Advanced Active Directory Management and Group Policy Implementation

BY:
Aabhash Paudel 3746

Nov 25 - 2024
L&T Edutech
Sri Vnkateshwara College of Engineering & Technology

S.N	Content
1)	Introduction
2)	Objectives
3)	Methodology
4)	Documentation
5)	Challenges and Resolution
6)	Conclusion
7)	References

Project Report

Advanced Active Directory Management and Group Policy Implementation

1. Introduction

Active Directory (AD) is a critical service in Windows Server that centralizes domain management, user authentication, and resource access. This project focuses on setting up an AD environment and managing user accounts. The tasks include configuring AD, creating and managing user accounts, enforcing security policies, and using PowerShell for administrative purposes. The objective is to gain practical experience in managing an enterprise-level directory service.

2. Objectives

Our primary objective was to expand and fortify the existing Active Directory (AD) infrastructure.The specific objectives included:

The key objectives of the project are:

1. To install and configure Active Directory in a new Windows Server instance.
2. To create and manage user accounts with specific restrictions.
3. To enforce logon and security policies for users.
4. To configure Organizational Units (OUs) and manage computer accounts.
5. To explore PowerShell for automating Active Directory administration.

3. Methodology

3.1 Environment Setup

- **Virtualization Platform**: Oracle VirtualBox was used to create a virtualized Windows Server 2019 environment.
- **Networking**: A bridged adapter configuration was used to connect the server to the mobile hotspot for proper networking.
- **System**: Windows Server 2019 Standard Edition installed on the VM.

3.2 Step-by-Step Implementation

1. **Install and Configure Active Directory**

- Installed the “Active Directory Domain Services” role via the Server Manager.
- Promoted the server as a Domain Controller for a new domain (e.g., example.local).
- Configured the Directory Services Restore Mode (DSRM) password for recovery.

2. **Create a User in Active Directory**
   - Used the Active Directory Users and Computers (ADUC) console.
   - Created a new user (e.g., John.Doe) under a custom Organizational Unit (OU).
   - Assigned an initial password and set the requirement to change the password upon first login.
3. **Limit the Computers a User Can Log On To**
   - Edited the properties of the user account in ADUC.
   - Specified a list of computers the user can access under the “Logon To” tab.
4. **Limit the Logon Hours for a User**
   - Configured the logon hours in the “Account” properties of the user.
   - Restricted access outside of designated working hours.
5. **Reset a User’s Password**
   - Demonstrated password reset functionality via ADUC for user accounts.
6. **Unlock or Enable an Account in Active Directory**
   - Simulated an account lockout and unlocked it using ADUC.
7. **Manage User Accounts and Groups**
   - Created and managed Security Groups in ADUC.
   - Added users to groups for role-based access control.
8. **Manage Computer Accounts and Organizational Units (OUs)**
   - Organized computers and users into separate OUs for better management.
   - Applied Group Policy Objects (GPOs) to specific OUs for enforcing policies.
9. **Use PowerShell for AD Administration**
   - Used cmdlets like New-ADUser, Get-ADUser, and Set-ADUser for user creation and modifications.
   - Automated tasks like resetting passwords and configuring group memberships.

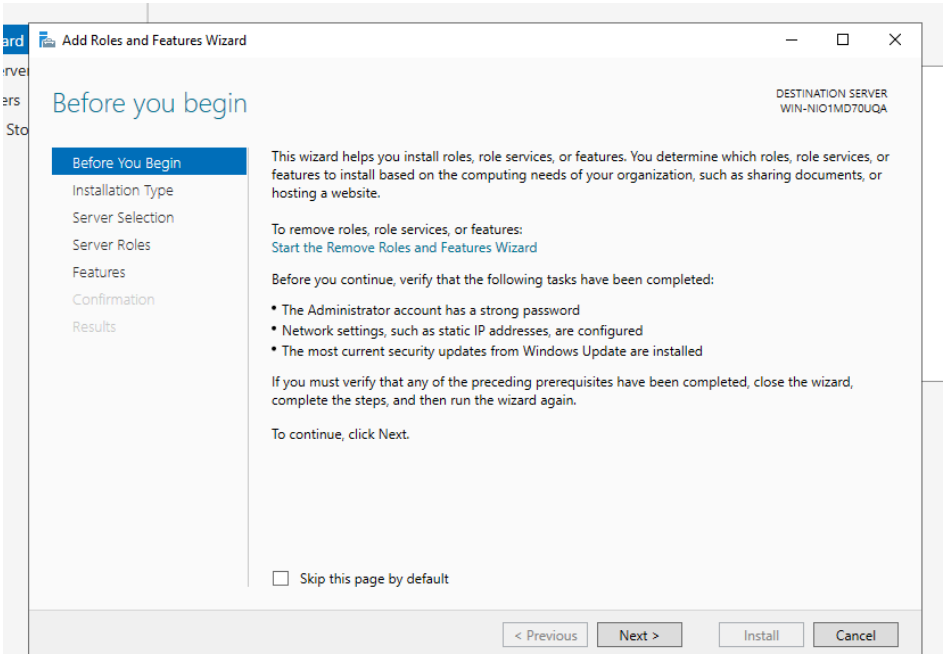
3. Documentation

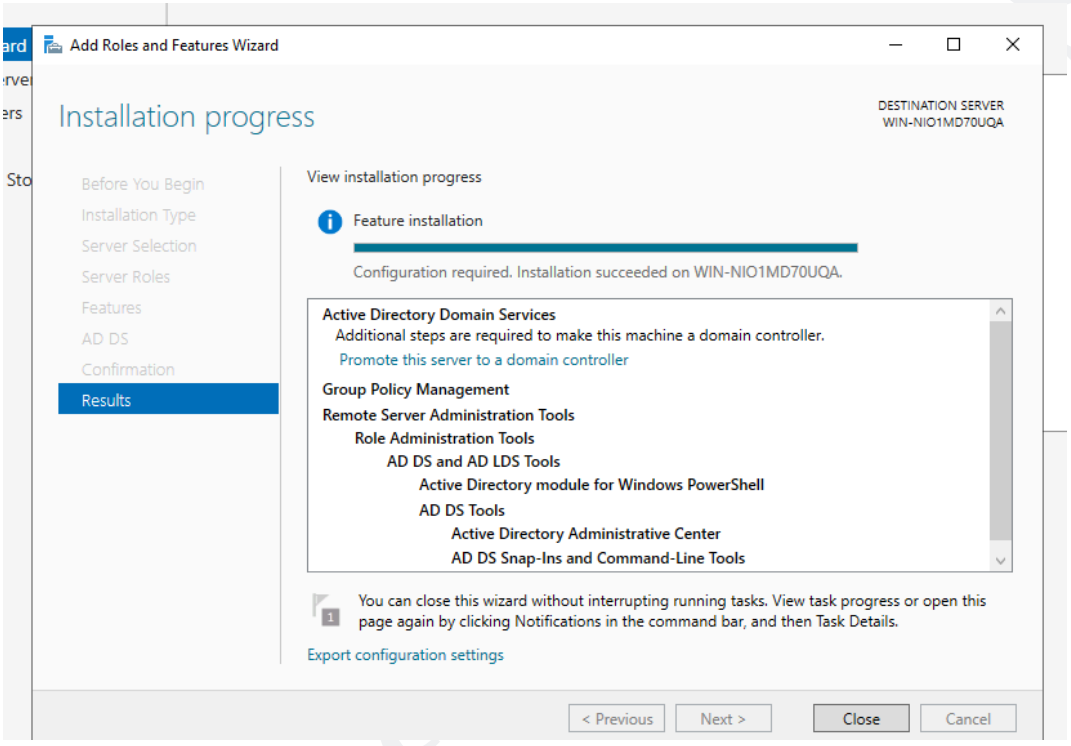
Key Configuration Screenshots:

- 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)**

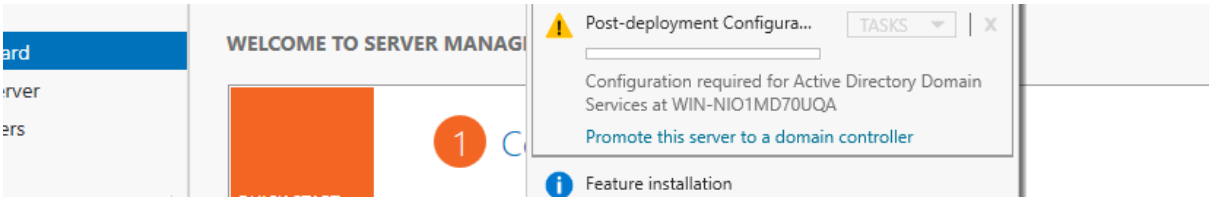
1. Install AD DS Role:



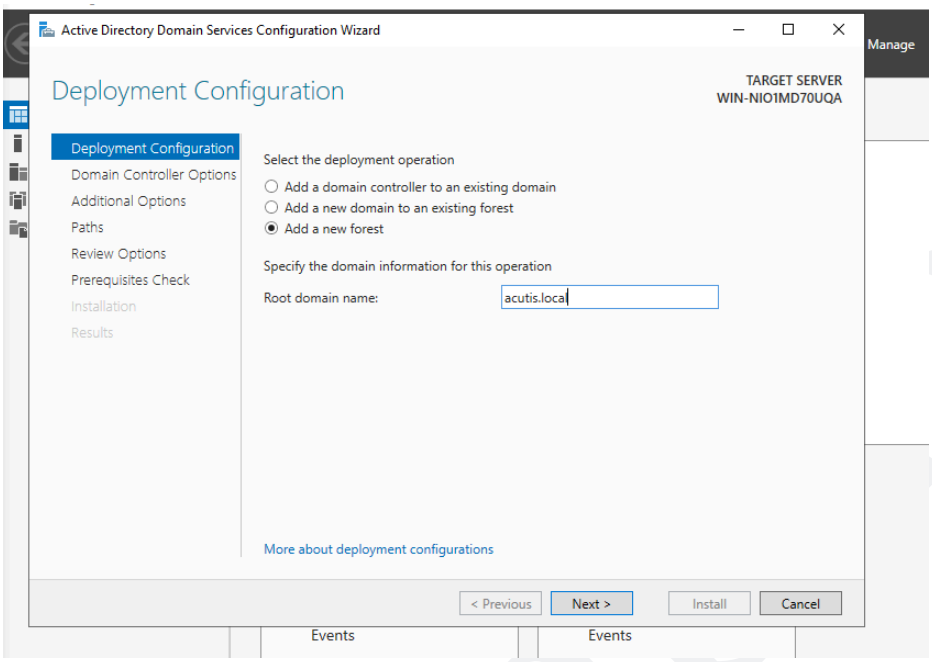


Promote the Server to a Domain Controller:

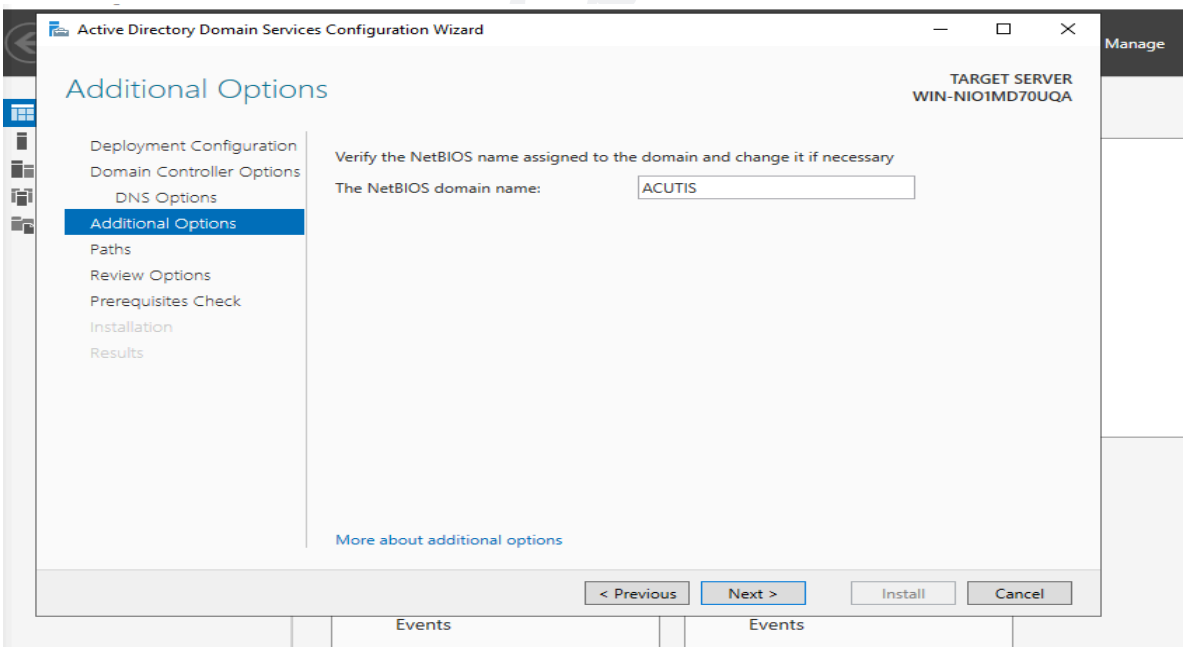
After installation, click the **Promote this server to a domain controller** link.

