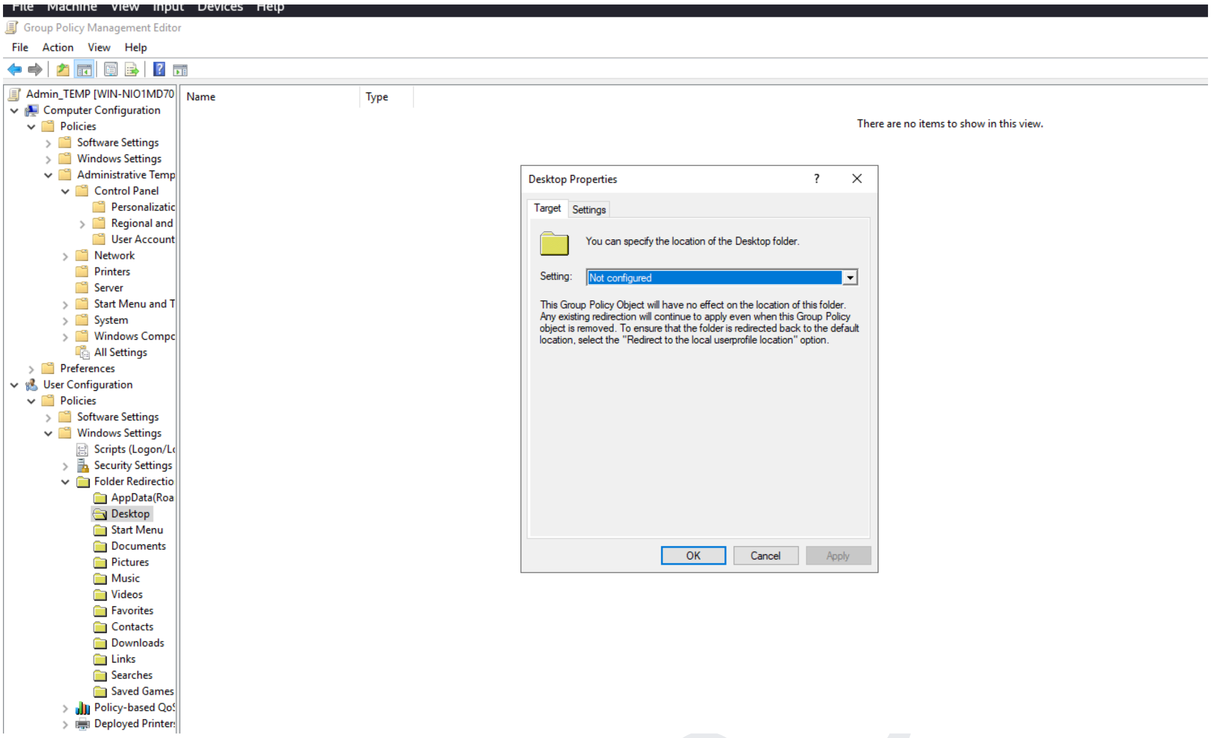
There are no items to show in this view.

You can specify the location of the Desktop folder.

Setting: Not configured

Basic - Redirect everyone's folder to the same location
Advanced - Specify locations for various user groups
Not configured

