TOPIC: SECURING ACTIVE DIRECTORY DOMAIN SERVICES

Objective:

The objective of Module 7 is to secure the Active Directory Domain Services (AD DS) environment by configuring account and password policies, delegating precise permissions, implementing administrative controls, deploying Read-Only Domain Controllers (RODCs), and auditing changes. This ensures that user and administrative accounts are protected, group memberships are strictly managed, and all critical directory operations are logged for review and compliance.

Pre-requisites:

- **Environment**: VMware Workstation with six VMs, all joined to the AD DS domain RPSLAB.COM (except LON-RHEL).
- **Main Domain Controller**: LON-DC1 (Windows Server 2016 Datacenter Evaluation GUI).
- **Administrative Privileges**: Access to administrator accounts on Windows Server 2016 and relevant client machines.
- **Active Directory Tools**: Group Policy Management Console, Active Directory Administrative Center, Active Directory Users and Computers.
- **Service Accounts**: Existing IT and administrative user groups.
- **Network Connectivity**: All Windows VMs (except LON-RHEL) connected and able to communicate with LON-DC1.

Topics Covered:

- Implementing security policies for accounts, passwords, and administrative groups
- Deploying and configuring Read-Only Domain Controllers (RODC)
- Configuring password replication policies
- Creating and associating Managed Service Accounts (MSA)
- Administrative auditing

Procedure:

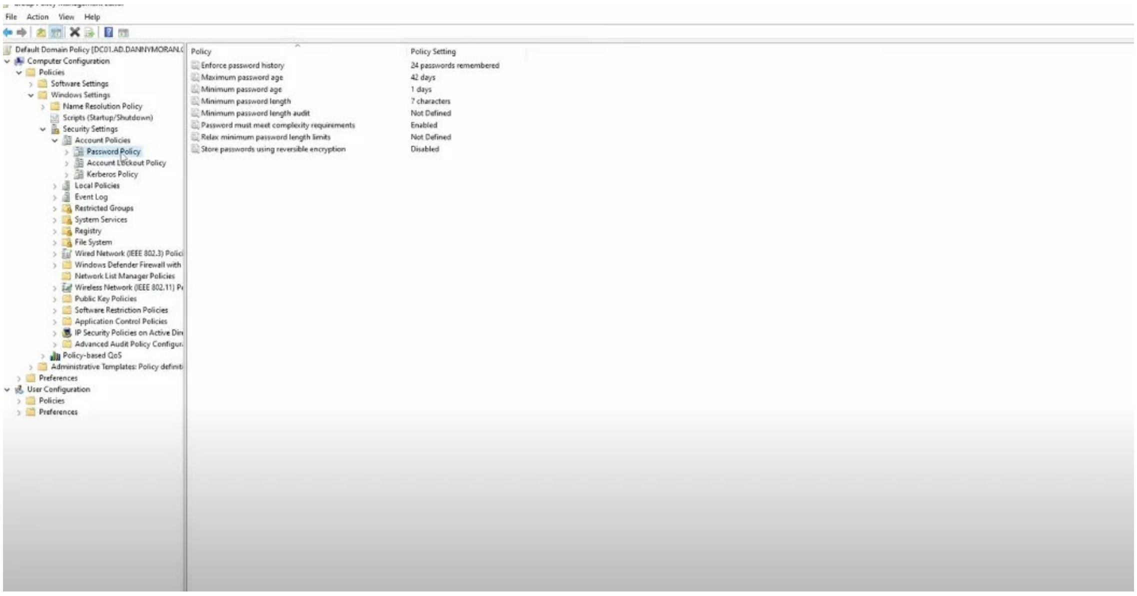
Exercise 1: Implementing Security Policies for Accounts, Passwords, and Administrative Groups

