3/16/2021

Hands On Exercise

Chapter 3

User and Service Account Configuration

El Adel, Taoufik

IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY

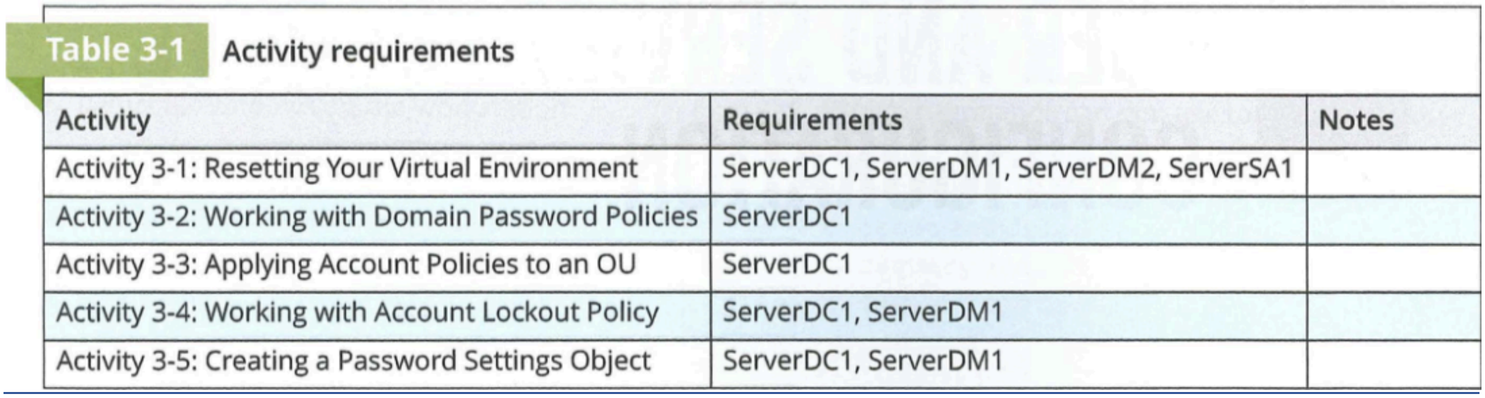


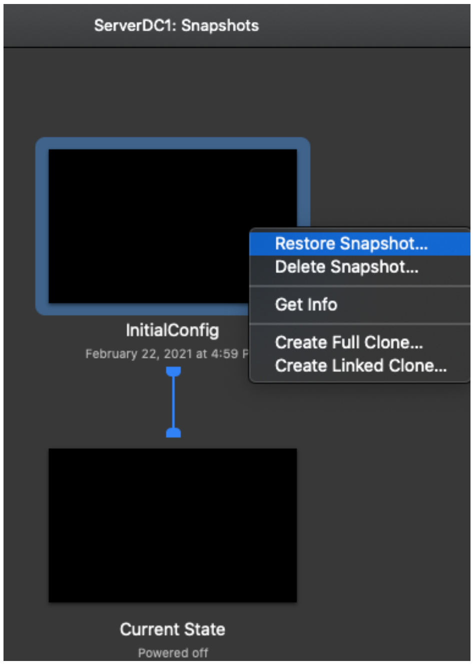
Table 3-1 Activity requirements

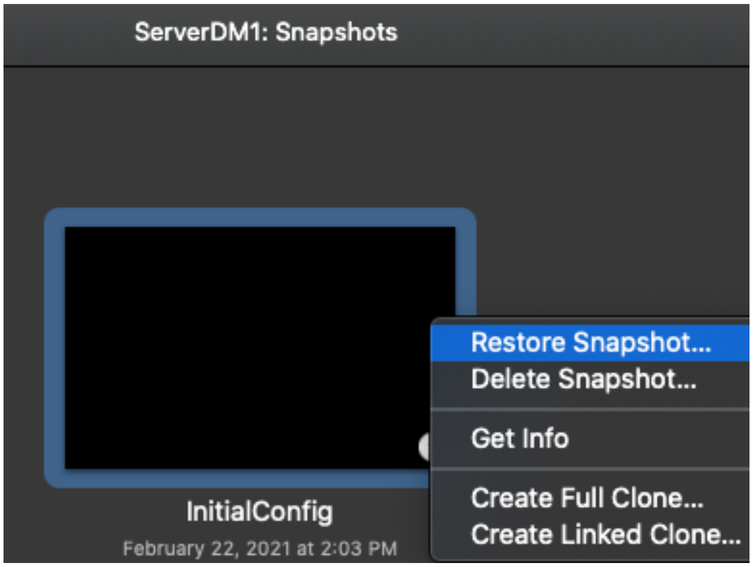
Activity	Requirements	Notes
Activity 3-1: Resetting Your Virtual Environment	ServerDC1, ServerDM1, ServerDM2, ServerSA1	
Activity 3-2: Working with Domain Password Policies	ServerDC1	
Activity 3-3: Applying Account Policies to an OU	ServerDC1	
Activity 3-4: Working with Account Lockout Policy	ServerDC1, ServerDM1	
Activity 3-5: Creating a Password Settings Object	ServerDC1, ServerDM1	

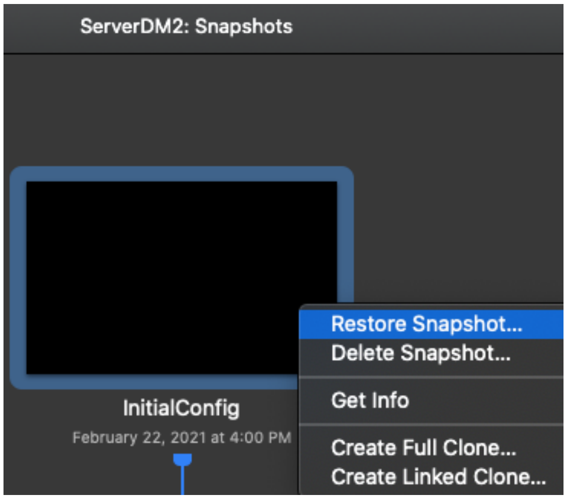
Activity 3-1: Resetting Your Virtual Environment

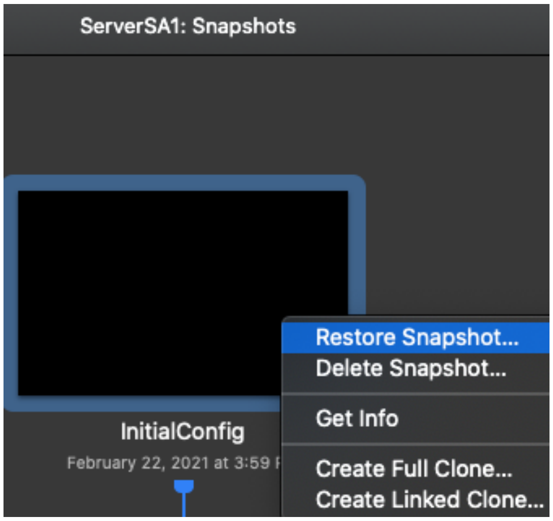
Description: Applying the InitialConfig snapshot to ServerDC1, ServerDM1, ServerDM2, and ServerSA1.

- **3-1-1:** Be sure the servers are shut down. In your virtualization program, apply the InitialConfig checkpoint or snapshot to ServerDC1, ServerDM1, ServerDM2, and ServerSA1.

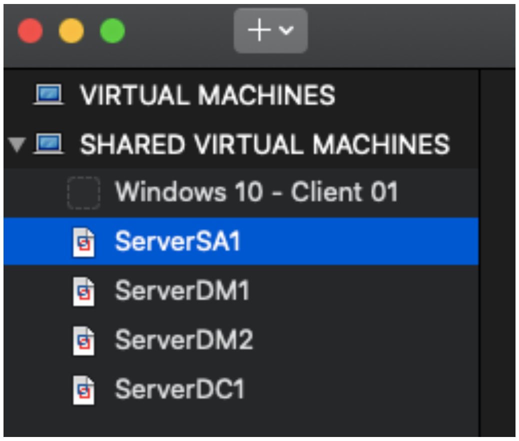








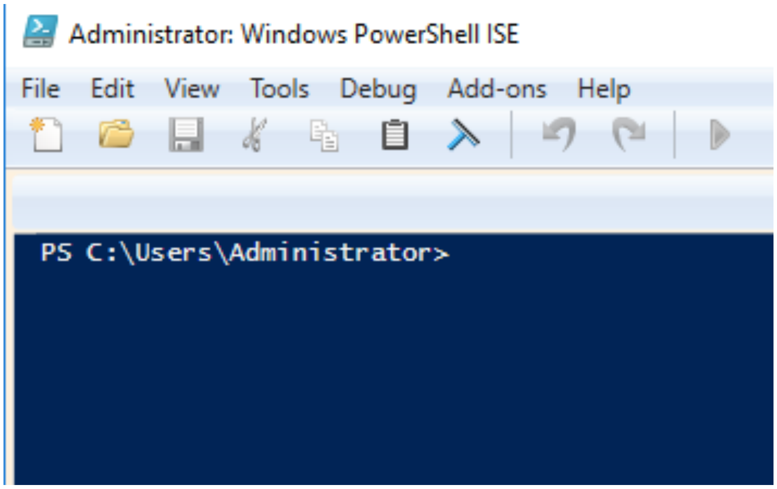
- **3-1-2:** When the snapshot or checkpoint has finished being applied, continue to the next activity.