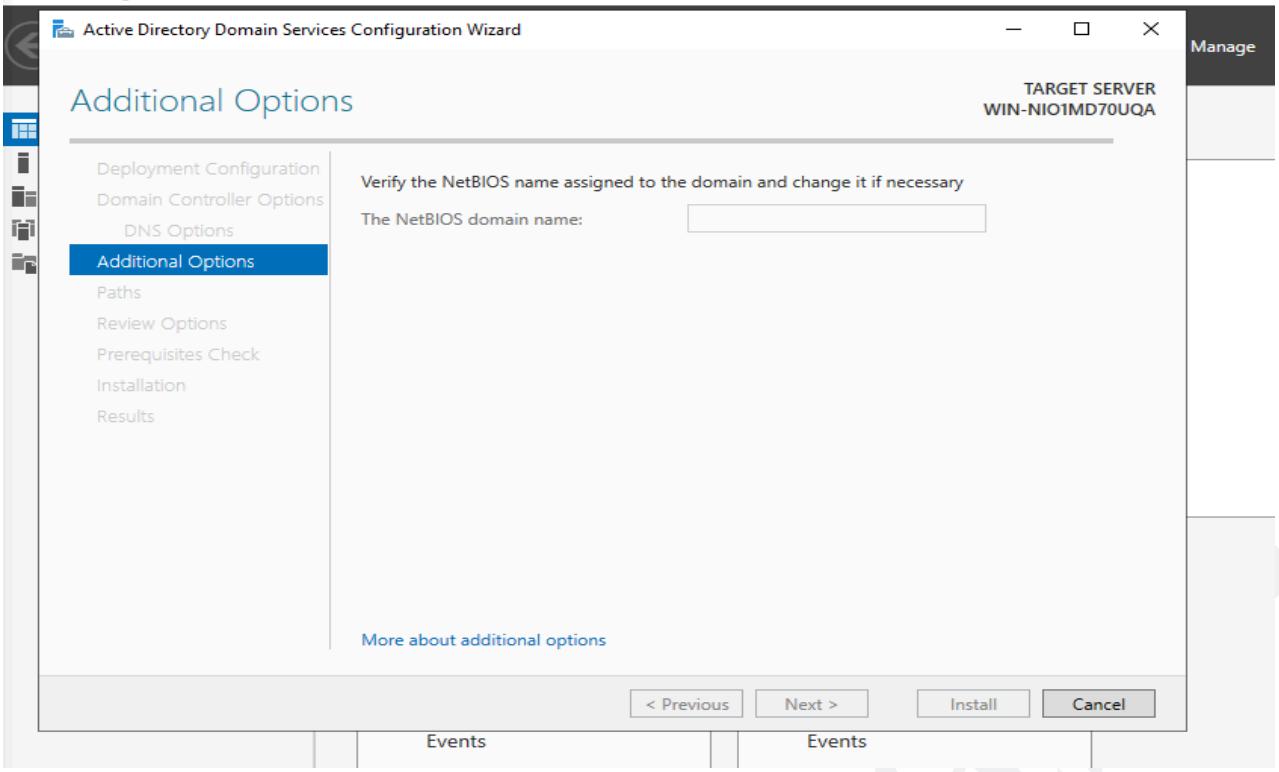


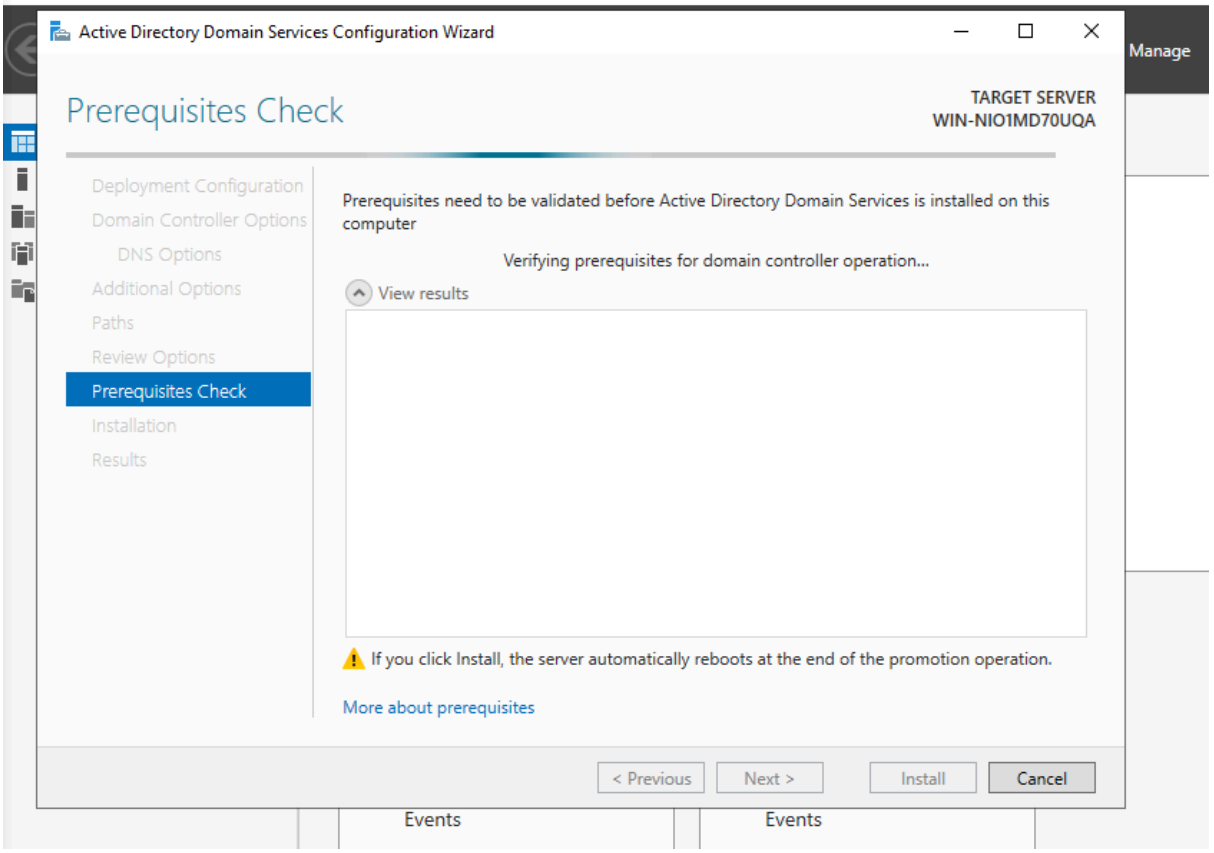
Root domain name was setup as : **acutis.local**