Step 1: Identify Required Settings

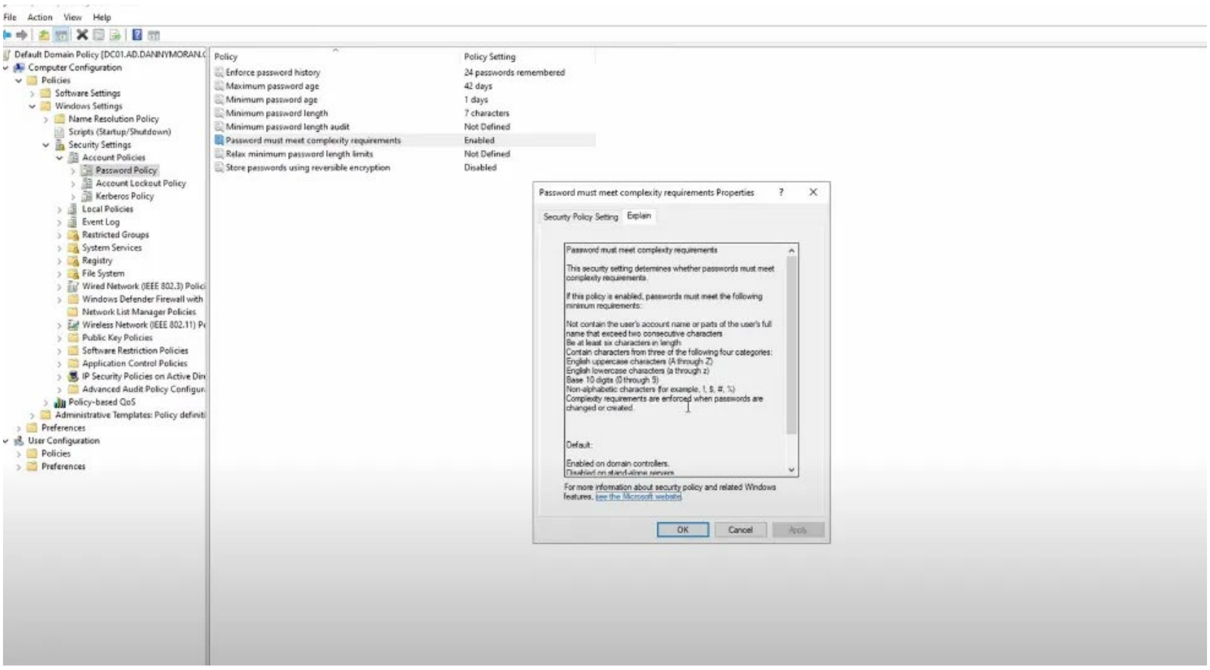
- Define and document password and account lockout settings for both regular users and IT administrators.
- Use the Default Domain Policy for all users; configure fine-grained password policies for administrative groups such as IT and Domain Admins.

Step 2: Configure Password Settings for All Users

1. Open Group Policy Management on LON-DC1.
2. Edit the Default Domain Policy to set:
    - Password history: 10
    - Maximum password age: 60 days
    - Minimum password age: 1 day
    - Minimum password length: 8 characters
    - Complexity requirements: Enabled
    - Store passwords using reversible encryption: Disabled
    - Account lockout duration: 60 minutes
    - Account lockout threshold: 5
    - Reset account lockout counter after: 20 minutes


File
Action
View
Help
Default Domain Policy [DC01.AD.DANNYMORAN.(
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polici
Windows Defender Firewall with
Network List Manager Policies
Wireless Network (IEEE 802.11) P
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Dir
Advanced Audit Policy Configur
Policy-based QoS
Administrative Templates: Policy definiti
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled


File
Action
View
Help
Default Domain Policy [DC01.AD.DANNYMORAN.C
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polici
Windows Defender Firewall with
Network List Manager Policies
Wireless Network (IEEE 802.11) Po
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Dir
Advanced Audit Policy Configur
Policy-based QoS
Administrative Templates: Policy definiti
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

Password must meet complexity requirements Properties

Security Policy Setting | Explain

Password must meet complexity requirements

This security setting determines whether passwords must meet complexity requirements.

If this policy is enabled, passwords must meet the following minimum requirements:

Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
Be at least six characters in length
Contain characters from three of the following four categories:
English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)
Complexity requirements are enforced when passwords are changed or created.

Default:

Enabled on domain controllers.
Disabled on stand-alone servers.

For more information about security policy and related Windows features, see the Microsoft website.