Activity 3-2: Working with Domain Password Policies

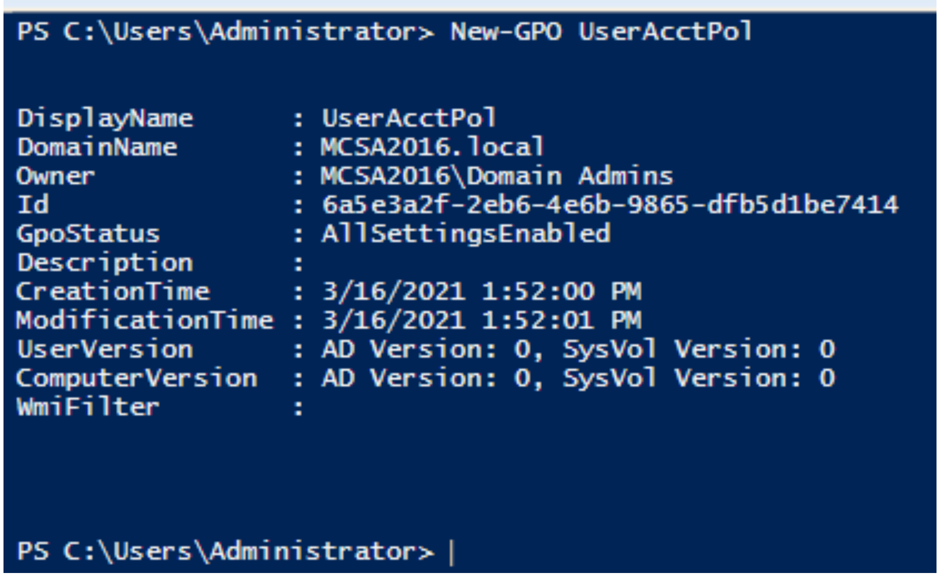
Description: In this activity, you change password policies from their default settings. Rather than edit the Default Domain Policy GPO, you create a new GPO and link it to the domain. The settings in the new GPO take precedence over the Default Domain Policy so that you can revert to the default account policies easily by unlinking the new GPO from the domain.

- **3-2-1:** Sign in to ServerDC1 as **Administrator** and open a PowerShell window.



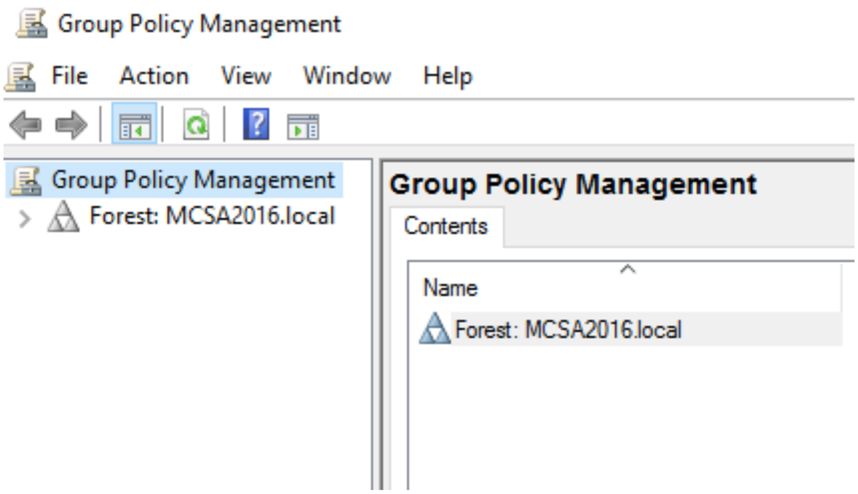
```
PS C:\Users\Administrator>
```

- **3-2-2:** Type **New-GPO UserAcctPol** and press **Enter**. Close the PowerShell window.

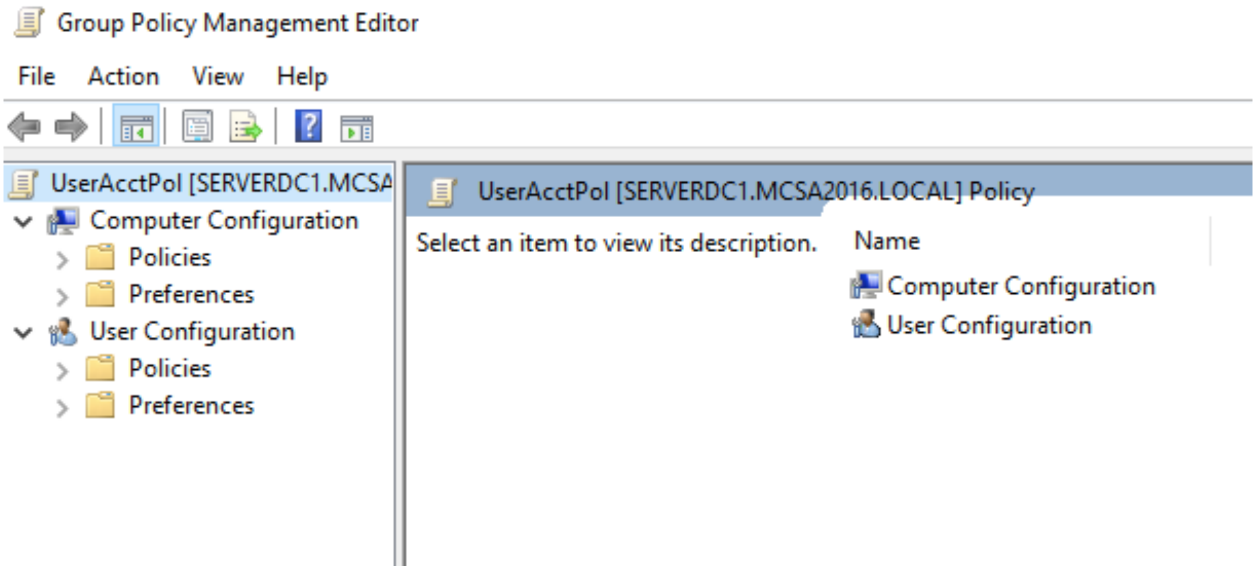


```
PS C:\Users\Administrator> New-GPO UserAcctPol


DisplayName      : UserAcctPol
DomainName       : MCSA2016.local
Owner            : MCSA2016\Domain Admins
Id               : 6a5e3a2f-2eb6-4e6b-9865-dfb5d1be7414
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 3/16/2021 1:52:00 PM
ModificationTime : 3/16/2021 1:52:01 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :



PS C:\Users\Administrator> |
```

- 3-2-3: Open the Group Policy Management Console.

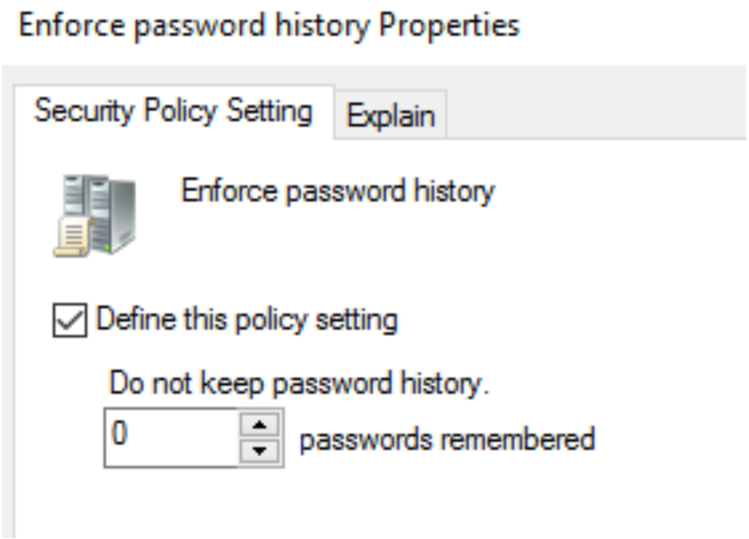


- 3-2-4: Click to expand the domain object, **MCSA2016.local,** and click to expand **Group Policy Objects.** Right-click **UserAcctPol** and click **Edit.**



Select an item to view its description.

- 3-2-5: In the Group Policy Management Editor, click to expand **Computer Configuration, Policies, Windows Settings, Security Settings,** and **Account Policies,** and then click **Password Policy.** In the right pane, double-click **Enforce password history.** Click the **Define this policy setting** check box, leave the passwords remembered value at **0,** and then click **OK.**



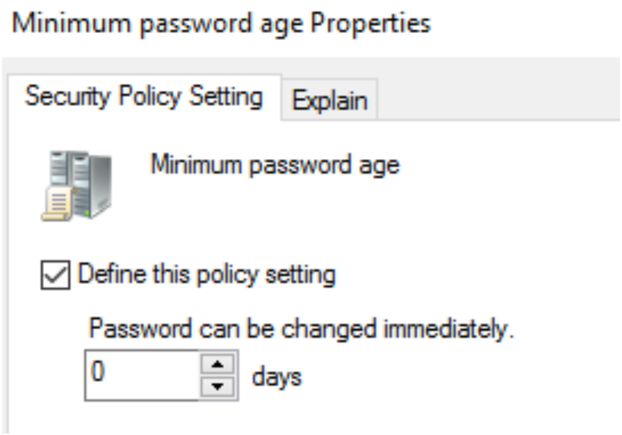
Enforce password history

☑ Define this policy setting

Do not keep password history.