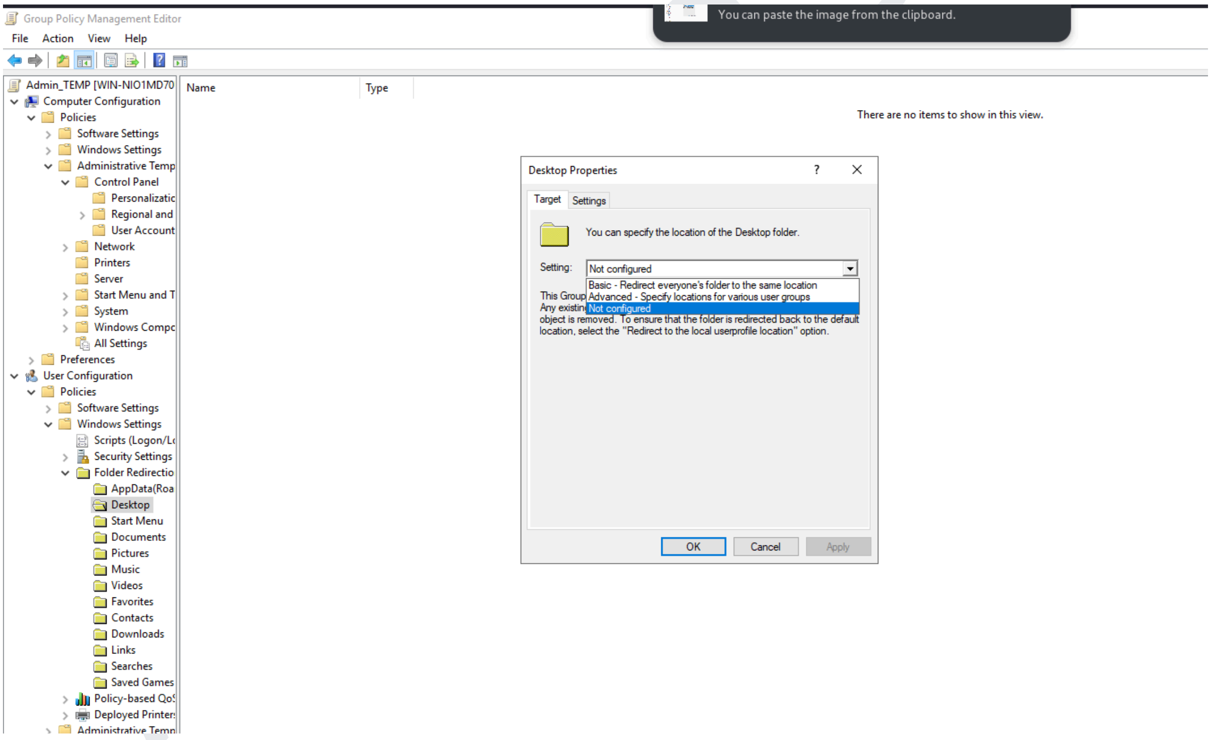
This Group
Any existin
object is removed. To ensure that the folder is redirected back to the default location, select the "Redirect to the local userprofile location" option.



You can specify the location of the Desktop folder.

Setting: Not configured

This Group Policy Object will have no effect on the location of this folder. Any existing redirection will continue to apply even when this Group Policy object is removed. To ensure that the folder is redirected back to the default location, select the "Redirect to the local userprofile location" option.



You can specify the location of the Desktop folder.

Setting: Not configured

Basic - Redirect everyone's folder to the same location
Advanced - Specify locations for various user groups
Not configured

This Group Any existin object is removed. To ensure that the folder is redirected back to the default location, select the "Redirect to the local userprofile location" option.

6. Challenges and Resolutions

1. Challenge: Initial difficulty in networking the virtual machines.
   - Resolution: Switched from NAT to Bridged Adapter in VirtualBox settings to establish proper connectivity.
   2. Challenge: Cloning a Domain Controller required meticulous pre-requisites like creating the configuration file.
   - Resolution: Followed Microsoft's guidelines for DC cloning and tested thoroughly in a virtual environment.
   3. Challenge: Setting the server in VM office with limited Hardware capability
   - Resolution: Assigned Less memory to each system to work effeciently

7. Conclusion

This project successfully simulated the deployment and management of an Active Directory environment using Windows Server 2019. The exploration of advanced features such as RODCs, Authentication Silos, and GPOs demonstrated the flexibility and security capabilities of AD DS. The challenges faced provided valuable insights into real-world scenarios, emphasizing the importance of careful planning and testing.The configured AD DS environment and detailed documentation serve as a valuable reference for implementing similar projects in enterprise environments.

8. References

- Microsoft Documentation:

- Active Directory Domain Services Overview:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/

- Group Policy Management:

https://docs.microsoft.com/en-us/windows-server/administration/grouppolicy/grouppolicy-overview

- Online Forums and Tutorials:
  - TechNet Forums for troubleshooting GPO and AD DS issues.
  - VirtualBox Networking Guides for proper VM setup.