Step 3: Configure a Fine-Grained Password Policy (PSO) for IT Administrators

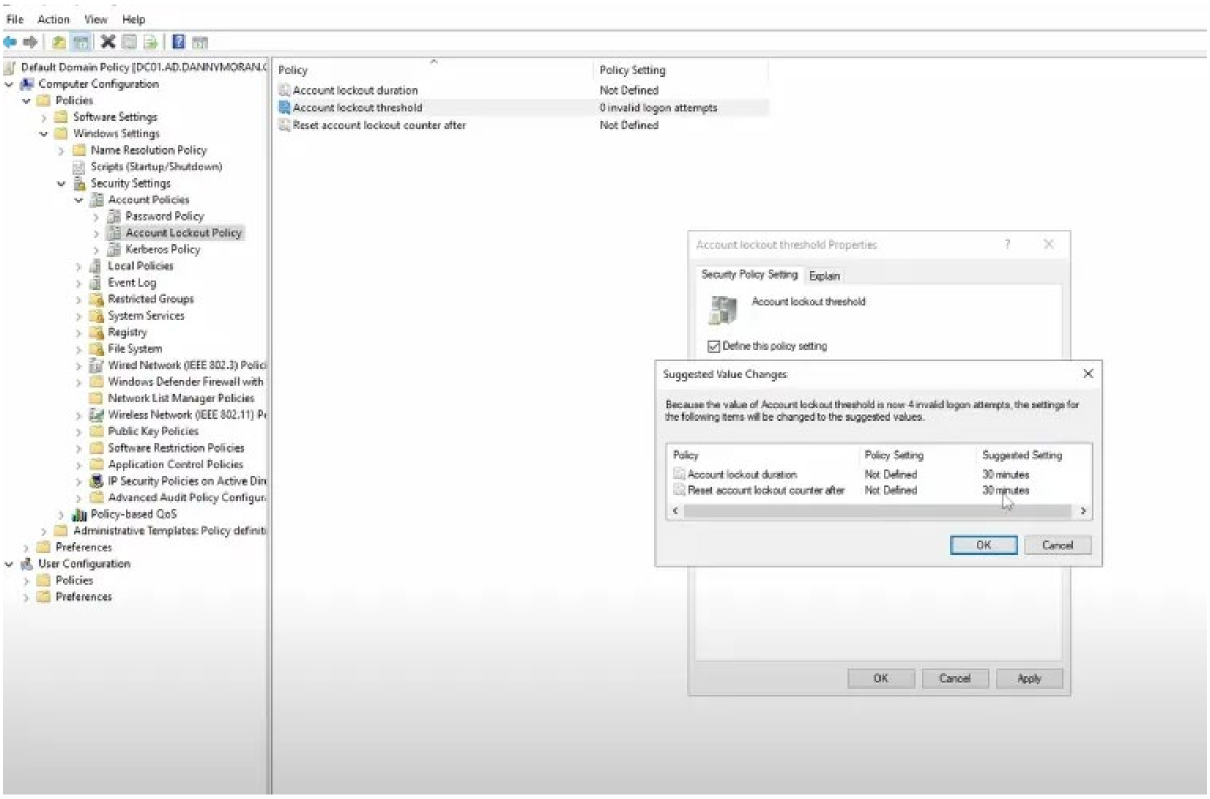
1. In Active Directory Administrative Center, navigate to the Password Settings Container.
2. Create a new Password Settings Object named "Adatum Administrators Password Settings".
3. Set parameters:
    - Minimum password length: 10
    - Password history: 10
    - Maximum password age: 30 days
    - Minimum password age: 1 day
    - Complexity: Enabled
    - Account lockout threshold: 3
    - Reset counter after: 20 minutes
    - Lockout duration: Until unlocked by administrator
4. Apply PSO directly to IT and Domain Admins groups (if needed, use PowerShell to change group scope to Global).

Step 4: Limit Local Administrators Group Membership

1. Create a dedicated OU for member servers (e.g., "Adatum Servers").
2. Move target member servers into this OU.

3. In Group Policy Management, create and link a GPO "Restricted Administrators on Member Servers" to this OU.

4. Use Restricted Groups policy to ensure only Domain Admins, IT group, and local Administrator are members of local Administrators group.


File
Action
View
Help
Default Domain Policy [DC01.AD.DANNYMORAN.C
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polici
Windows Defender Firewall with
Network List Manager Policies
Wireless Network (IEEE 802.11) P
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Dir
Advanced Audit Policy Configur
Policy-based QoS
Administrative Templates: Policy definiti
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Account lockout duration	Not Defined
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Defined