0 passwords remembered

- 3-2-6: Double-click **Minimum password age.** Click the **Define this policy setting** check box, set the value to **0** days so that passwords can be changed immediately, and then click **OK.** Windows provides a suggested value for Maximum password age because this policy must be defined if Minimum password age is defined. Click **OK** to accept the suggested value. Close the Group Policy Management Editor. Settings that you didn't define, such as Minimum password length, are still set because the Default Domain Policy defines them.

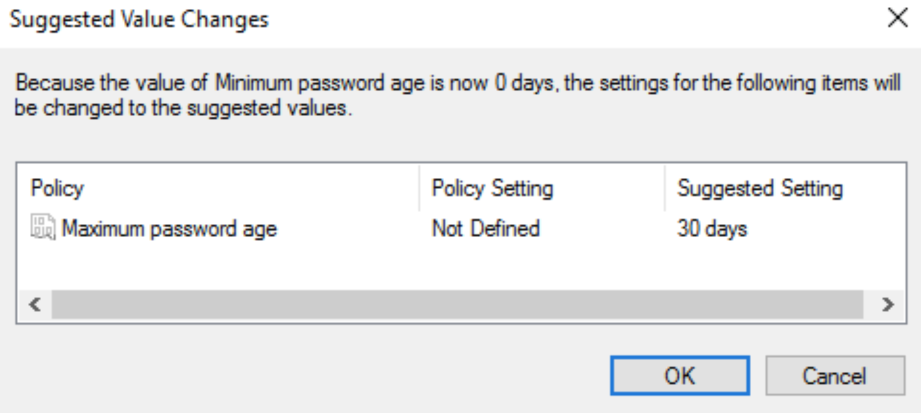


Minimum password age

☑ Define this policy setting

Password can be changed immediately.

0 days

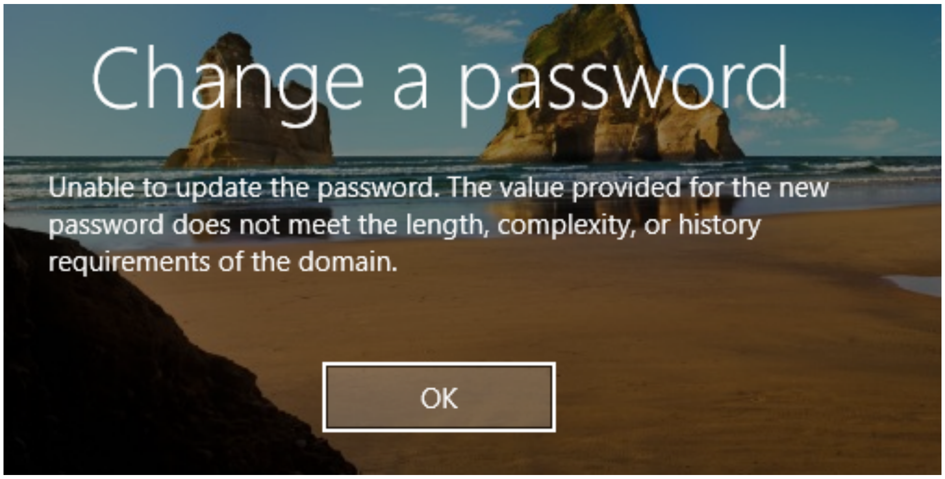


Suggested Value Changes

Because the value of Minimum password age is now 0 days, the settings for the following items will be changed to the suggested values.

Policy	Policy Setting	Suggested Setting
Maximum password age	Not Defined	30 days

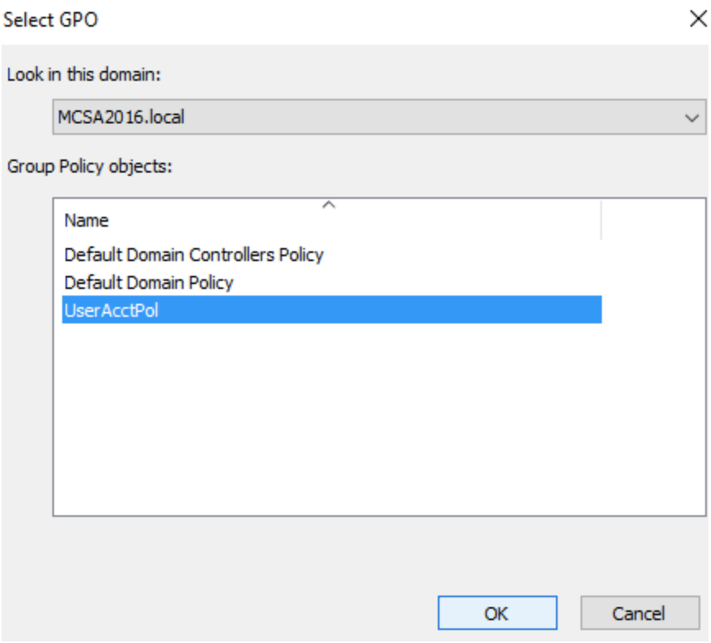
- 3-2-7: Before you test this policy, see how it works with the current policy in place. The default value for the Enforce password history policy you changed is 24, which means you shouldn't be able to change your password to the same value. Press **Ctrl+Alt+Del,** and then click **Change a password.** In the Old password text box, type your current password. In the New password and Confirm password text boxes, type your current password and press **Enter.** You see a message stating that Windows is unable to update the password. This is because Enforce password history is set to 24, which means that you can't reuse the same password until you have used 24 different passwords. Click **OK,** and then click **Cancel** and **Cancel** again to return to the desktop.



Change a password

Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain.

- 3-2-8: In the Group Policy Management console, link UserAcctPol to the domain by right-clicking **MCSA2016.local** and clicking **Link an Existing GPO.** In the Select GPO dialog box, click **UserAcctPol** (see Figure 3-6) and click **OK.**



Select GPO

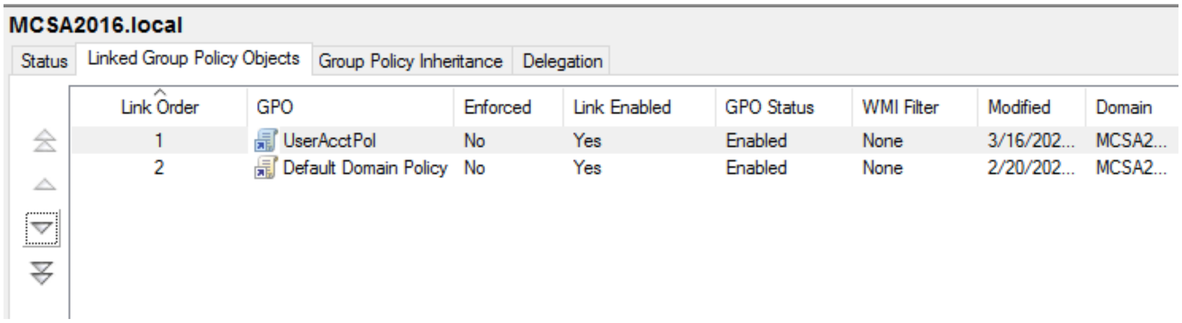
Look in this domain:

MCSA2016.local

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
UserAcctPol

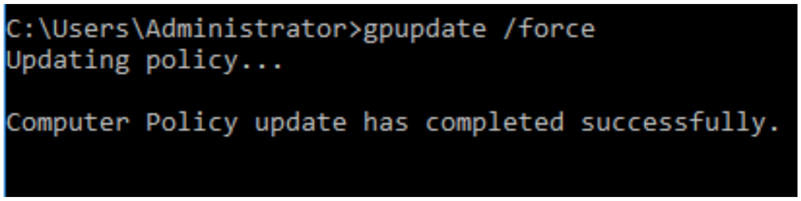
- 3-2-9: Click **MCSA2016.local,** and in the right pane, click **Linked Group Policy Objects.** The current link order causes the Default Domain Policy to take precedence over UserAcctPol. You want UserAcctPol to have precedence, so click **UserAcctPol** and click the **up arrow** to change UserAcctPol's link order to **1** (see Figure 3-7).



MCSA2016.local

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	UserAcctPol	No	Yes	Enabled	None	3/16/202...	MCSA2...
2	Default Domain Policy	No	Yes	Enabled	None	2/20/202...	MCSA2...

- 3-2-10: Open a command prompt window, and then type **gpupdate /force** and press **Enter.** When the command finishes running, try to change your password again following the instructions in Step 7, using the same password for both the old and new passwords. You should be successful. Click **OK.** Close the command prompt window.