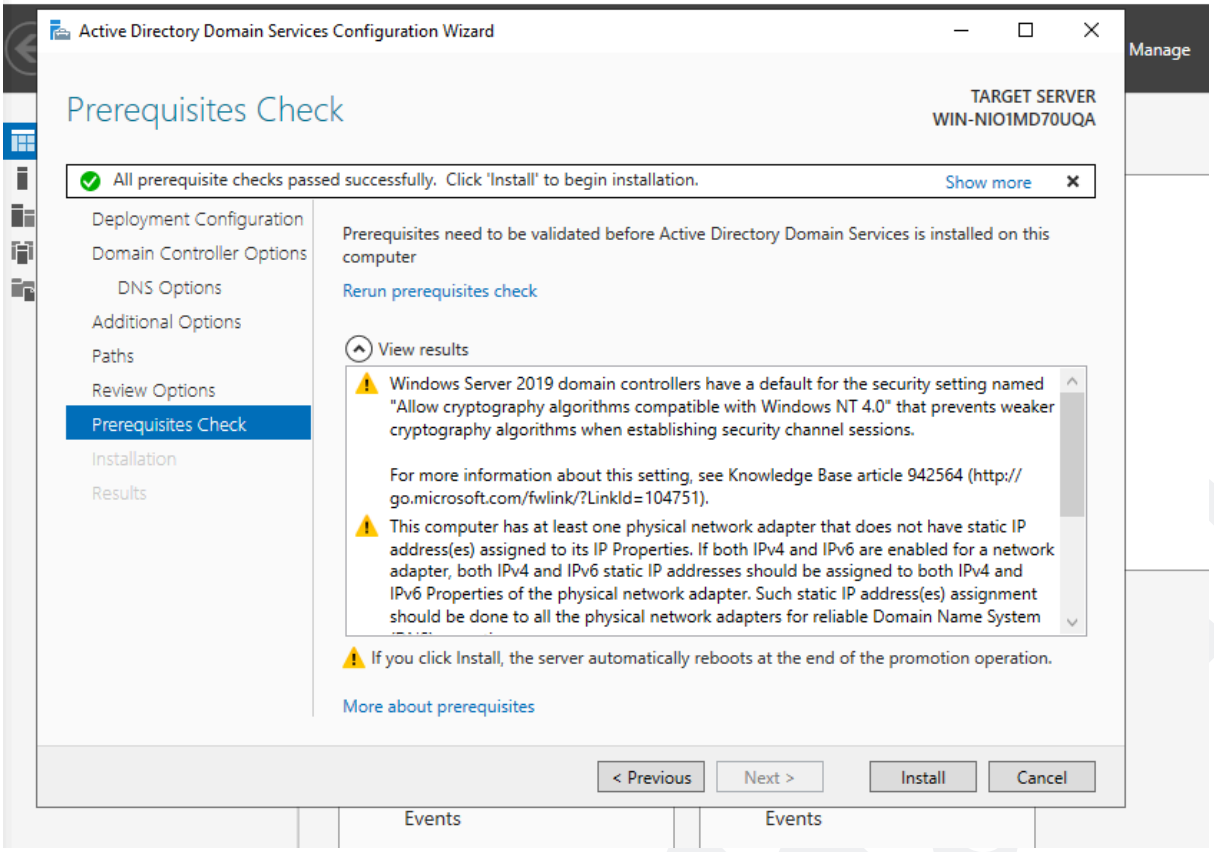


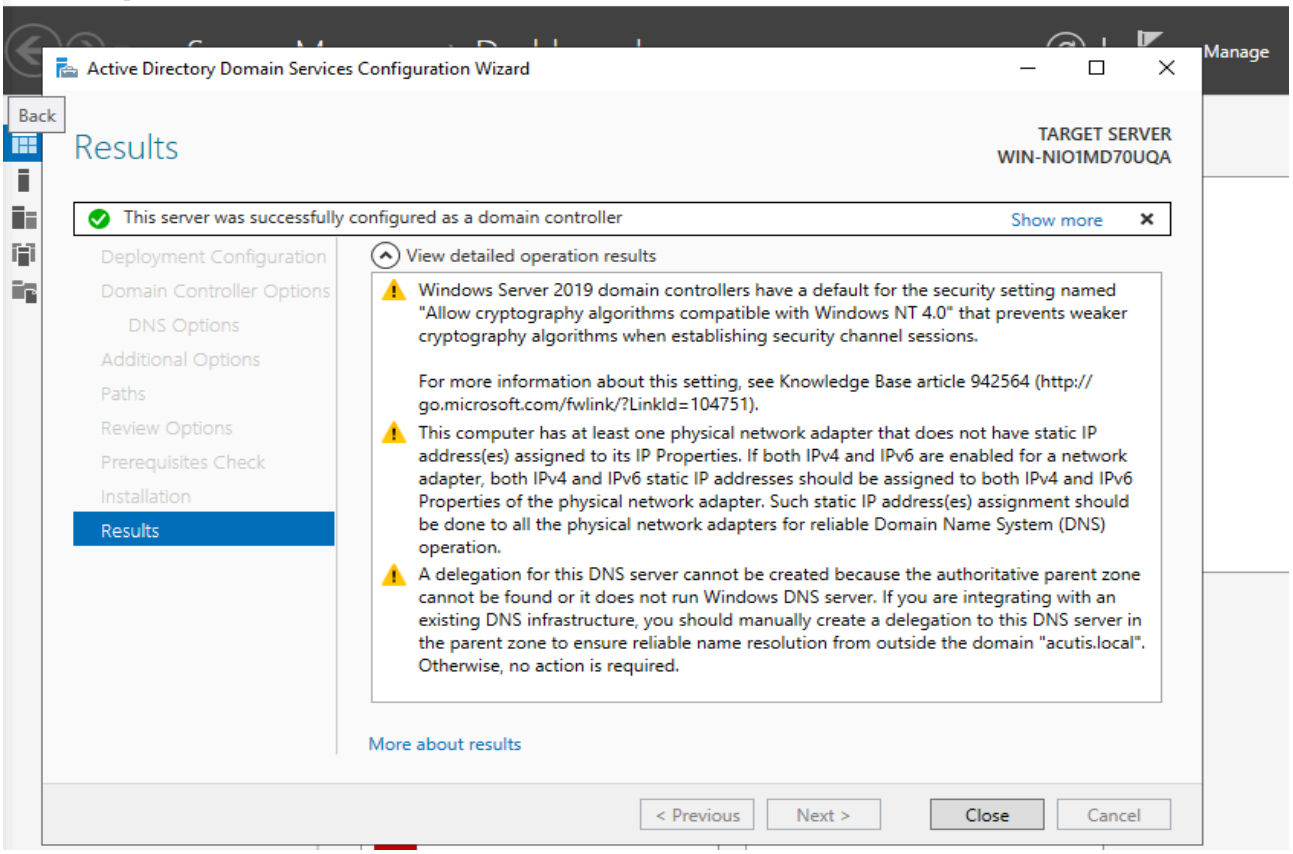
Follow the wizard, setting up the Directory Services Restore Mode (DSRM) password.




Active Directory Domain Services Configuration Wizard
Manage
Additional Options
TARGET SERVER
WIN-NIO1MD70UQA
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
More about additional options
< Previous
Next >
Install
Cancel
Events
Events

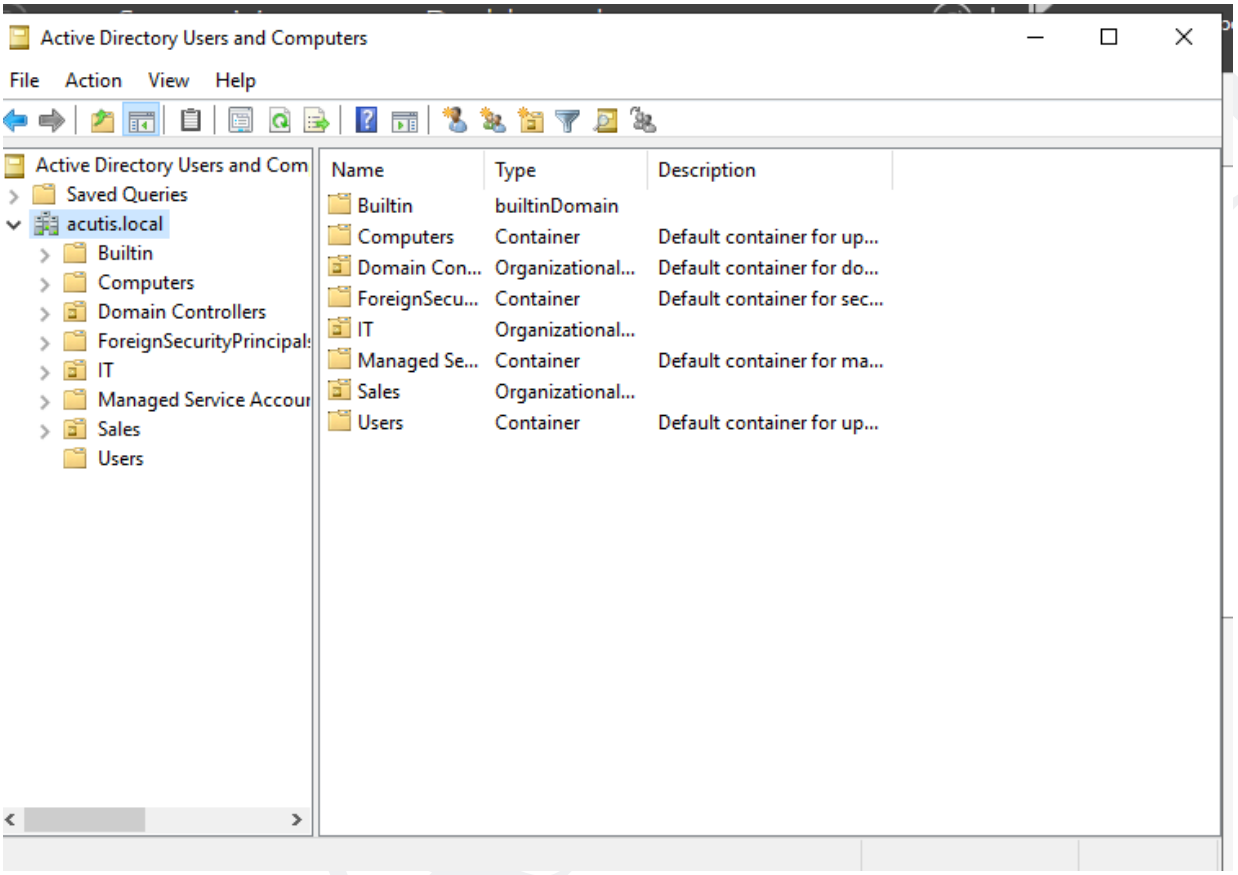

Active Directory Domain Services Configuration Wizard
Manage
Prerequisites Check
TARGET SERVER
WIN-NIO1MD70UQA
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active 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
< Previous
Next >
Install
Cancel
Events
Events

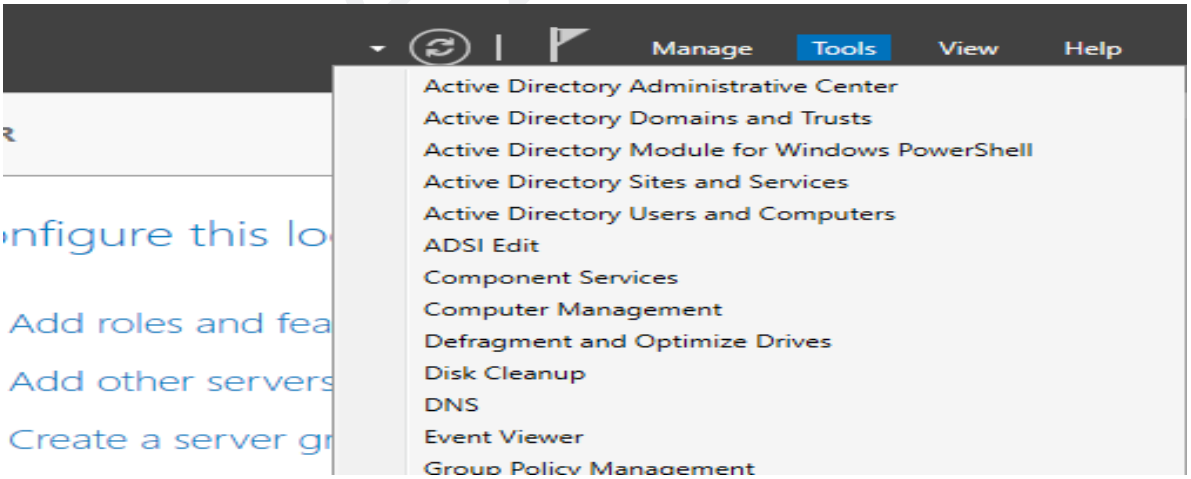

Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
WIN-NIO1MD70UQA
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
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
< Previous
Next >
Install
Cancel
Manage
Events
Events

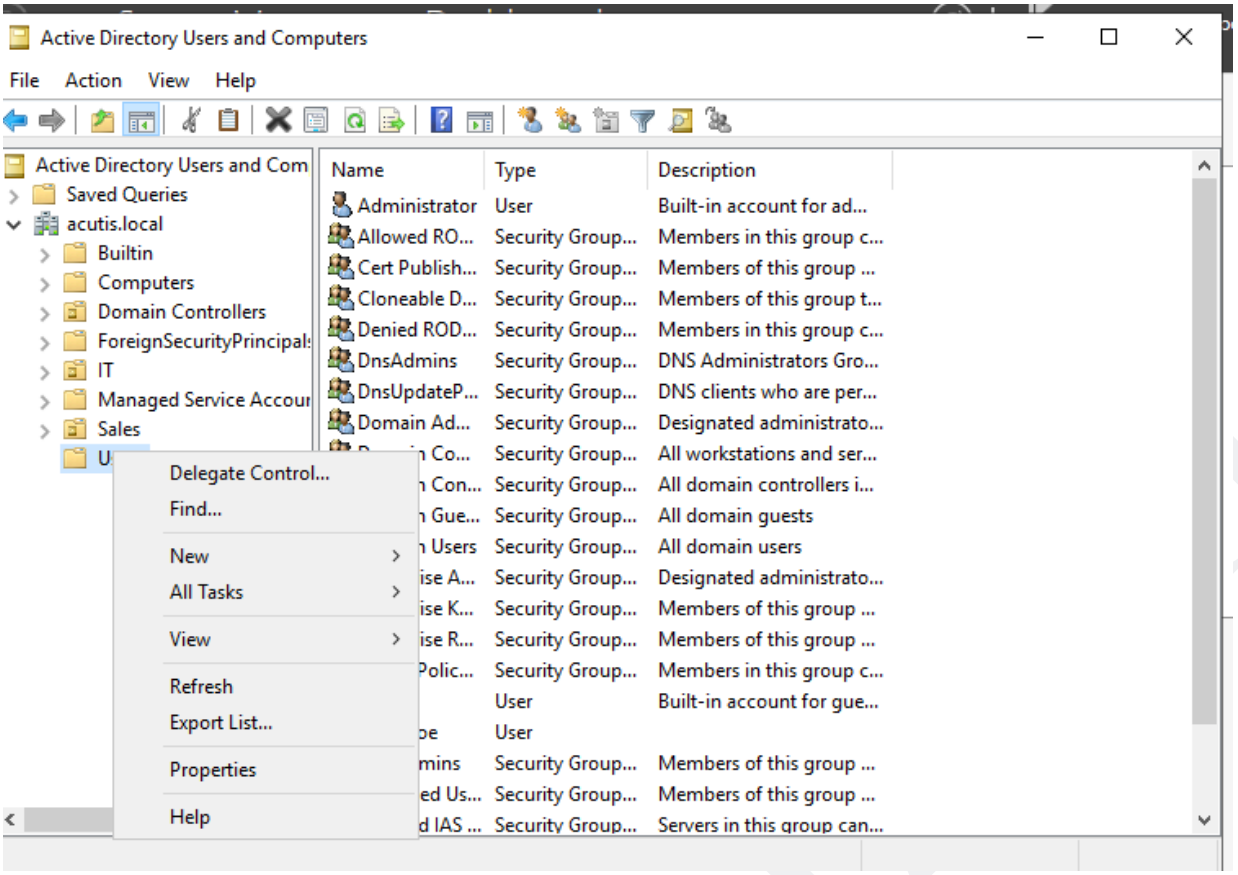

Active Directory Domain Services Configuration Wizard
Back
Results
TARGET SERVER
WIN-NIO1MD70UQA
This server was successfully configured as a domain controller
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
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
< Previous
Next >
Close
Cancel
Manage