Account lockout threshold Properties

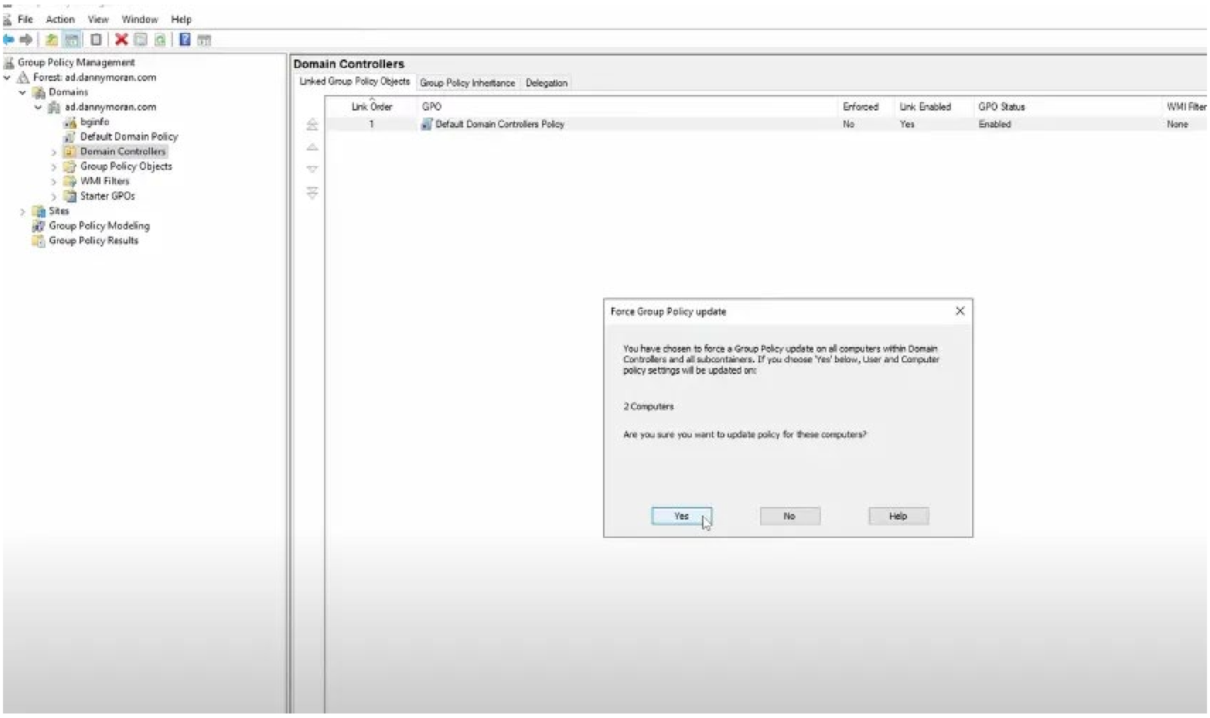
Account lockout threshold

☑ Define this policy setting

Suggested Value Changes

Because the value of Account lockout threshold is now 4 invalid logon attempts, the settings for the following items will be changed to the suggested values.

Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Defined	30 minutes
Reset account lockout counter after	Not Defined	30 minutes



Domain Controllers

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter
1	Default Domain Controllers Policy	No	Yes	Enabled	None

Force Group Policy update

You have chosen to force a Group Policy update on all computers within Domain Controllers and all subcontainers. If you choose 'Yes' below, User and Computer policy settings will be updated on:

2 Computers

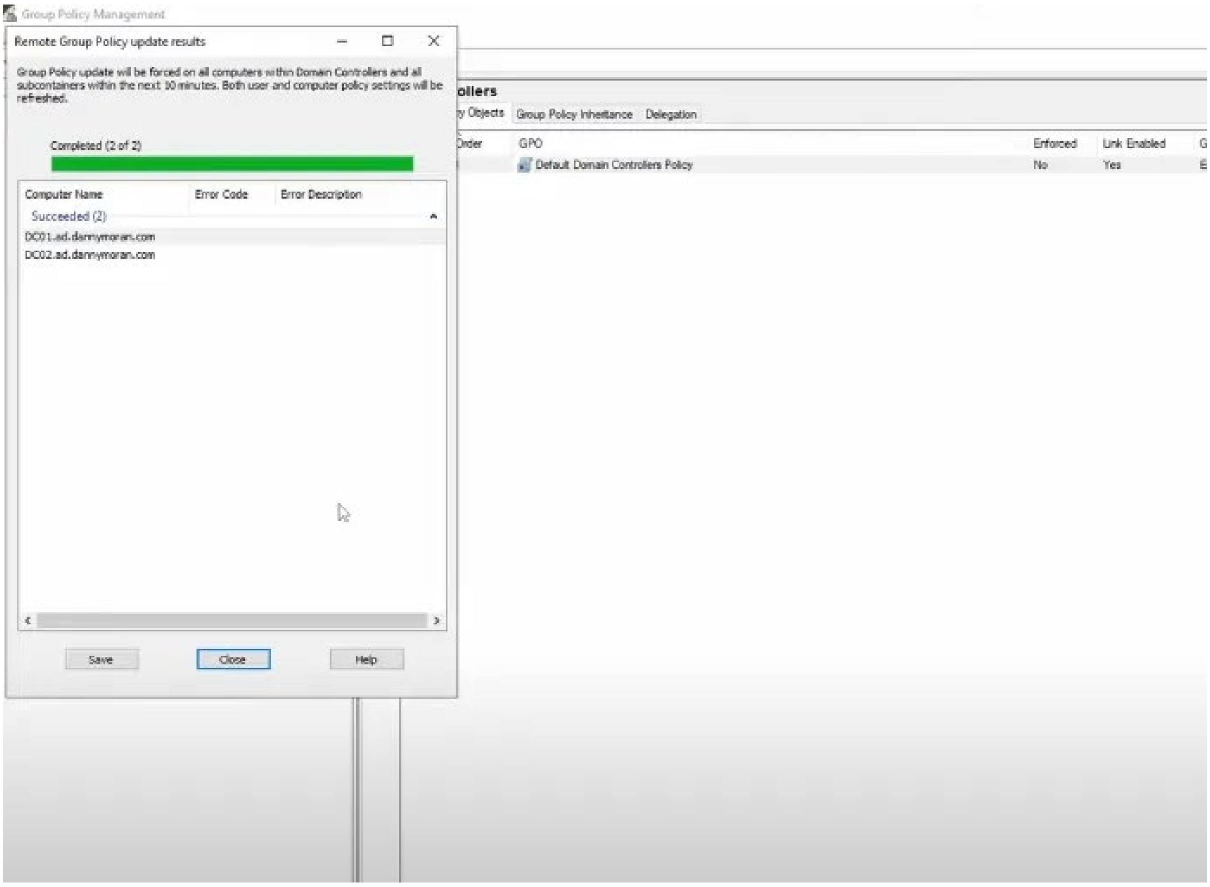
Are you sure you want to update policy for these computers?

Step 5: Restrict Membership of Critical Built-in Groups

1. Edit the Default Domain Controllers Policy.
2. Use Restricted Groups setting to ensure Server Operators, Account Operators, Enterprise Admins, and Schema Admins are empty unless required.

Step 6: Implement Administrative Auditing

1. Edit Default Domain Controllers Policy.
2. Configure advanced auditing in Group Policy Editor:
   - Audit Directory Services Changes (DS Access > Success)
   - Audit Security Group Management (Account Management > Success)
   - Force audit policy subcategory settings override
3. Use Active Directory Users and Computers to add auditing entries for critical changes.
4. Verify changes in Event Viewer (e.g., Event IDs 4728 for group membership changes; Event IDs 5136 for directory object modifications).



Group Policy update will be forced on all computers within Domain Controllers and all subcontainers within the next 10 minutes. Both user and computer policy settings will be refreshed.

Completed (2 of 2)