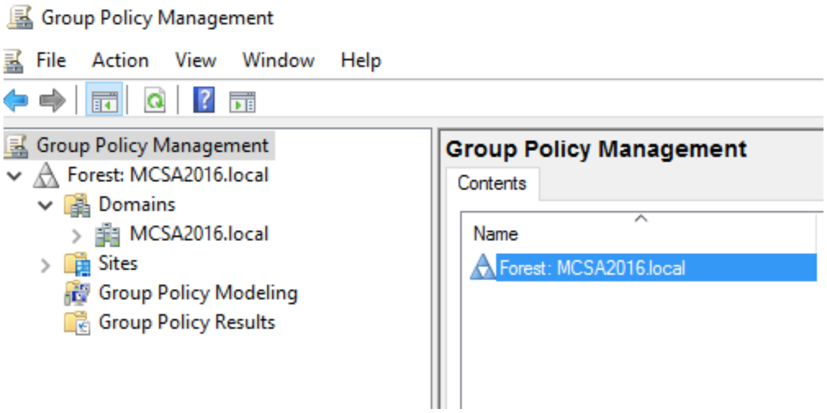
```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

- 3-2-11: Continue to the next activity.

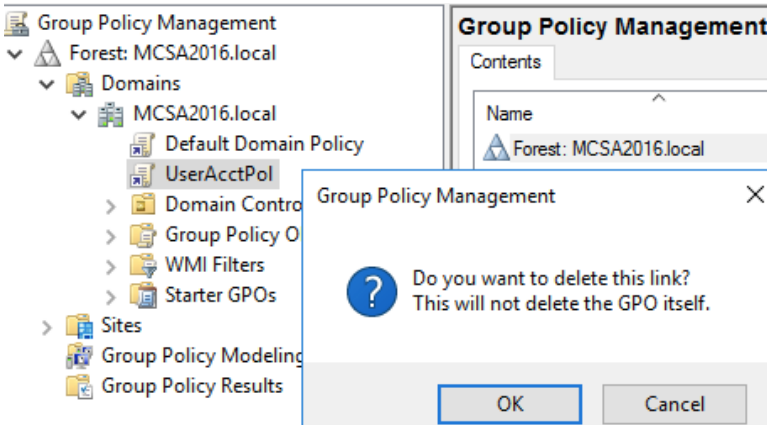
Activity 3-3: Applying Account Policy to an OU

Description: In this activity, you unlink the UserAcctPol GPO from the domain and link it to the Domain Controllers OU. Next, you test to see which GPO's settings have an effect on domain accounts.

- 3-3-1: On ServerDC1, open the Group Policy Management console, if necessary.

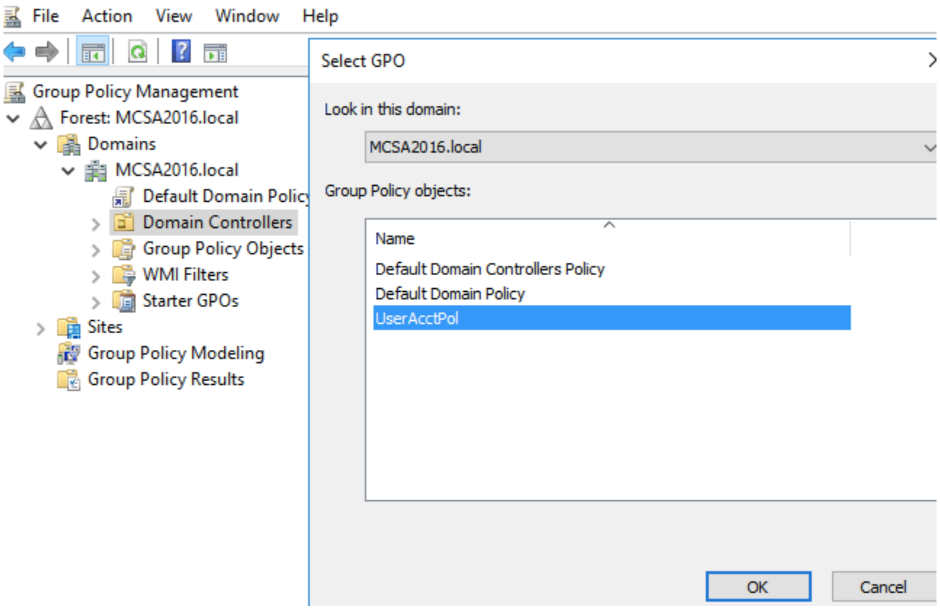


- 3-3-2: Click to expand **MCSA2016.local**, if necessary. Right-click **UserAcctPol** and click **Delete**. Note that this action does not delete the GPO; it only unlinks it from the domain. Click **OK.**



Do you want to delete this link?
This will not delete the GPO itself.

- 3-3-3: Right-click the **Domain Controllers** OU and click **Link an Existing GPO**. In the Select GPO dialog box, click **UserAcctPol**, and then click **OK**.

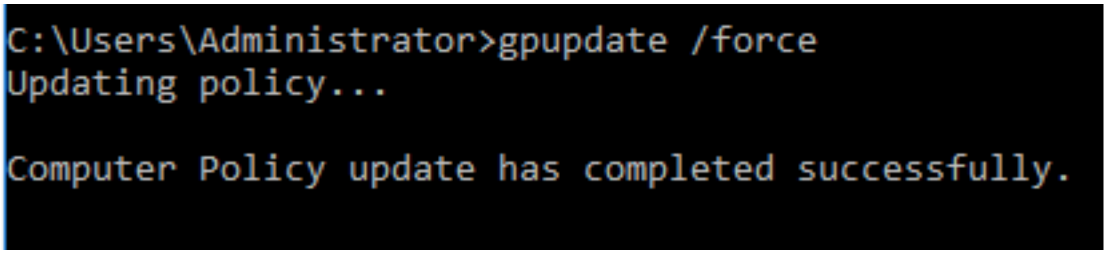


Look in this domain: MCSA2016.local

Group Policy objects:

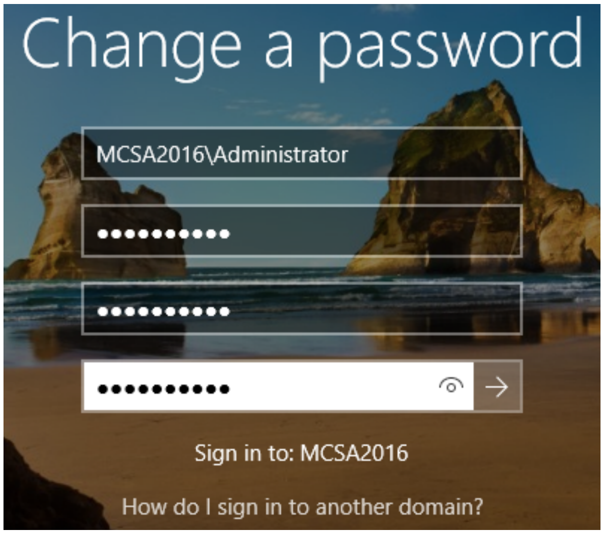
Name
Default Domain Controllers Policy
Default Domain Policy
UserAcctPol

- 3-3-4: The Domain Controllers OU contains the ServerDC1 computer account, which holds the Active Directory database containing all domain users. Open a command prompt window, and then type **gpupdate /force** and press **Enter.** Close the command prompt window.



```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

- 3-3-5: **Press Ctrl+Alt+Del**, and then click **Change a password**. In the Old password text box, type your current password. In the New password and Confirm password text boxes, type your current password.


Change a password

MCSA2016\Administrator

••••••••••

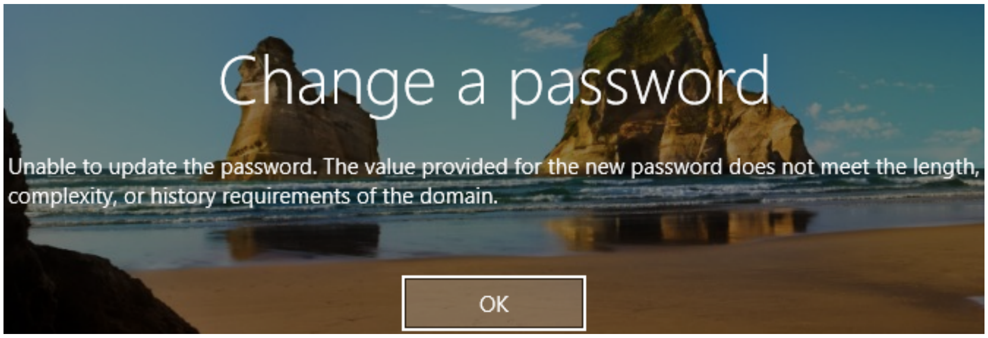
••••••••••

••••••••••

Sign in to: MCSA2016

How do I sign in to another domain?

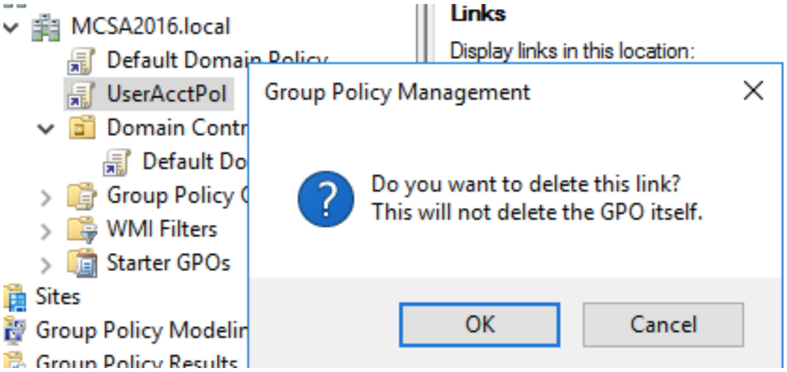
- **3-3-6:** You see a message stating that Windows is unable to update the password. This is because the Default Domain Policy is in effect. Enforce password history is set to 24 in the Default Domain Policy, so you can't change your password to the same value you used before. Because account policies can be set only at the domain level for domain accounts, the UserAcctPol GPO linked to the Domain Controllers OU has no effect on account policies for the Administrator user.


Change a password

Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain.