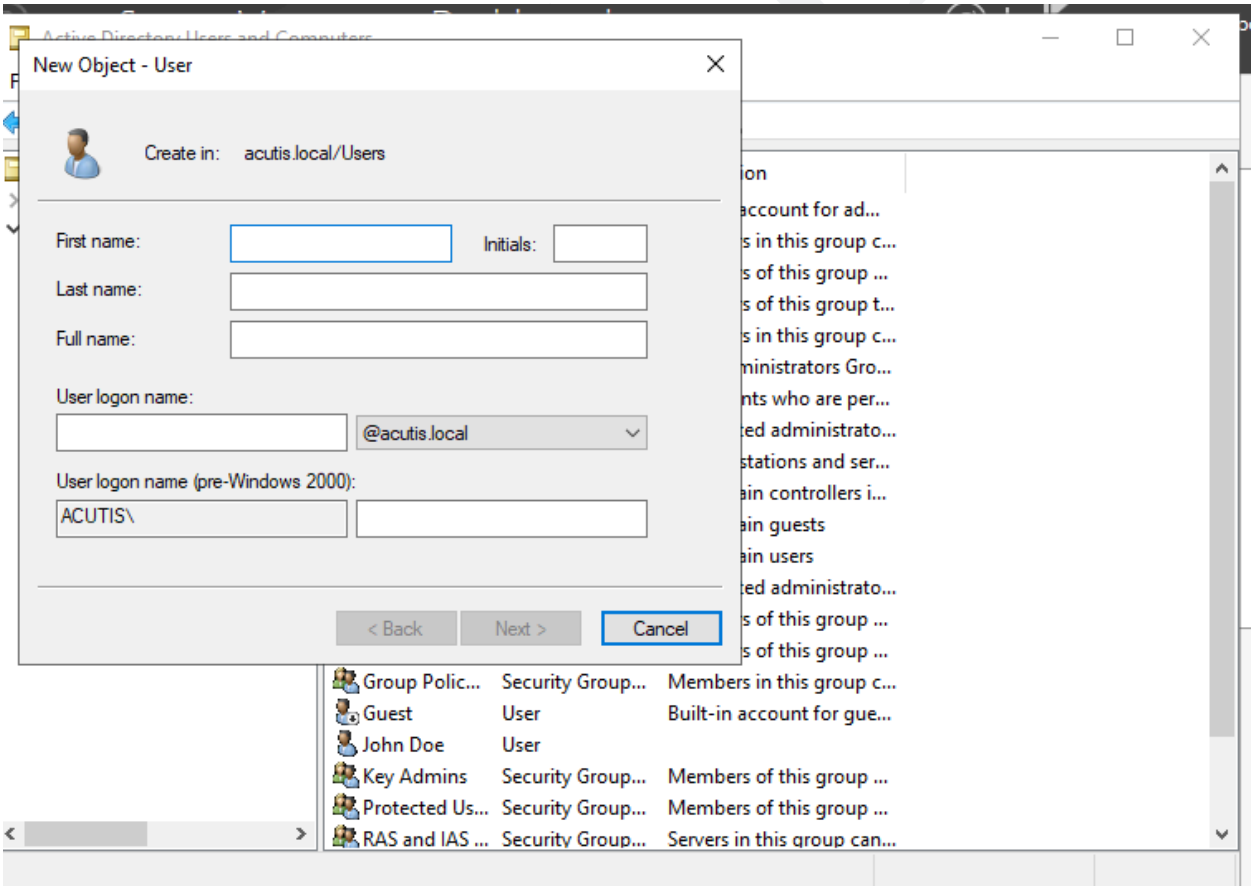
5.2 Create a User in Active Directory

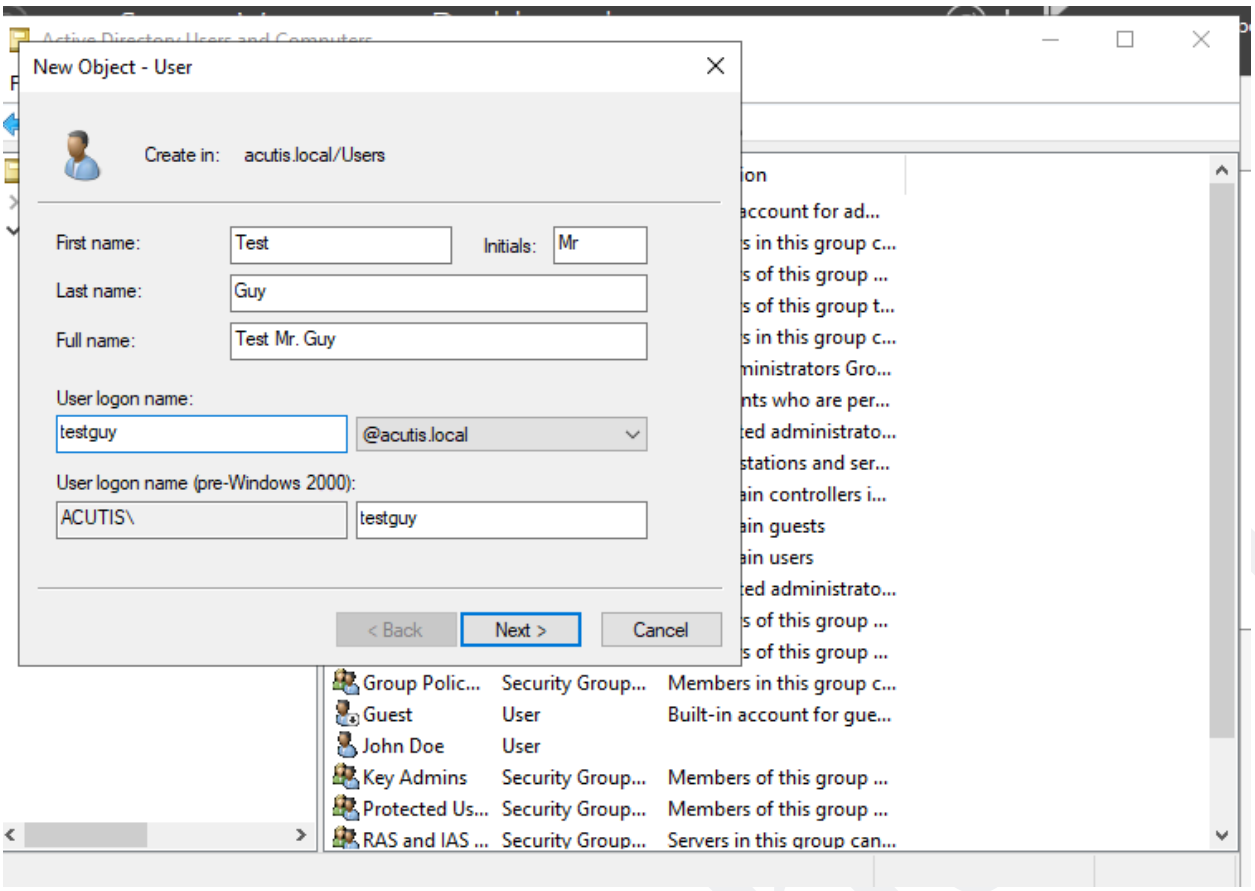
- Open Active Directory Users and Computers (ADUC) from the Start menu.
- Create a user:
  - Enter user details (e.g., John.Doe).
  - Set Password