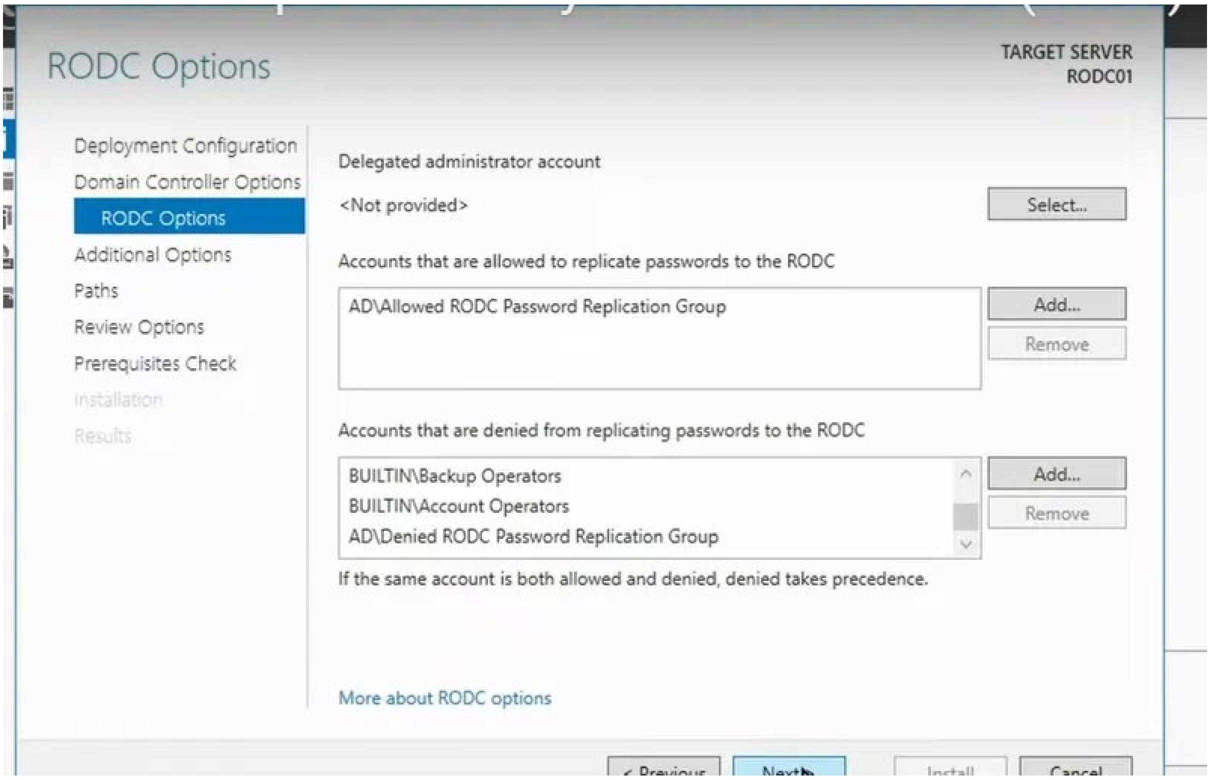
Computer Name	Error Code	Error Description
Succeeded (2)		
DC01.ad.dannymoran.com		
DC02.ad.dannymoran.com		

Order	GPO	Enforced	Link Enabled	G
	Default Domain Controllers Policy	No	Yes	E

Exercise 2: Deploying and Configuring an RODC

Step 1: Stage a Delegated Installation of an RODC

1. Remove LON-SVR1 from the domain (move to workgroup).
2. Delete LON-SVR1 computer object from AD DS.
3. In AD Sites and Services, create new Site "Munich".
4. In Active Directory Administrative Center, pre-create an RODC account for LON-SVR1 and delegate installation rights to user Nestor.



RODC Options

TARGET SERVER
RODC01

Delegated administrator account

<Not provided>

Accounts that are allowed to replicate passwords to the RODC

AD\Allowed RODC Password Replication Group

Accounts that are denied from replicating passwords to the RODC

BUILTIN\Backup Operators
BUILTIN\Account Operators
AD\Denied RODC Password Replication Group

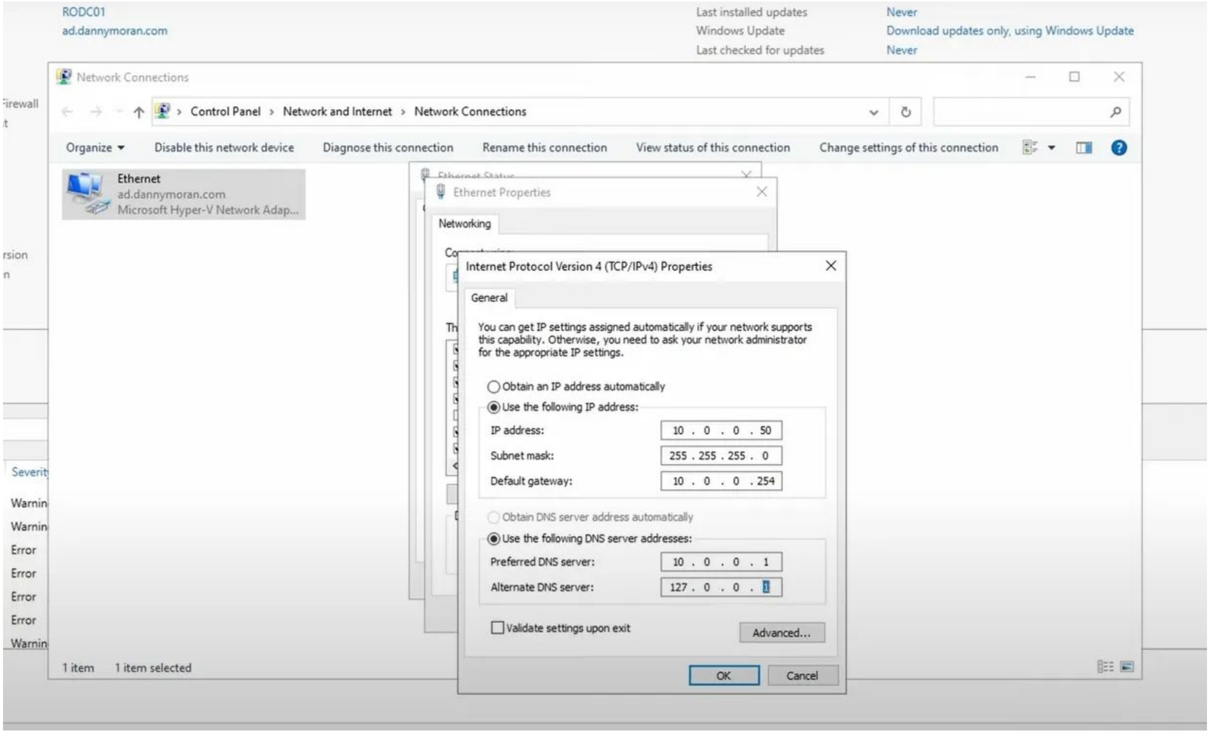
If the same account is both allowed and denied, denied takes precedence.