OK

- **3-3-7:** Unlink the **UserAcctPol** GPO from the **Domain Controllers** OU.



Group Policy Management

Do you want to delete this link?
This will not delete the GPO itself.

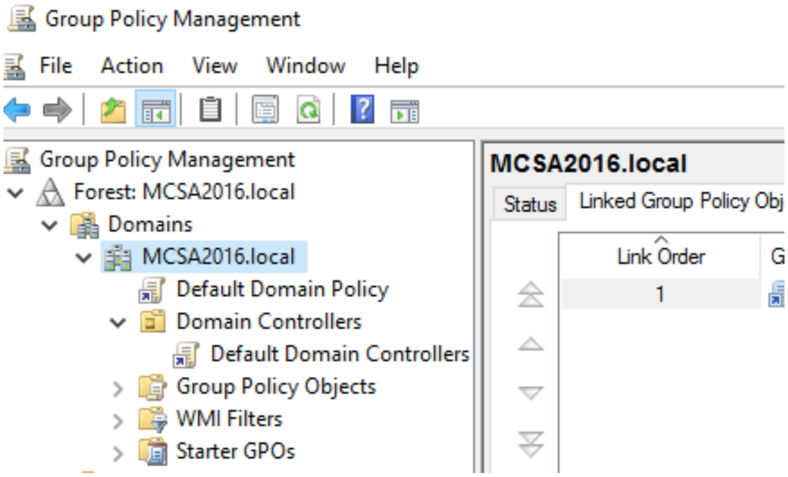
OK Cancel

- 3-3-8: Continue to the next activity.

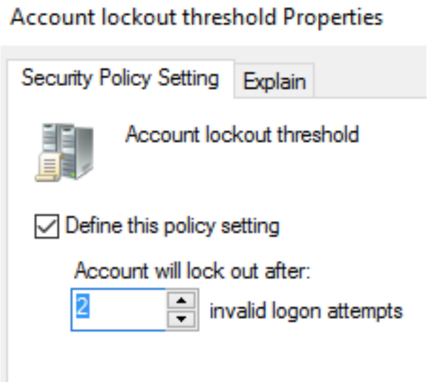
Activity 3-4: Working with Account Lockout Policy

Description: As a continuation of the previous activity, you change settings in the Account Lockout Policy node and test your changes.

- 3-4-1: On ServerDC1, open the Group Policy Management console, if necessary.



- 3-4-2: Click **Group Policy Objects**, and then right-click **UserAcctPol** and click **Edit**. In the Group Policy Management Editor, click to expand **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and **Account Policies**, and then click **Account Lockout Policy**. Double-click **Account lockout threshold**. Click the **Define this policy setting** check box, change the invalid logon attempts value to **2,** and then click **OK**.

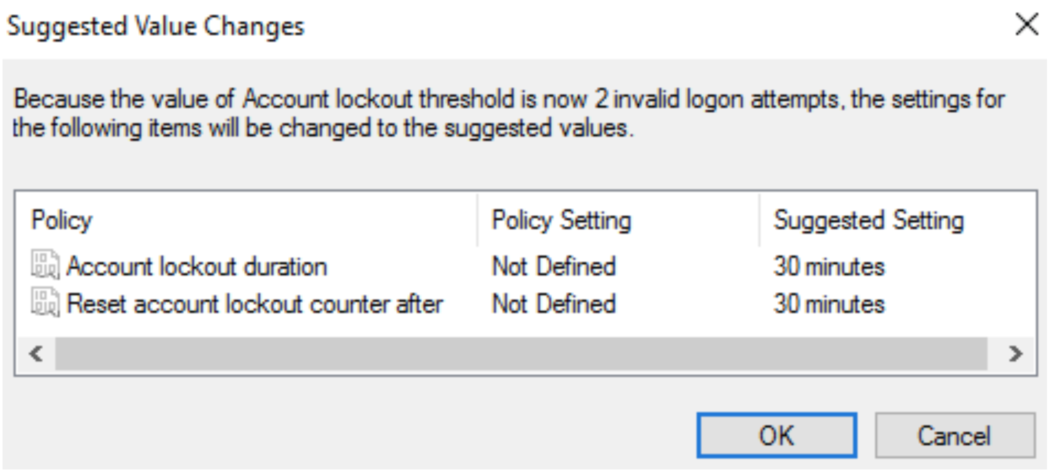

Account lockout threshold Properties
Security Policy Setting
Explain
Account lockout threshold

☑ Define this policy setting

Account will lock out after:

2 invalid logon attempts

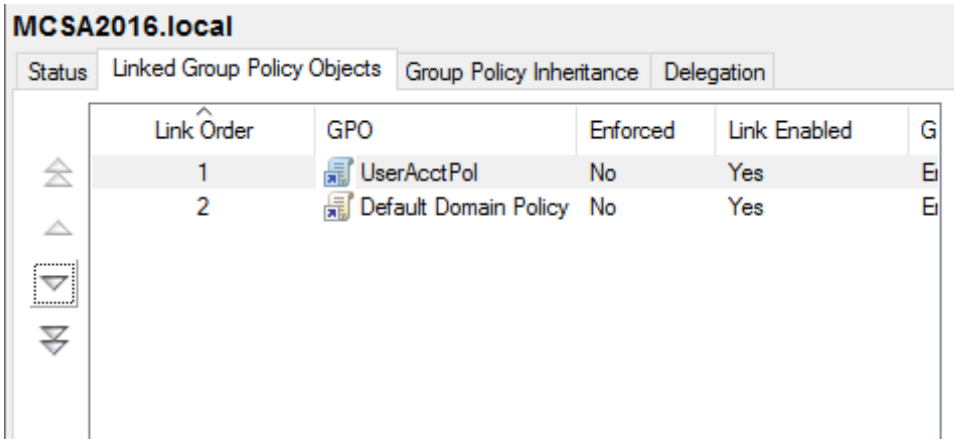
- **3-4-3:** The Suggested Value Changes dialog box suggests values for *Account lockout duration* and *Reset account lockout counter after.* Click **OK** to accept these settings, and close the Group Policy Management Editor.



Because the value of Account lockout threshold is now 2 invalid logon attempts, the settings for the following items will be changed to the suggested values.

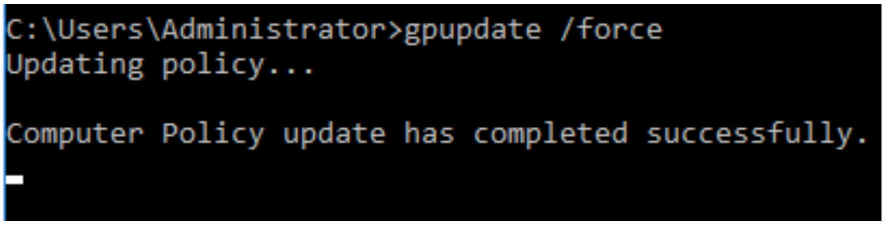
Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Defined	30 minutes
Reset account lockout counter after	Not Defined	30 minutes

- **3-4-4**: Link **UserAcctPol** to the domain node, and make sure it's first in the link order.



Link Order	GPO	Enforced	Link Enabled	G
1	UserAcctPol	No	Yes	E
2	Default Domain Policy	No	Yes	E