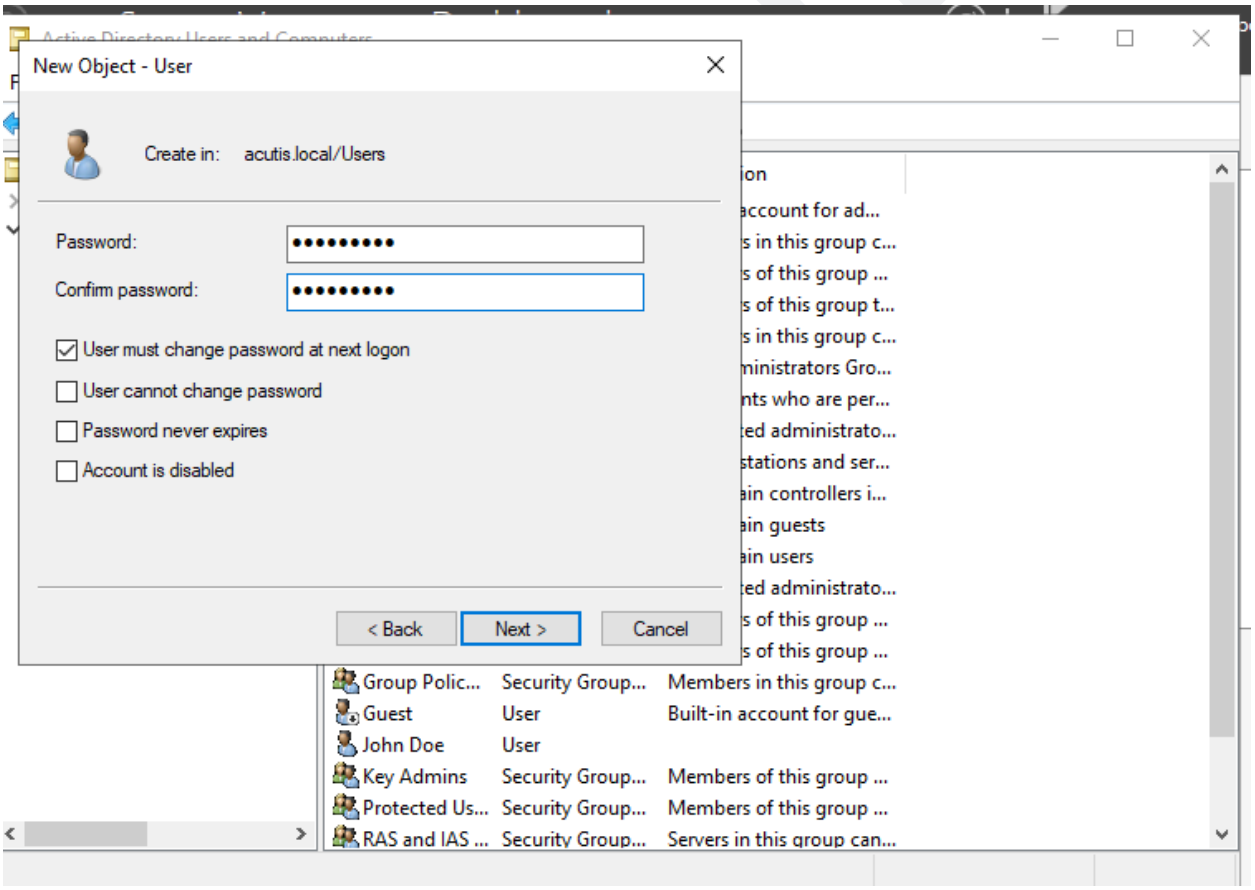


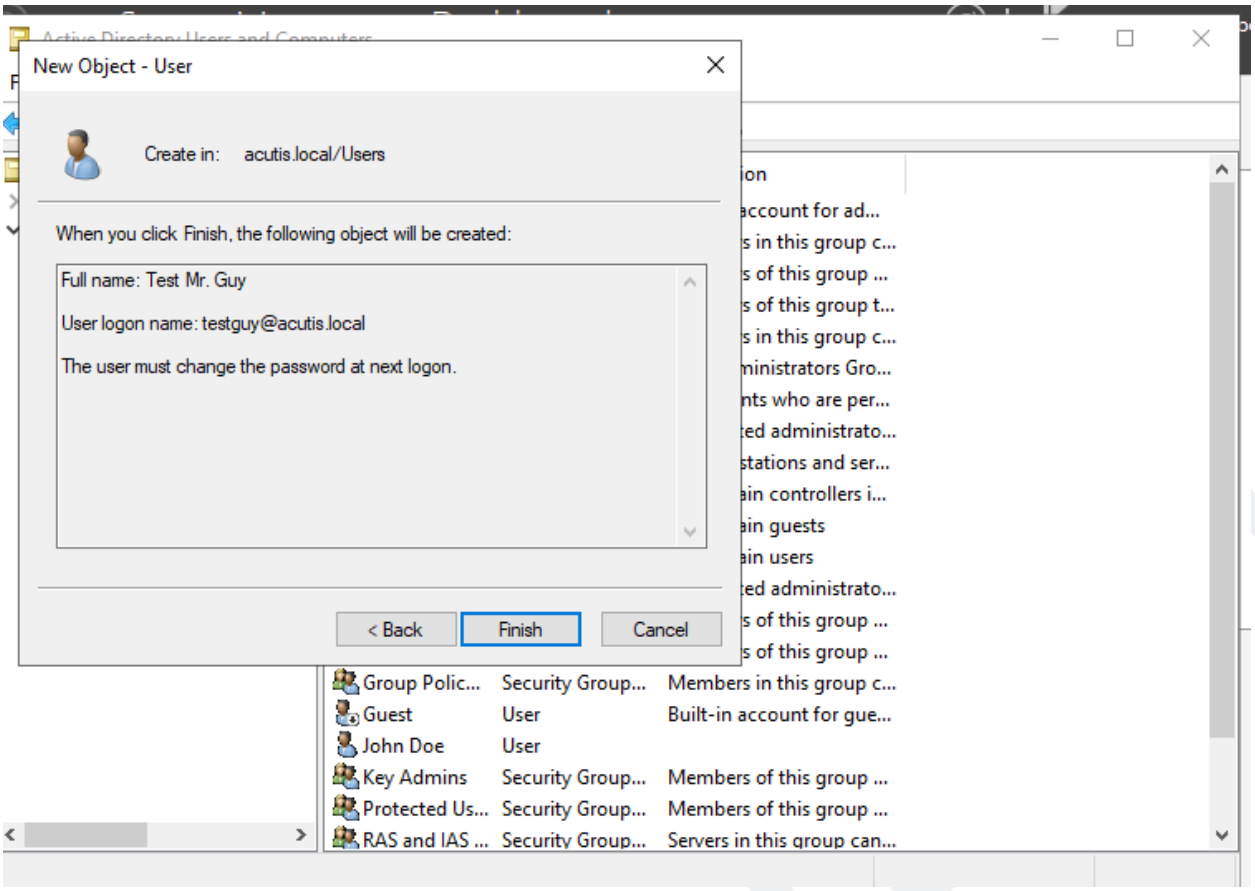



Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
acutis.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
IT
Managed Service Accou
Sales
Name Type Description
Administrator User Built-in account for ad...
Allowed RO... Security Group... Members in this group c...
Cert Publish... Security Group... Members of this group ...
Cloneable D... Security Group... Members of this group t...
Denied ROD... Security Group... Members in this group c...
DnsAdmins Security Group... DNS Administrators Gro...
DnsUpdateP... Security Group... DNS clients who are per...
Domain Ad... Security Group... Designated administrato...
Delegate Control...
Find...
New
All Tasks
View
Refresh
Export List...
Properties
Help

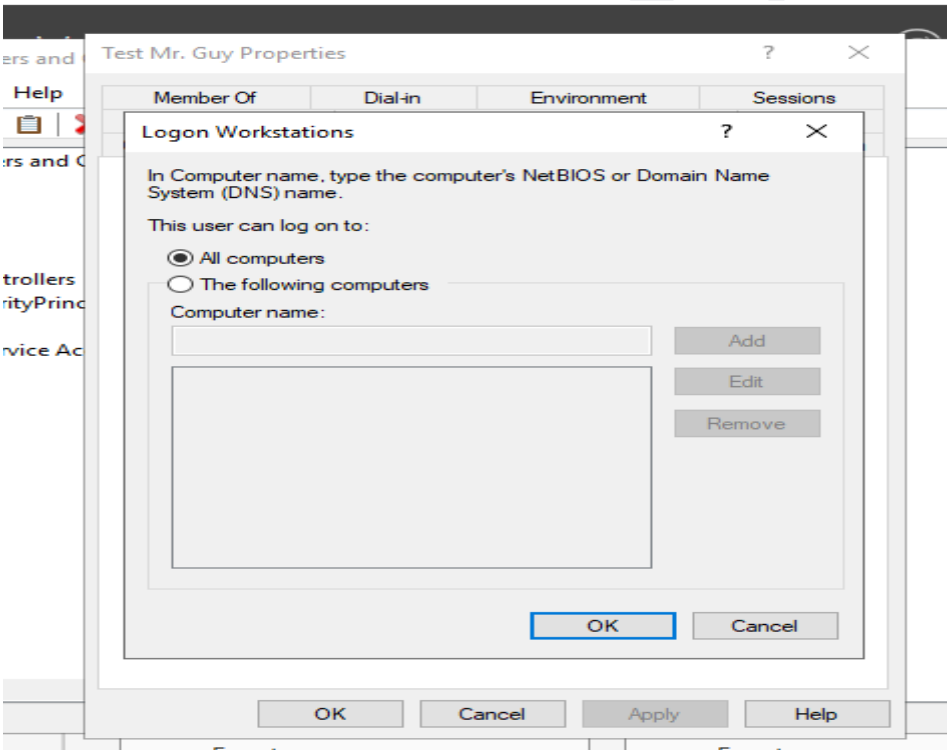

New Object - User
Create in: acutis.local/Users
First name:
Initials:
Last name:
Full name:
User logon name:
@acutis.local
User logon name (pre-Windows 2000):
ACUTIS\
< Back
Next >
Cancel
Group Polic... Security Group... Members in this group c...
Guest User Built-in account for gue...
John Doe User
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...


New Object - User
Create in: acutis.local/Users
First name: Test
Initials: Mr
Last name: Guy
Full name: Test Mr. Guy
User logon name:
testguy
@acutis.local
User logon name (pre-Windows 2000):
ACUTIS\
testguy
< Back
Next >
Cancel
Group Polic... Security Group... Members in this group c...
Guest User Built-in account for gue...
John Doe 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...

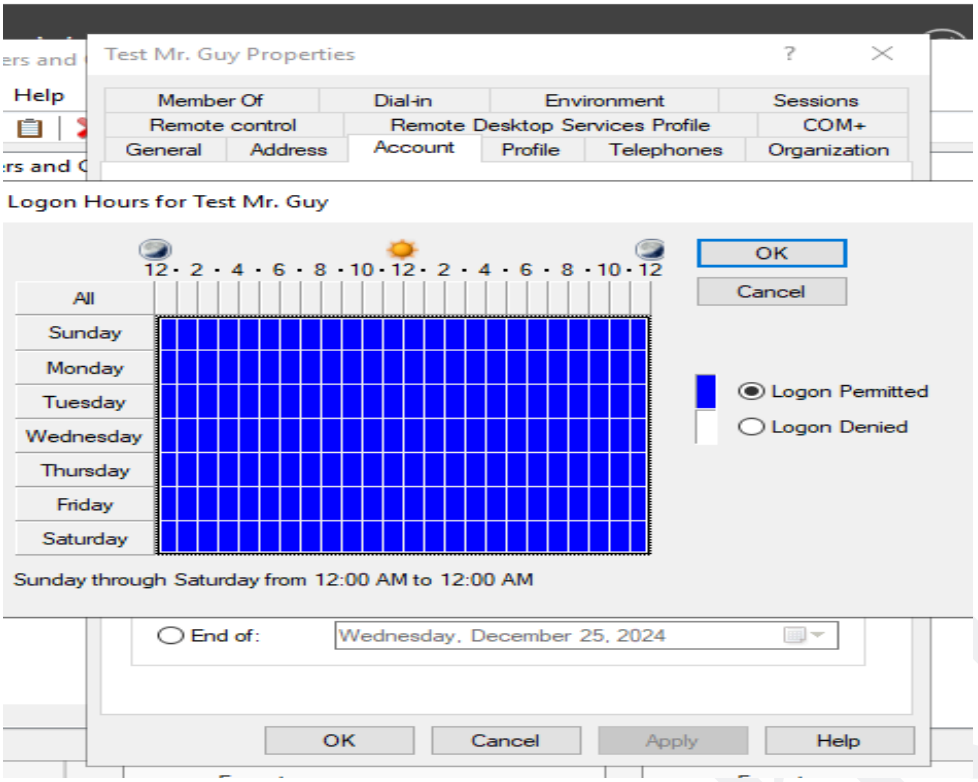

New Object - User
Create in: acutis.local/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel
Group Polic... Security Group... Members in this group c...
Guest User Built-in account for gue...
John Doe 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...

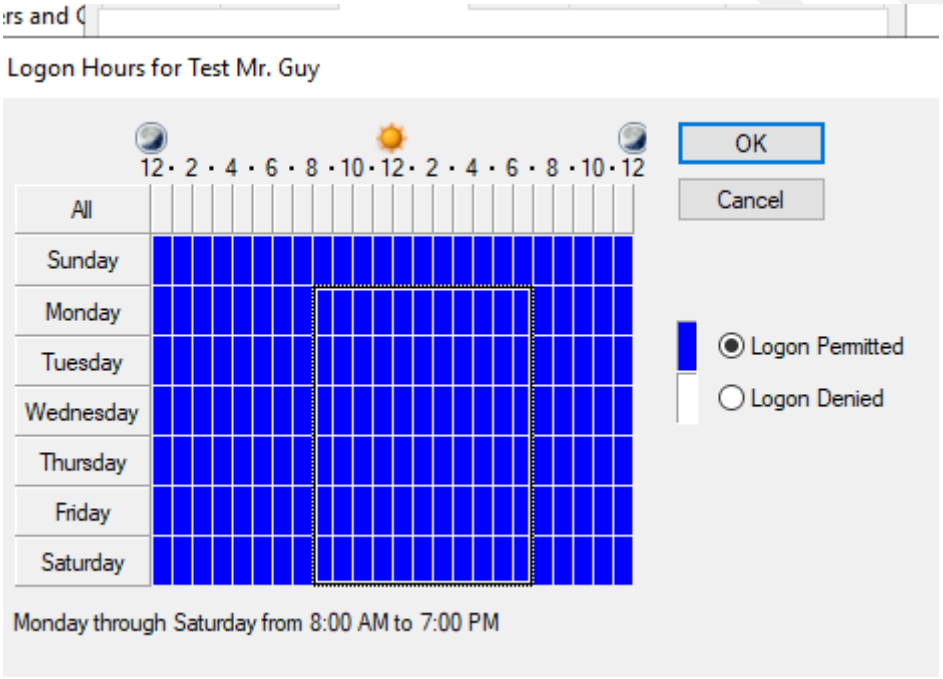


- **Limit the Computers a User Can Log On To**
  - Specify the computers the user is allowed to log on to.

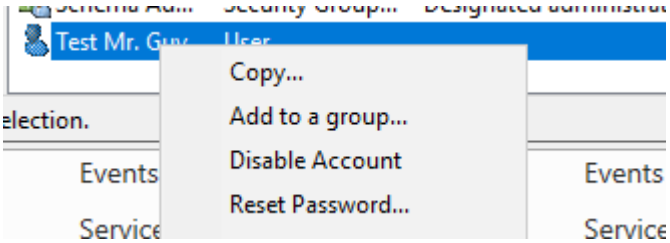


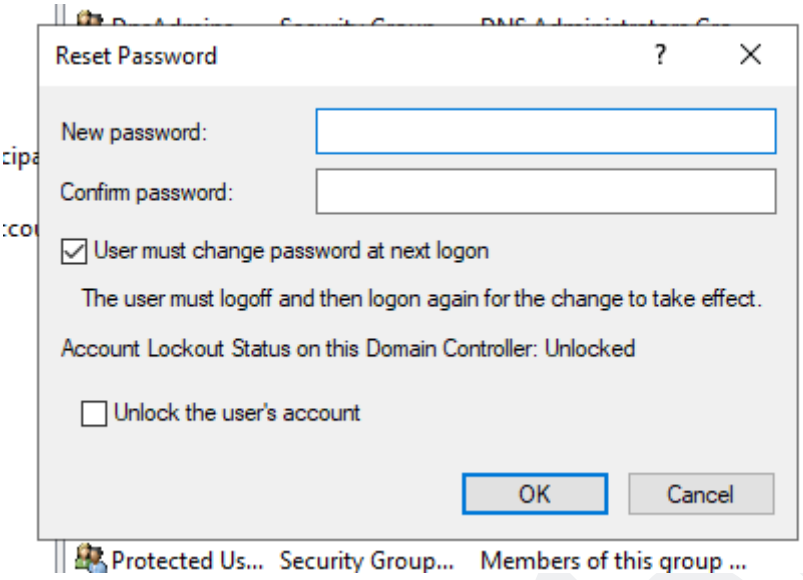
- **Limit the Logon Hours for a User**
  - Use the grid to set allowed logon times and block unauthorized hours.