Step 2: Complete RODC Deployment

1. On LON-SVR1, install AD DS role.
2. Promote server to a read-only domain controller using the pre-created account, supplying delegated credentials.

Step 3: Configure Password Replication Policy

1. Add IT group to Denied RODC Password Replication Policy Group so their passwords aren't cached on RODCs.
2. Create a group for branch office users allowed to replicate passwords to Munich RODC.
3. Set password replication permissions in AD Administrative Center.



RODC01
ad.dannymoran.com

Last installed updates: Never
Windows Update: Download updates only, using Windows Update
Last checked for updates: Never

Network Connections

Control Panel > Network and Internet > Network Connections

Organize ▾ | Disable this network device | Diagnose this connection | Rename this connection | View status of this connection | Change settings of this connection

Ethernet
ad.dannymoran.com
Microsoft Hyper-V Network Adap...

1 item   1 item selected

Ethernet Properties — Networking

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

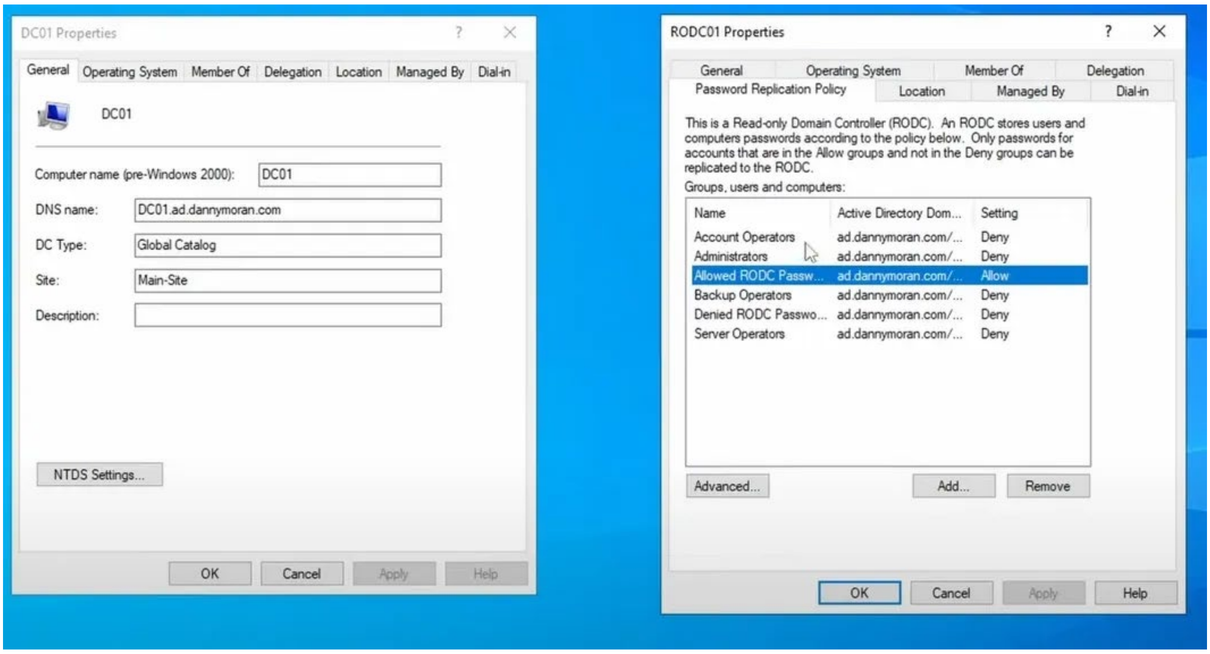
IP address:	10 . 0 . 0 . 50
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 0 . 0 . 254