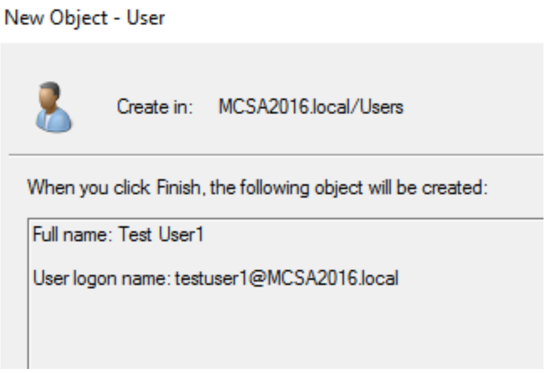
- **3-4-5:** Open a command prompt window, and then type **gpupdate /force** and press **Enter**. (Password policies that affect domain users are stored on domain controllers, not member computers, so the policy must be updated on the domain controller even though you will sign in from ServerDM1 .) Close the command prompt window.



```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

- 3-4-6: Open Active Directory Users and Computers and create a user in the Users folder with the following properties:

  Full name: **Test User1**
  User logon name: **testuser1**
  Password: **Password01**
  User must change password at next logon: **Unchecked**
  Repeat this step to create another user with Full Name **Test User2** and User logon name **testuser2** with the same password and password properties.



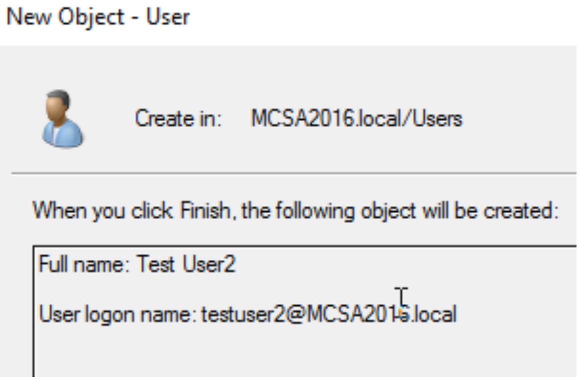
New Object - User

Create in: MCSA2016.local/Users

When you click Finish, the following object will be created:

Full name: Test User1

User logon name: testuser1@MCSA2016.local



New Object - User

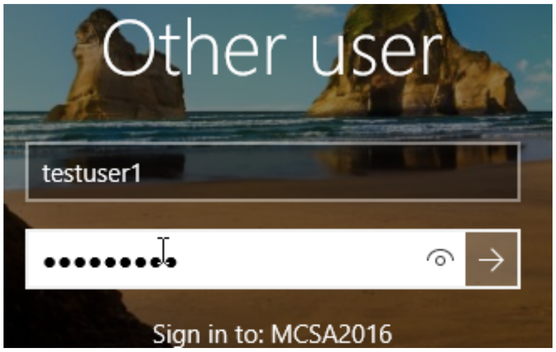
Create in: MCSA2016.local/Users

When you click Finish, the following object will be created:

Full name: Test User2

User logon name: testuser2@MCSA2016.local

- 3-4-7: Start ServerDM1 if necessary and attempt to sign in twice as **testuser1** with an incorrect password. Attempt to sign in a third time with the correct password (Password01). You should get a message stating that the account is currently locked out. Click **OK**.

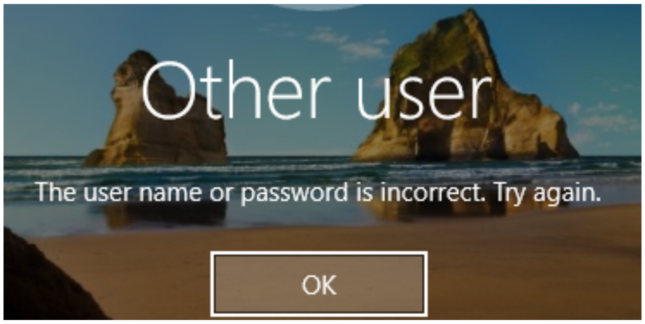


Other user

testuser1

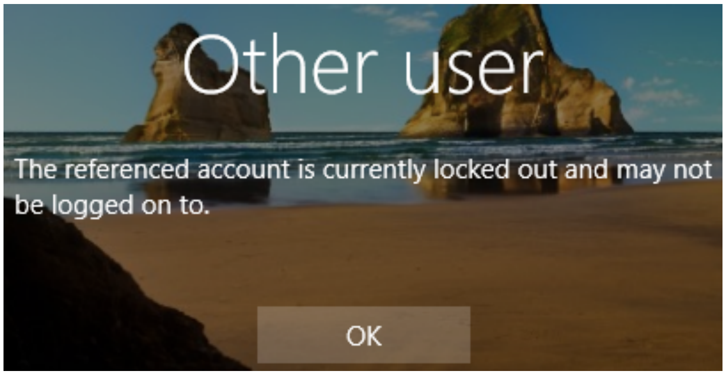
•••••••••

Sign in to: MCSA2016



Other user

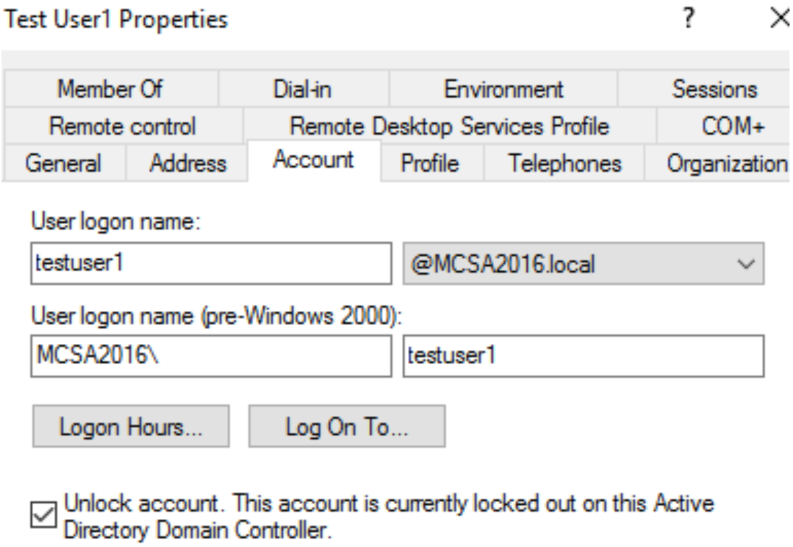
The user name or password is incorrect. Try again.



Other user

The referenced account is currently locked out and may not be logged on to.

- **3-4-8:** On ServerDC1, open Active Directory Users and Computers. Open the Properties dialog box for **Test User1** and click the **Account** tab. Under the Logon Hours button is a message stating that the account is locked out. Click the **Unlock account** check box to unlock the account manually (see Figure 3-8) but be aware that the account unlocks automatically after the number of minutes in the Account lockout duration setting expires if it hasn't been unlocked manually. Click **OK.**



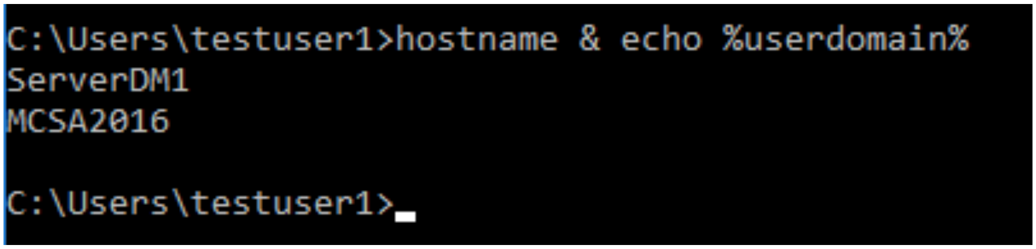
Test User1 Properties

User logon name:
testuser1 @MCSA2016.local

User logon name (pre-Windows 2000):
MCSA2016\ testuser1

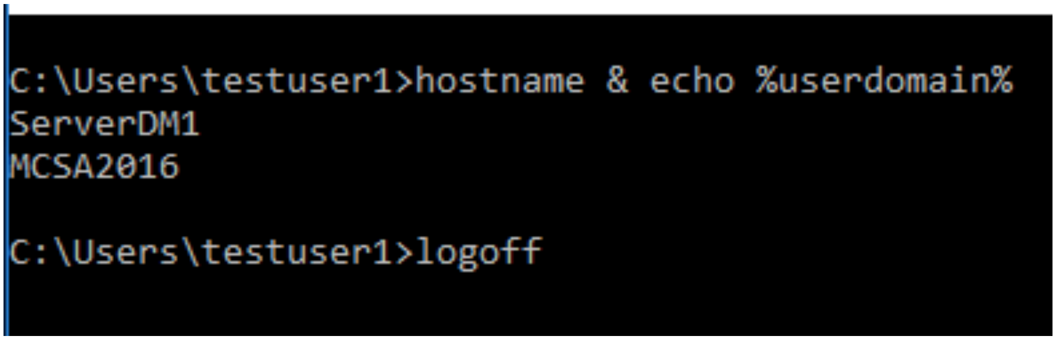
☑ Unlock account. This account is currently locked out on this Active Directory Domain Controller.

- **3-4-9:** Attempt to sign in as **testuser1** from ServerDM1 again. You should be successful.

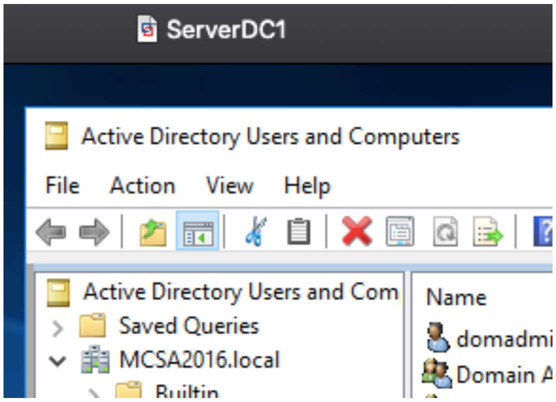


```
C:\Users\testuser1>hostname & echo %userdomain%
ServerDM1
MCSA2016

C:\Users\testuser1>_
```

- **3-4-10:** Sign out of ServerDM1 but stay signed in to ServerDC1 and continue to the next activity.



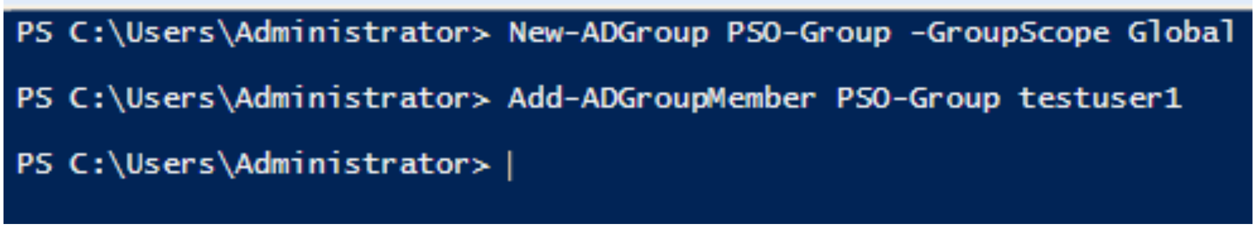
```
C:\Users\testuser1>hostname & echo %userdomain%
ServerDM1
MCSA2016