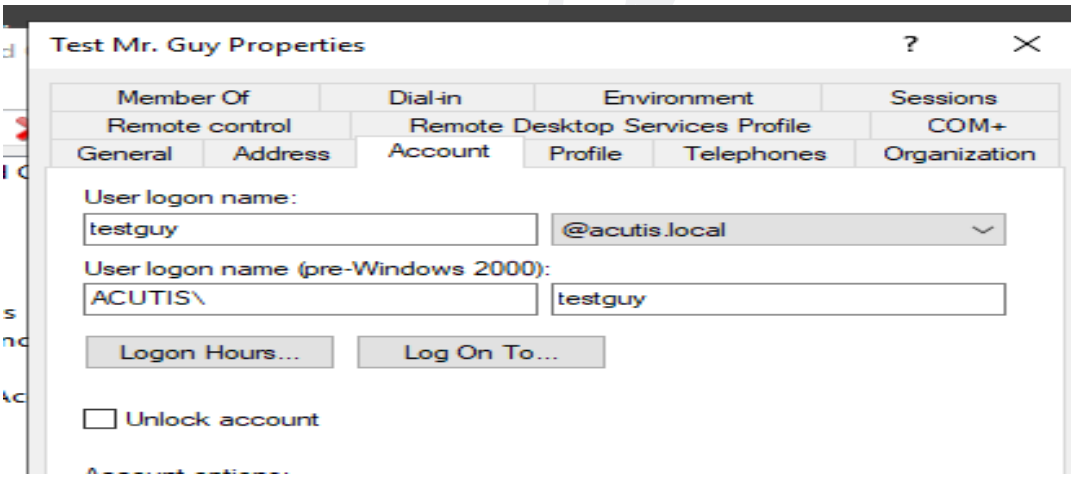


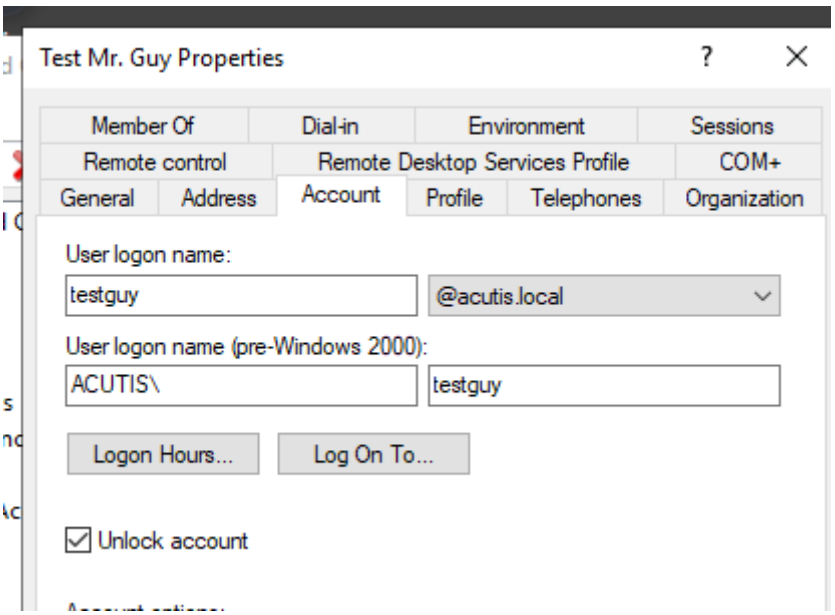
- **Reset a User’s Password**
  - Enter the new password and configure additional options as needed.



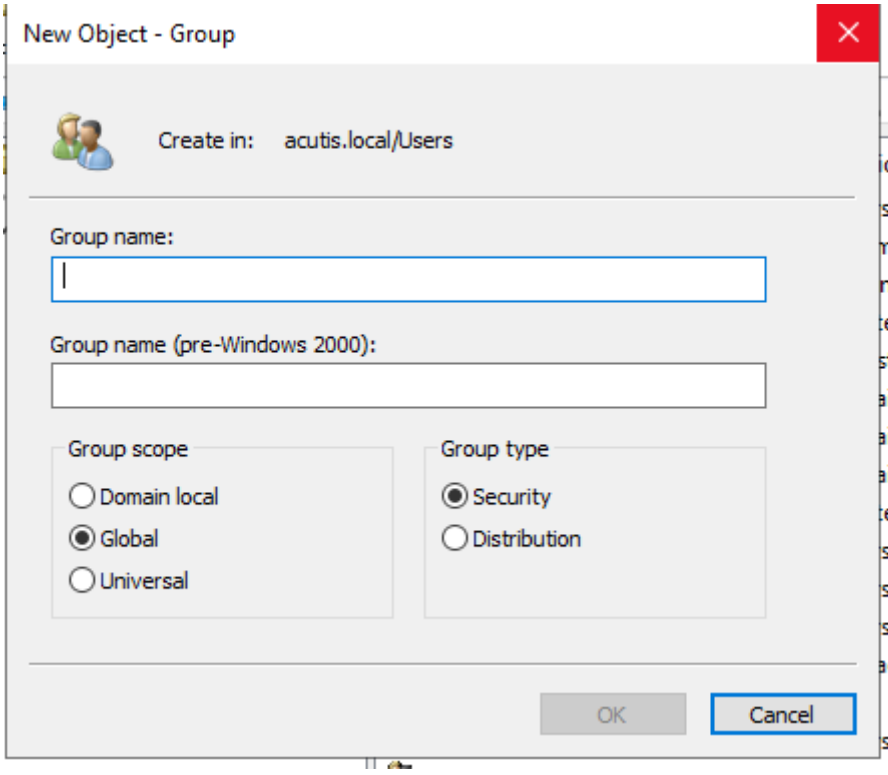


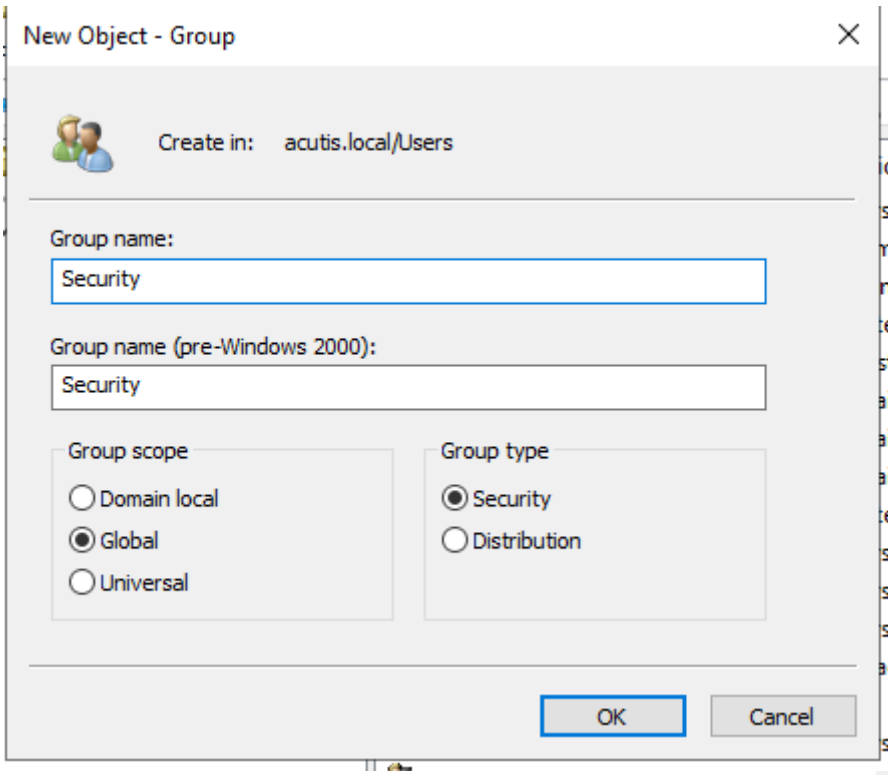
- **Unlock or Enable an Account in Active Directory**
  - If a user account gets locked,Under the **Account** tab, uncheck **Account is locked out**.

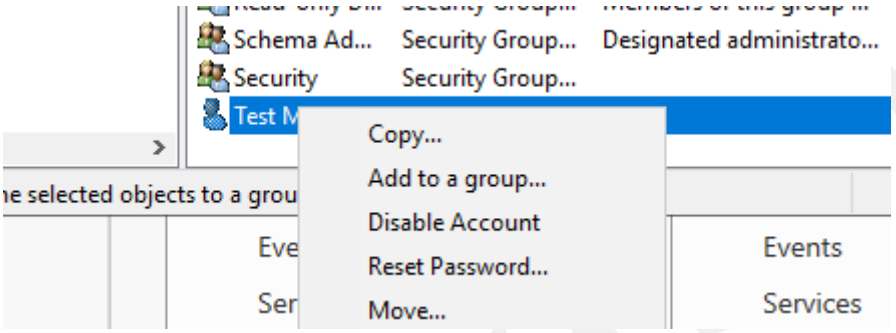


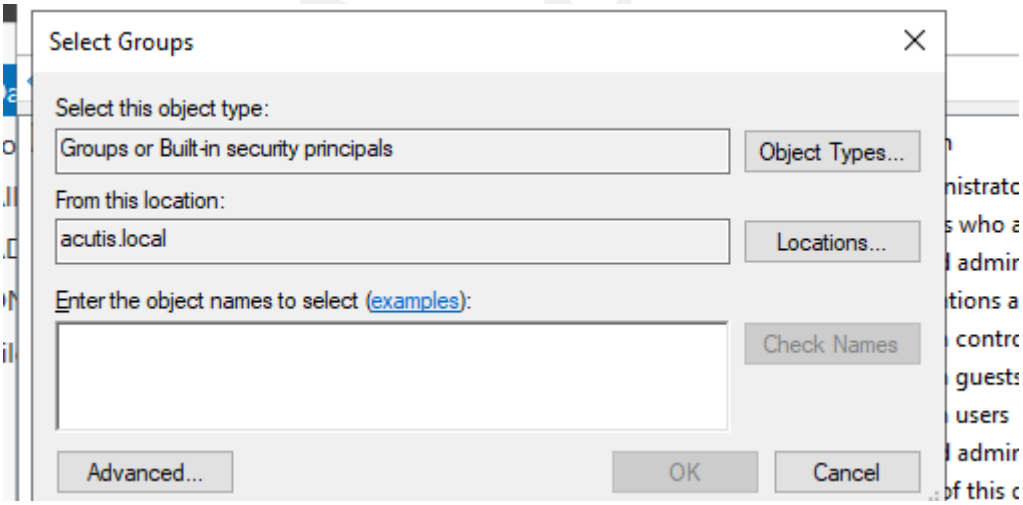


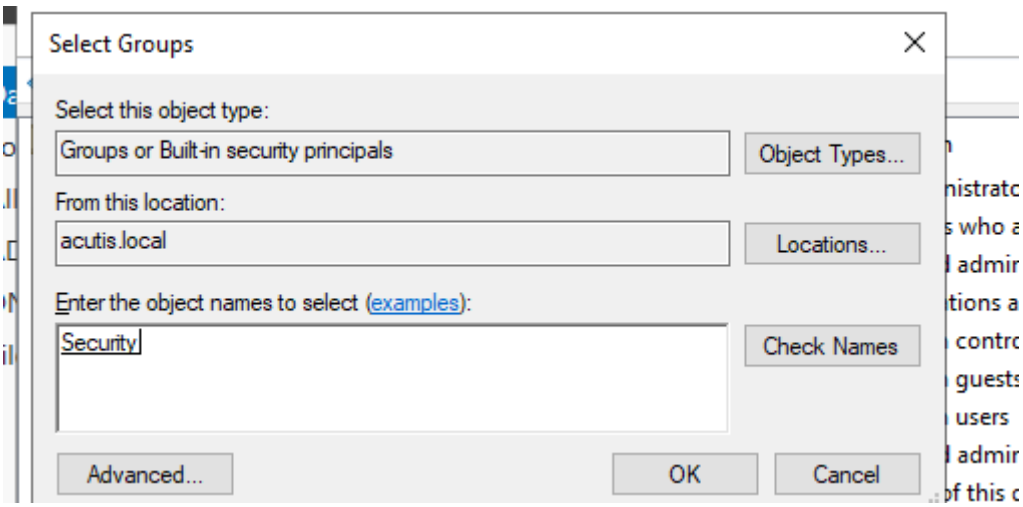
- **Manage User Accounts and Groups**
  - Create different Groups as requirements (e.g: Security)
  - Add users to groups:



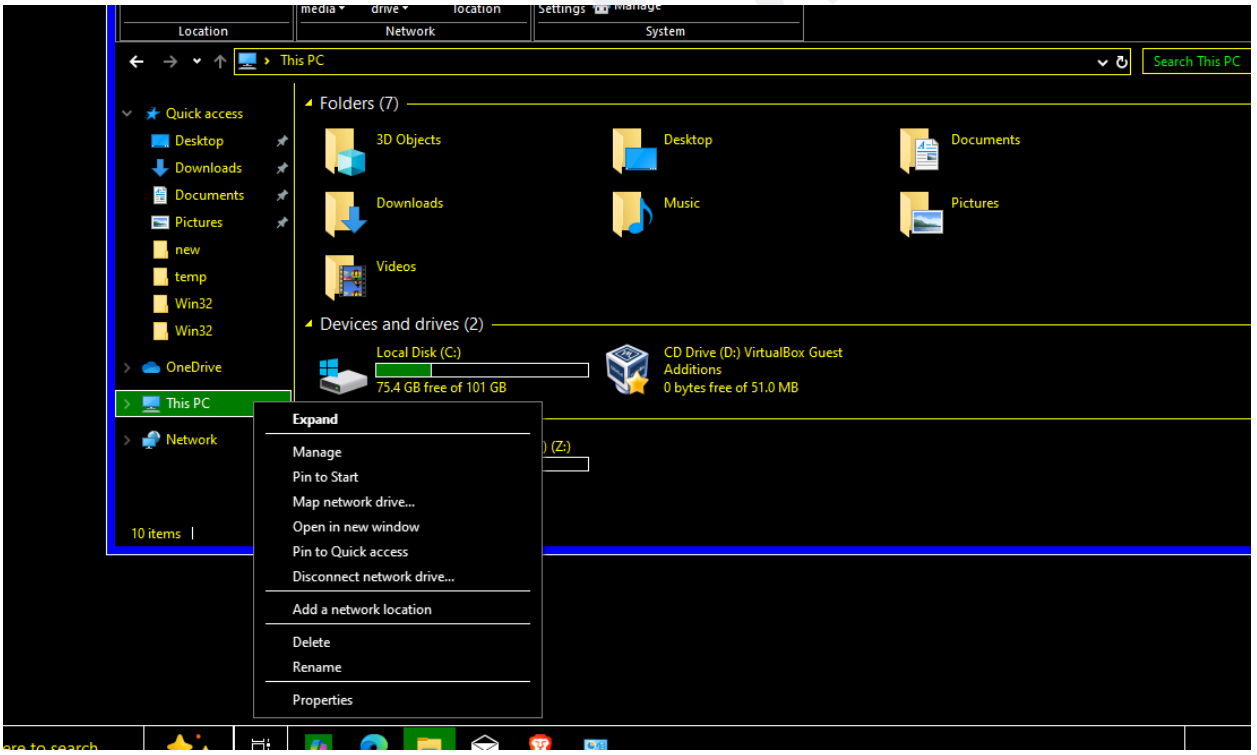

New Object - Group
Create in: acutis.local/Users
Group name:
Security
Group name (pre-Windows 2000):
Security
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
OK
Cancel

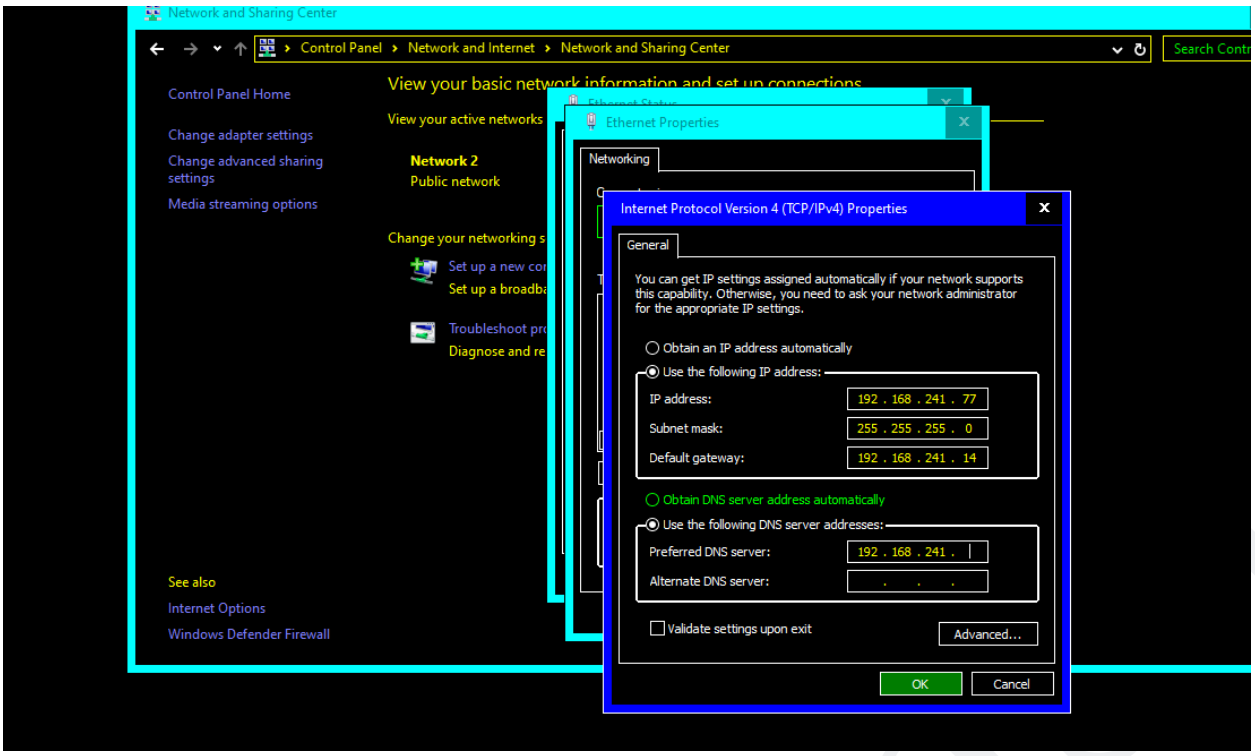

Schema Ad...
Security Group...
Designated administrato...
Security
Security Group...
Test M
Copy...
Add to a group...
Disable Account
Reset Password...
Move...
Events
Services

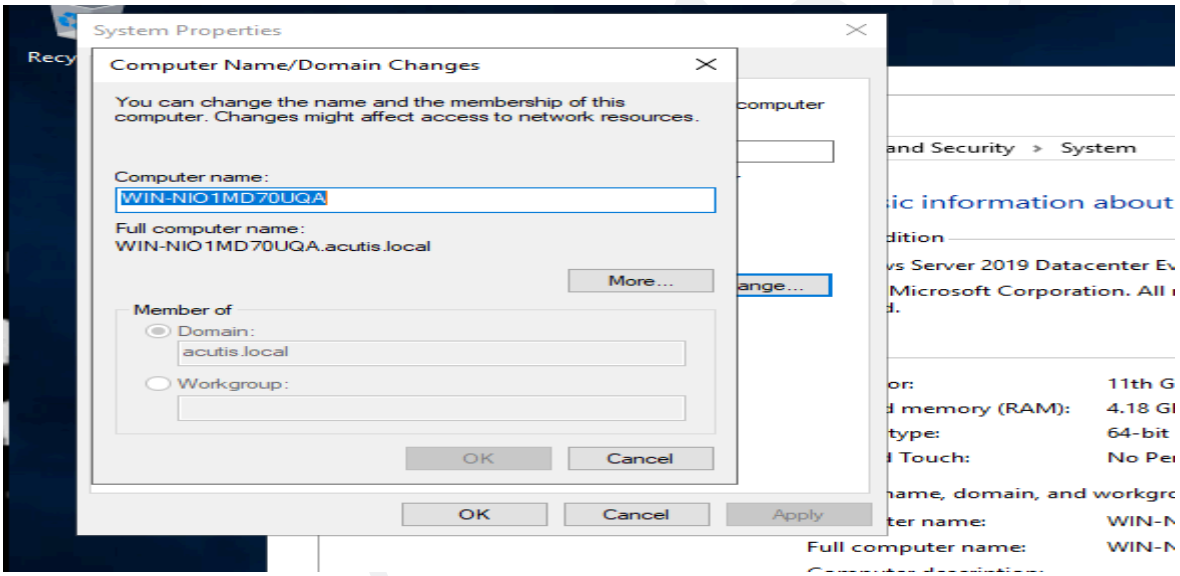

Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
acutis.local
Locations...
Enter the object names to select (examples):
Check Names
Advanced...
OK
Cancel



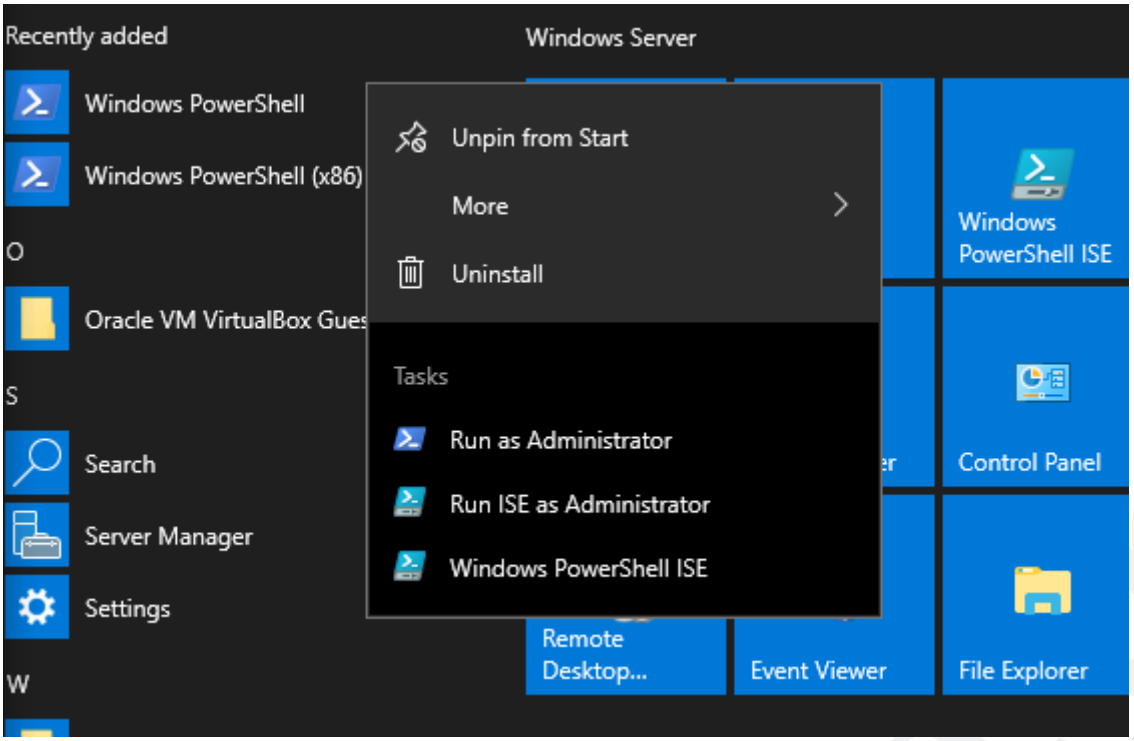
- **Manage Computer Accounts and Organizational Units (OUs)**
  - Add computers to AD:
    - Open **System Properties** on a client computer and Join the computer to the domain by providing domain admin credentials.
  - Organize OU's:
    - Create OUs in ADUC for computers, users, or groups.
    - Move objects (e.g., computers, users) into respective OUs by dragging and dropping them.