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	10 . 0 . 0 . 1
Alternate DNS server:	127 . 0 . 0 . 1

□ Validate settings upon exit

Advanced... | OK | Cancel



DC01 Properties

General | Operating System | Member Of | Delegation | Location | Managed By | Dial-in

DC01

Computer name (pre-Windows 2000):	DC01
DNS name:	DC01.ad.dannymoran.com
DC Type:	Global Catalog
Site:	Main-Site
Description:	

NTDS Settings... | OK | Cancel | Apply | Help

RODC01 Properties

General | Operating System | Member Of | Delegation | Password Replication Policy | Location | Managed By | Dial-in

This is a Read-only Domain Controller (RODC). An RODC stores users and computers passwords according to the policy below. Only passwords for accounts that are in the Allow groups and not in the Deny groups can be replicated to the RODC.

Groups, users and computers:

Name	Active Directory Dom...	Setting
Account Operators	ad.dannymoran.com/...	Deny
Administrators	ad.dannymoran.com/...	Deny
Allowed RODC Passw...	ad.dannymoran.com/...	Allow
Backup Operators	ad.dannymoran.com/...	Deny
Denied RODC Passwo...	ad.dannymoran.com/...	Deny
Server Operators	ad.dannymoran.com/...	Deny

Advanced... | Add... | Remove | OK | Cancel | Apply | Help

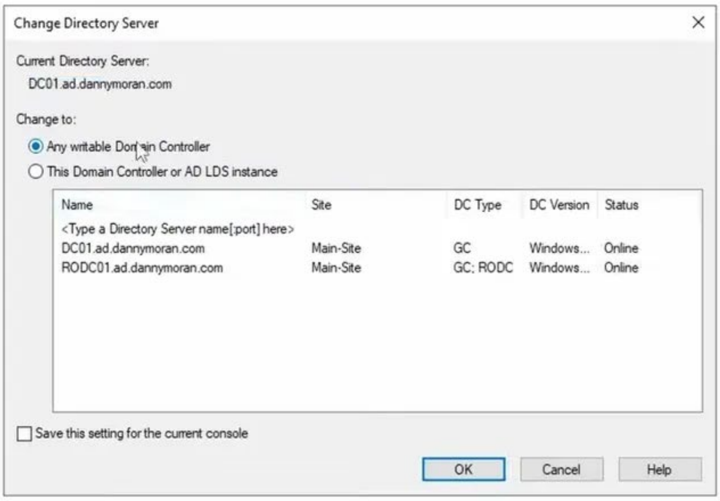
Step 4: Evaluate Resultant Password Replication Policy

1. In AD Administrative Center, review which accounts have their passwords stored on the RODC.
2. Test with a designated user to ensure allowed/denied replication settings operate as intended.

Exercise 3: Creating and Associating a Group Managed Service Account (gMSA)

Step 1: Create and Associate an MSA

1. Open AD PowerShell (on LON-DC1).
2. Run Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10)) to create the KDS root key.
3. Create service account:
    - New-ADServiceAccount –Name Webservice –DNSHostName LON-DC1 –PrincipalsAllowedToRetrieveManagedPassword LON-DC1$
    - Associate account: Add-ADComputerServiceAccount –identity LON-DC1 –ServiceAccount Webservice
4. Install the MSA on target servers and configure IIS Application Pool to use the account for required applications.



Change Directory Server

Current Directory Server:
DC01.ad.dannymoran.com

Change to:

● Any writable Domain Controller

○ This Domain Controller or AD LDS instance

Name	Site	DC Type	DC Version	Status
<Type a Directory Server name[:port] here>				
DC01.ad.dannymoran.com	Main-Site	GC	Windows...	Online
RODC01.ad.dannymoran.com	Main-Site	GC; RODC	Windows...	Online

□ Save this setting for the current console

Conclusion:

Module 7 ensures the AD DS environment is securely configured, with dedicated password and lockout policies tailored for both users and administrators. It strictly controls group memberships through OU structure and Restricted Groups, deploys RODCs for secure branch operations, and leverages fine-grained password policies and MSAs for service hardening. Comprehensive audit policies guarantee all changes are logged for review, strengthening security and traceability throughout your environment.