C:\Users\testuser1>logoff
```



Activity 3-5: Creating a Password Settings Object

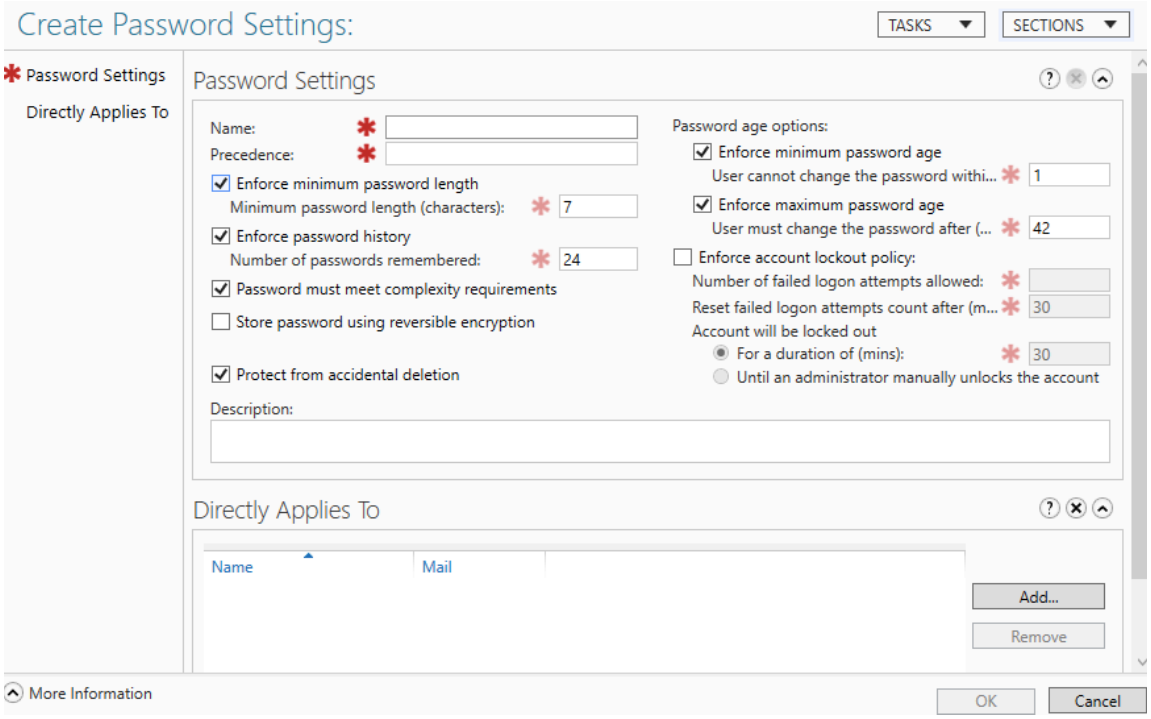
Description: In this activity, you first create a group to link to a new PSO. Then, you create a new PSO, define password settings, and link it to a group. Finally, you test the settings.

- **3-5-1:** First, you'll create a new group to link the PSO to and add a user to it. On ServerDC1, open a PowerShell window. Type **New-ADGroup PSO-Group -GroupScope Global** and press **Enter**. Next add testuser1 to the group by typing **Add-ADGroupMember PSO-Group testuser1** and press **Enter**. Close the PowerShell window.