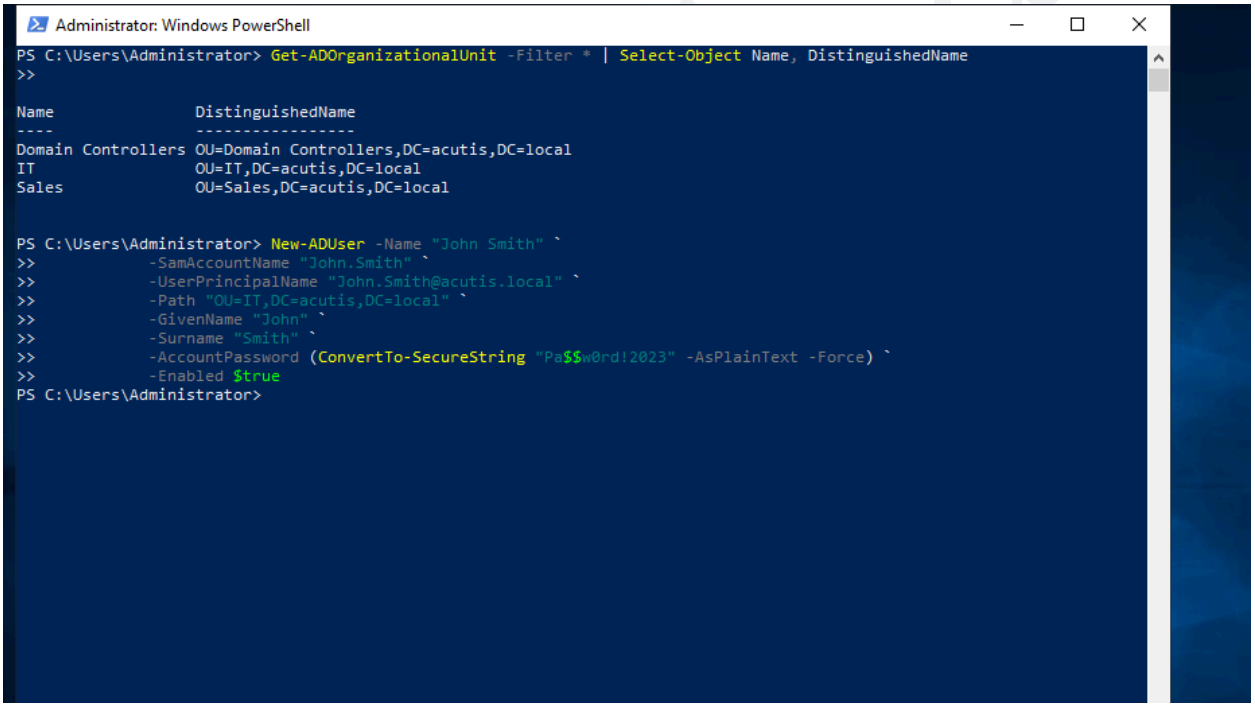






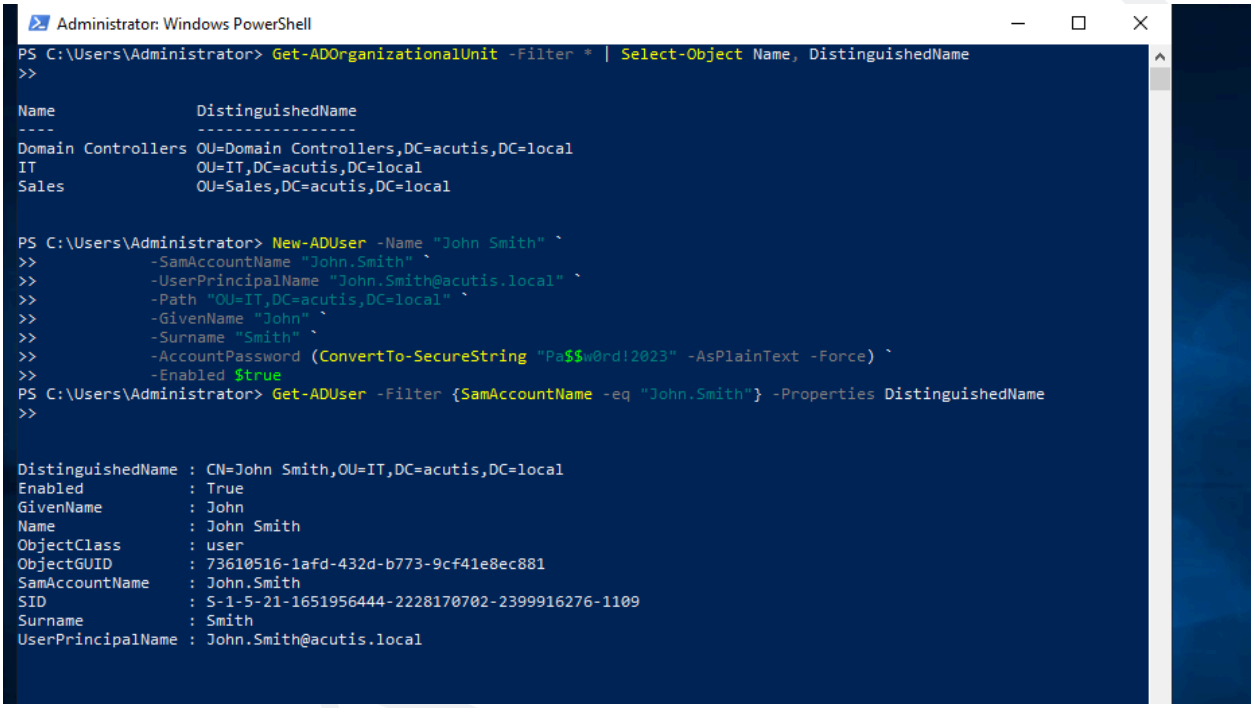
- **Use PowerShell for AD Administration**
  - Open PowerShell as an administrator.
  - Use cmdlets to automate tasks:


Recently added
Windows Server
Windows PowerShell
Windows PowerShell (x86)
O
Oracle VM VirtualBox Gues
S
Search
Server Manager
Settings
W
Unpin from Start
More
Uninstall
Tasks
Run as Administrator
Run ISE as Administrator
Windows PowerShell ISE
Windows PowerShell ISE
Control Panel
Remote Desktop...
Event Viewer
File Explorer

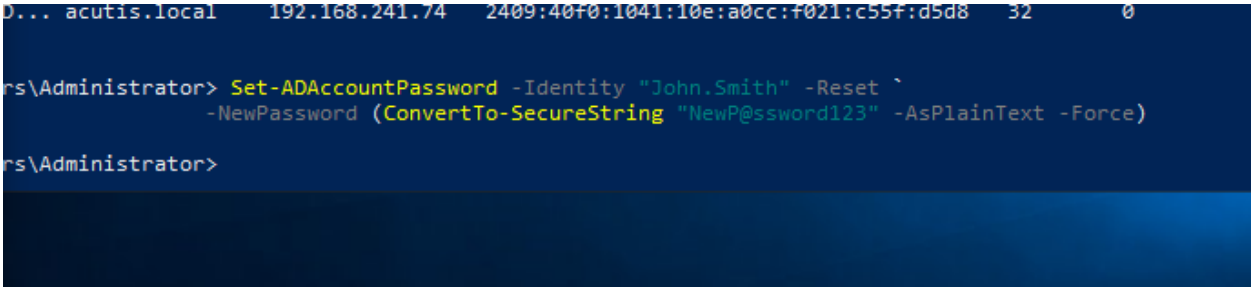

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter * | Select-Object Name, DistinguishedName
>>
Name DistinguishedName
---- -----------------
Domain Controllers OU=Domain Controllers,DC=acutis,DC=local
IT OU=IT,DC=acutis,DC=local
Sales OU=Sales,DC=acutis,DC=local
PS C:\Users\Administrator> New-ADUser -Name "John Smith" `
>> -SamAccountName "John.Smith" `
>> -UserPrincipalName "John.Smith@acutis.local" `
>> -Path "OU=IT,DC=acutis,DC=local" `
>> -GivenName "John" `
>> -Surname "Smith" `
>> -AccountPassword (ConvertTo-SecureString "Pa$$w0rd!2023" -AsPlainText -Force) `
>> -Enabled $true
PS C:\Users\Administrator>

```
New-ADUser -Name "John Smith" `
        -SamAccountName "John.Smith" `
        -UserPrincipalName "John.Smith@acutis.local" `
        -Path "CN=Users,DC=acutis,DC=local" `
        -AccountPassword (ConvertTo-SecureString "P@ssword123" -AsPlainText -Force) `
        -Enabled $true
```

- **Details of John Smith:**



- **Change Password:**



- **Unlock Account:**

```
rs\Administrator> Set-ADAccountPassword -Identity "John.Smith" -Reset `
                  -NewPassword (ConvertTo-SecureString "NewP@ssword123" -AsPlainText -Force)

rs\Administrator> Unlock-ADAccount -Identity "John.Smith"

rs\Administrator>
```

- **Add a User to a Group**

```
                  -NewPassword (ConvertTo-SecureString "NewP@ssword123" -AsPlainText -Force)

rs\Administrator> Unlock-ADAccount -Identity "John.Smith"

rs\Administrator> Add-ADGroupMember -Identity "Security" -Members "John.Smith"

rs\Administrator>
```

- **Remove a user from group**

```
rs\Administrator> Remove-ADGroupMember -Identity "Security" -Members "John.Smith" -Confirm:$false

rs\Administrator>
```

- **View All Users in AD**

```
PS C:\Users\Administrator> Get-ADUser -Filter * -Properties DisplayName, EmailAddress | Select-Object DisplayNa
me, EmailAddress
>>

DisplayName  EmailAddress
-----------  ------------



John Doe
Test Mr. Guy
```

- List Group Members

```
PS C:\Users\Administrator> Get-ADGroupMember -Identity "Security"
>>


distinguishedName : CN=Test Mr. Guy,CN=Users,DC=acutis,DC=local
name              : Test Mr. Guy
objectClass       : user
objectGUID        : 81f89442-26a8-4653-91aa-3f0c0cd6e8d0
SamAccountName    : testguy
SID               : S-1-5-21-1651956444-2228170702-2399916276-1107
```

- Check Account Lockout Status

```
PS C:\Users\Administrator> Get-ADUser -Identity "John.Smith" -Properties LockedOut | Select-Object Name, Locked
Out
>>

Name       LockedOut
----       ---------
John Smith     False


PS C:\Users\Administrator>
```

5. Challenges and Resolutions

1. **Networking Issues**:
   - Initially, the virtual machine had limited connectivity due to incorrect adapter settings.
   - Resolution: Configured the bridged adapter in VirtualBox for proper network connectivity.
2. **Logon Restrictions Not Working Properly**:
   - Resolution: Verified settings and ensured all user accounts synced correctly across the domain controllers.
3. **PowerShell Scripting Errors**:
   - Resolution: Referred to the official PowerShell documentation and used Get-Help to resolve errors.

6. Conclusion

The project successfully demonstrated the setup and management of an Active Directory environment. Through hands-on tasks like creating user accounts, enforcing restrictions, and leveraging PowerShell, a deep understanding of AD's capabilities was gained. The challenges encountered enhanced troubleshooting skills, preparing for real-world enterprise scenarios.

7. References

Microsoft Documentation:

- Active Directory Domain Services Overview:

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

- PowerShell cmdlets for Active Directory:

https://learn.microsoft.com/en-us/powershell/module/activedirectory/

Online Tutorials:

- TechNet Forum Discussions for troubleshooting AD DS issues.
- Practical guidance from YouTube tutorials for AD DS setup and PowerShell scripting.

Oracle VirtualBox Documentation:

- Bridged Adapter Configuration: VirtualBox Networking