```
PS C:\Users\Administrator> New-ADGroup PSO-Group -GroupScope Global
PS C:\Users\Administrator> Add-ADGroupMember PSO-Group testuser1
PS C:\Users\Administrator> |
```

- 3-5-2: Open Active Directory Administrative Center. Click **MCSA2016 (local)** to see the folders and OUs in the middle pane. Double-click **System** and then **Password Settings Container.** In the Tasks pane, click **New,** and then click **Password Settings.**



Create Password Settings:

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

Description:

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

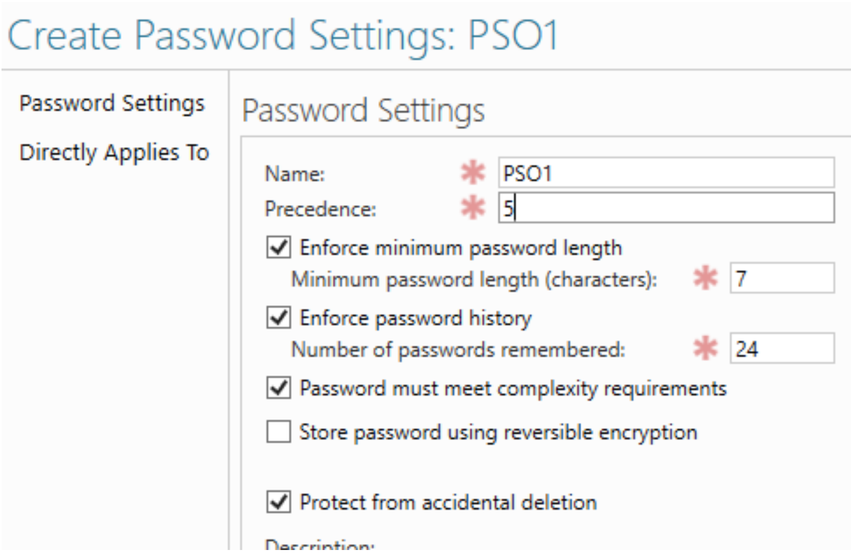
● For a duration of (mins): * 30

○ Until an administrator manually unlocks the account

Directly Applies To

Name	Mail

- 3-5-3: In the Create Password Settings dialog box, type **PSO1** in the Name text box and **5** in the Precedence text box. The Precedence value doesn't mean much until you have more than one PSO defined.



Create Password Settings: PSO1

Password Settings

Directly Applies To

Password Settings

Name: * PSO1

Precedence: * 5

☑ Enforce minimum password length

Minimum password length (characters): * 7

☑ Enforce password history

Number of passwords remembered: * 24

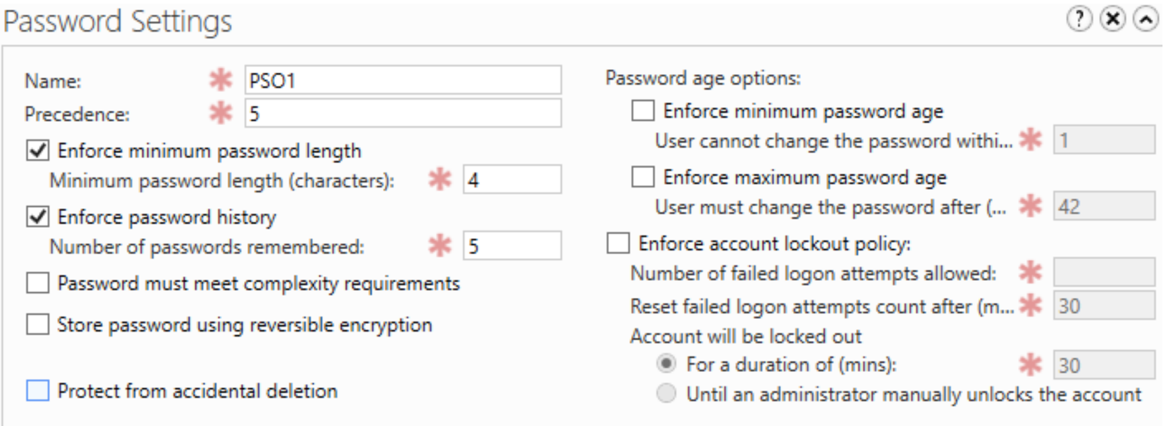
☑ Password must meet complexity requirements

☐ Store password using reversible encryption

☑ Protect from accidental deletion

Description:

- **3-5-4:** In the Minimum password length (characters) text box, type **4**, and in the Number of passwords remembered text box, type **5**. Click to clear the **Password must meet complexity requirements, Enforce minimum password age**, and **Enforce maximum password age** check boxes. Leave the **Enforce account lockout policy** at the default so that accounts are never locked out. Click to **clear Protect from accidental deletion** because you're deleting this PSO at the end of this activity.



Password Settings

Name: * PSO1

Precedence: * 5

☑ Enforce minimum password length

Minimum password length (characters): * 4

☑ Enforce password history

Number of passwords remembered: * 5

☐ 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: *

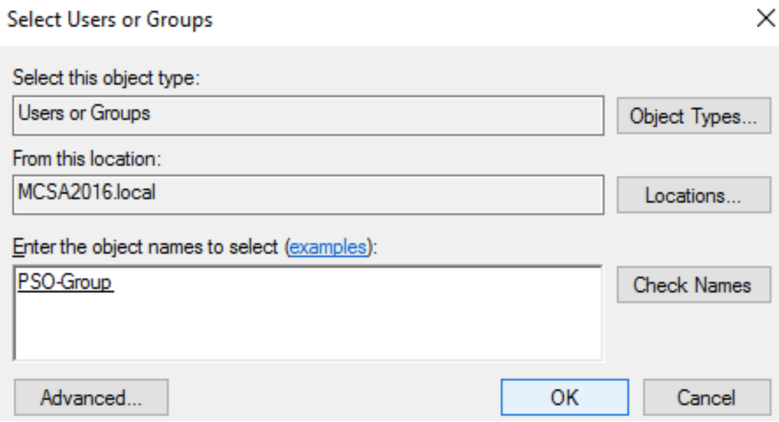
Reset failed logon attempts count after (m... * 30

Account will be locked out

● For a duration of (mins): * 30

○ Until an administrator manually unlocks the account

- **3-5-5:** Click the **Add button**, and type **PSO-Group**. Click **Check Names** and then **OK**. The settings should look like Figure 3-9. Click **OK.**



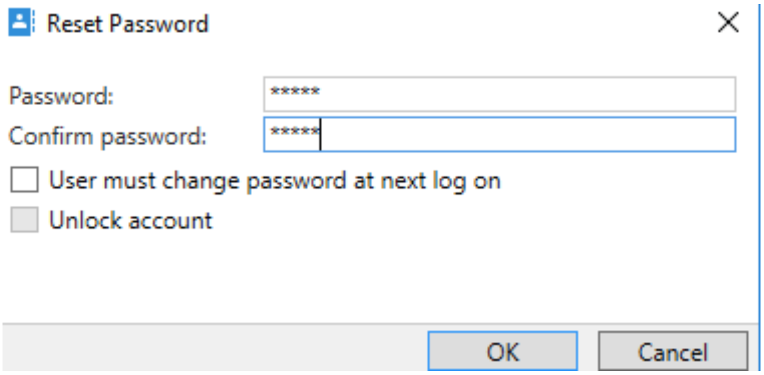
Select Users or Groups

Select this object type: Users or Groups

From this location: MCSA2016.local

Enter the object names to select (examples): PSO-Group

- 3-5-6: In Active Directory Administrative Center, click **MCSA2016 (local)** in the left pane, and then double-click **Users** in the middle pane. Click to select **Test User1.** In the Tasks pane, click **Reset password.** Type **pass1** in the Password and Confirm password text boxes and click to clear **User must change password at next log on.** Click **OK.** The new password is accepted. Recall that the password policy defined in the Default Domain Policy requires a complex password of at least 7 characters.



Reset Password

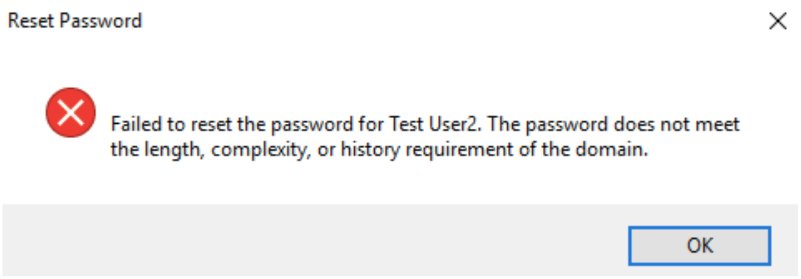
Password: *****

Confirm password: *****

□ User must change password at next log on

□ Unlock account

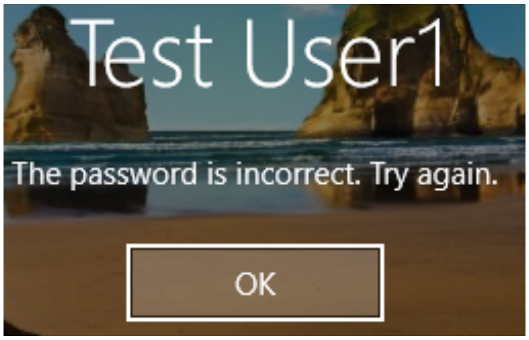
- 3-5-7: Click to select **Test User2**. In the Tasks pane, click **Reset password**. Type **pass1** in the Password and Confirm password text boxes, and then click **OK**. You see a message stating that the password doesn't meet complexity requirements. Click **OK** and then **Cancel**. The PSO you created applies only to members of the PSO-Group of which Test User2 is not a member.



Reset Password

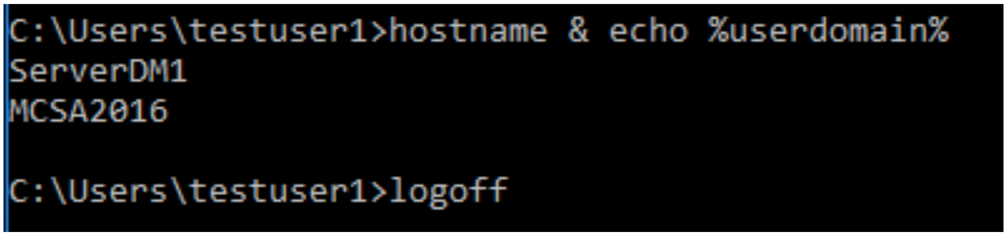
Failed to reset the password for Test User2. The password does not meet the length, complexity, or history requirement of the domain.

- 3-5-8: On ServerDM1, try to sign in as **testuser1** with an incorrect password three times. Recall that the domain policy is set to lockout accounts after two incorrect attempts to log on. Now, try to sign in with **pass1**. You're successful because the PSO applied to PSO-Group disables account lockout. Sign out of ServerDM1.



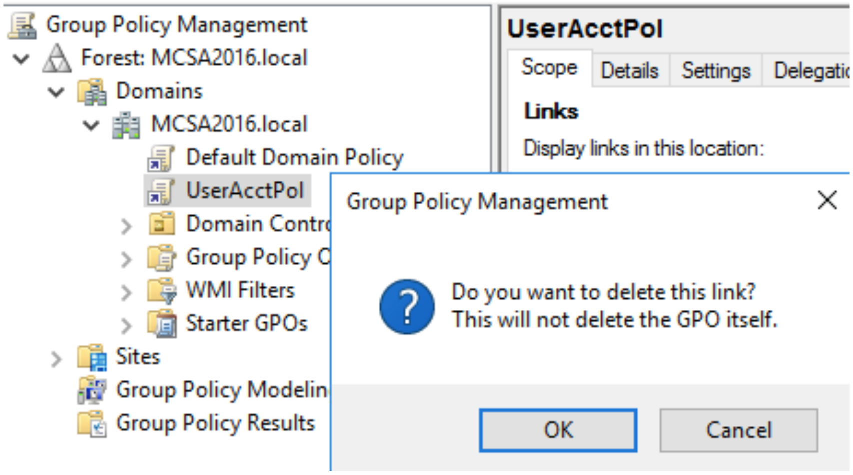
Test User1

The password is incorrect. Try again.

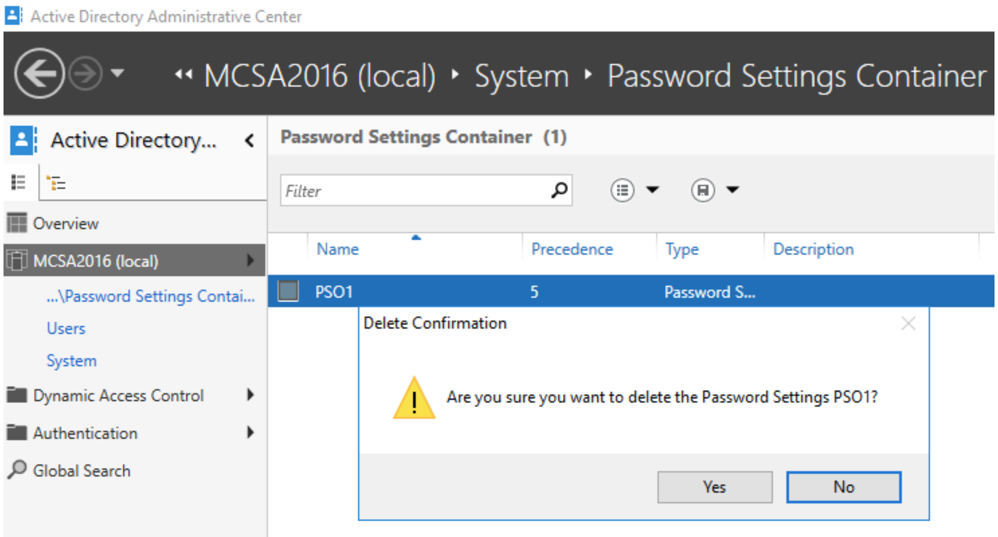


```
C:\Users\testuser1>hostname & echo %userdomain%
ServerDM1
MCSA2016

C:\Users\testuser1>logoff
```

- 3-5-9: Next, return account policies to their default values. On ServerDC1, open the Group Policy Management console. Expand the domain node so that you can see the two policies linked to it. Right-click **UserAcctPol** and click **Delete**. Click **OK** to confirm the deletion. That's it! No need to remember which policies to undo; by using a second GPO linked to the domain, you can simply link it or unlink it, depending on your policy requirements. In Active Directory Administrative Center, browse to the Password Settings Container, and then right-click **PSO1** and click **Delete**. Click **Yes** to confirm.



Do you want to delete this link?
This will not delete the GPO itself.



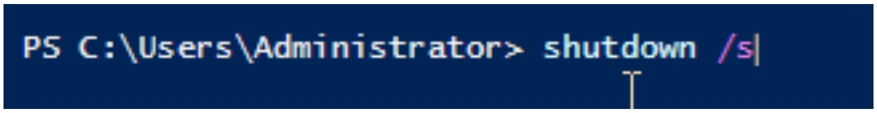
Active Directory Administrative Center
MCSA2016 (local) ‣ System ‣ Password Settings Container
Active Directory...
Overview
MCSA2016 (local)
...\Password Settings Contai...
Users
System
Dynamic Access Control
Authentication
Global Search
Password Settings Container (1)
Filter
Name
Precedence
Type
Description
Yes
No

Name	Precedence	Type	Description
PSO1	5	Password S...	

Delete Confirmation

Are you sure you want to delete the Password Settings PSO1?

- **3-5-10:** Shut down all servers.



```
PS C:\Users\Administrator> shutdown /s
```