# Week 4 Windows Server Activities - Active Directory

Activities

[Week 4 Windows Server Activities - Active Directory 1](#_Toc170907226)

[Activity 4-1: Exploring Active Directory Container Objects 1](#_Toc170907227)

[Activity 4-2: Viewing Default Leaf Objects 2](#_Toc170907228)

[Activity 4-3: Creating User Accounts in Active Directory 4](#_Toc170907229)

[Activity 4-4: Disabling, Renaming, and Enabling an Account 6](#_Toc170907230)

[Activity 4-5: Moving an Account 7](#_Toc170907231)

[Activity 4-6: Changing an Account’s Password 7](#_Toc170907232)

[Activity 4-7: Deleting an Account 8](#_Toc170907233)

[Assignment Submission 9](#_Toc170907234)

**How to Create Screenshots:** Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

# Activity 4-1: Exploring Active Directory Container Objects

Time Required: 10 minutes

Objective: Explore Active Directory container objects.

Required Tools and Equipment: Server1

Description: After installing Active Directory, you want to view its structure by exploring the default container objects in Active Directory Users and Computers.

1. Log on to Server1 as your administrator account.
2. In Server Manager, open Active Directory Users and Computers by clicking Tools, Active Directory Users and Computers from the menu.
3. Click the domain object (MyDomain.local) in the left pane.
4. Right-click the domain object and click Properties. Click the General tab, if necessary, and verify that both the domain and forest functional levels are Windows Server 2016. This is the highest level.
5. **Insert a screenshot:**

Click or tap here to enter text.

1. Enter a description for the domain, such as Windows Server 2019 Domain, and then click OK.
2. Click to expand the domain node, if necessary. Click the Builtin folder in the left pane to view its contents in the right pane: a list of group accounts created when Active Directory was installed.
3. Click the Computers folder in the left pane. This folder is empty.
4. Click the Domain Controllers OU. A computer object representing your domain controller is displayed in the right pane. The DC Type column displays GC, meaning the domain controller is a global catalog server.
5. Click the Users folder in the left pane. The right pane displays groups and two user accounts created by default when Active Directory is installed.
6. Leave Active Directory Users and Computers open for the next activity.

# Activity 4-2: Viewing Default Leaf Objects

Time Required: 15 minutes

Objective: View the properties of a variety of leaf objects.

Required Tools and Equipment: Server1

Description: You want to learn more about Active Directory objects, so you view the properties of several default leaf objects.

1. If necessary, log on to Server1 as your administrator account, and open Active Directory Users and Computers.
2. Click to expand the domain node so that folders and OUs are displayed under it, and then click the Builtin folder.
3. In the right pane, right-click the Administrators group and click Properties (or double-click the Administrators group).
4. Click the General tab, if necessary. Notice that the option buttons under Group scope and Group type are disabled because you can’t change this information for built-in groups.
5. Click the Members tab. You should see one user and two groups listed as members. The Name column displays the name of the user or group member, and the Active Directory Domain Services Folder column displays the domain and folder or OU where the member is located. Groups can be nested, as shown here; the Domain Admins and Enterprise Admins groups are members of the Administrators group.
6. Click the Member Of tab. Because built-in groups can’t be members of any other group, the Add and Remove buttons are disabled.
7. Click the Managed By tab. An administrator can specify another user or group that has the right to manage this group. Click Cancel.
8. In the left pane of Active Directory Users and Computers, click the Domain Controllers OU. Double-click the Server1 computer object in the right pane to open its Properties dialog box.
9. If necessary, click the General tab. Notice that only the Description text box can be changed for this object.
10. Click the Operating System tab, which displays the name, version, and service pack (if any) installed on the computer this computer object represents.
11. Click the Member Of tab. Because this computer object represents a domain controller, it’s a member of the Domain Controllers group. (If this computer object represents a domain member, it’s a member of the Domain Computers group.)
12. **Insert a screenshot.**

Click or tap here to enter text.

1. Click Cancel.
2. In the left pane of Active Directory Users and Computers, click the Users folder. Double-click the Administrator user to open its Properties dialog box.
3. If necessary, click the General tab. The information here is optional for user accounts but can be used as part of an employee directory. Type your first name and last name in the corresponding text boxes.
4. Click the Account tab. Here you can specify the user logon name, logon restrictions, and account options.
5. Click the Member Of tab. Note the groups the Administrator account belongs to.
6. **Insert a screenshot.**

Click or tap here to enter text.

1. Click Cancel.
2. Find the Guest user and notice the down arrow on its icon. Double-click the Guest user to open its Properties dialog box.
3. Click the Account tab. In the Account options list box, scroll down to view the available account options. The down arrow on the Guest user icon means the Guest user is disabled by default because it’s created with a blank password, which can pose a security risk. Click Cancel.
4. Leave Active Directory Users and Computers open for the next activity.

# Activity 4-3: Creating User Accounts in Active Directory

Time Required: Approximately 15 minutes

Objective: Learn how to create a user account in Active Directory.

Description: Management and access to resources through Active Directory begins through user accounts. In this activity, you learn how to set up a new account.

1. Open Active Directory Users and Computers.
2. Right-click the top domain in the tree in the left pane, **MyDomain.local**, point to New, and click **Organizational Unit**.
3. Enter **Employees**. Click OK.
4. Under the **Employees** OU, create a **Sales** OU and an **Accounting** OU.
5. Right Click the **Sales** OU, and Click New, User.
6. Type **Sales1** in the first name box, **Test** in the Last name box. Enter **Sales1** in the User logon name box.
7. **What options are automatically completed for you?**

Click or tap here to enter text.

1. **Insert a screenshot:**

Click or tap here to enter text.

1. Click Next.
2. Use **Password02** as the password. Ensure the box is checked for User must change password at next logon. This option forces users to enter a new password the first time they sign in, so that the account creator will not know their password. The other options include:   
   **User cannot change password:** This means that only the account administrator can change the user’s password.  
   **Password never expires:** This is used in situations in which an account must always be accessed, such as when a program accesses an account to run a special process  
   **Account is disabled:** This provides a way to prevent access to an account without deleting it. The Windows Server 2019 default password requirements are enabled when you create an account. A password must be seven characters or longer and cannot contain the account name or portions of the user’s full name (beyond two characters of the name). Also, a minimum of three of the following four rules apply: includes numbers, includes uppercase letters, includes lowercase letters, includes characters such as $, #, and !.
3. Click Next.
4. Verify the information you have entered and click Finish.
5. To continue configuring the account, in the middle pane, double-click the account you just created, **Sales1** (alternatively, you can right-click the account and click Properties).
6. **Insert a screenshot:**

Click or tap here to enter text.

1. Notice the tabs that are displayed for the account properties.
2. Click the General tab, if it is not already displayed, and enter a description of the account, such as Test account.
3. Click the Account tab to view the information you can enter on it.
4. Click the tabs you have not yet viewed to find out what information can be configured through each one.
5. Click OK.
6. Startup **Win11**. Click Other User to logon to the domain. Logon to **Win11** as **Sales1**. Change the password when requested to **Password01**.
7. Click the Start button, point your mouse at the top icon on the left that will show your username.
8. **Insert a screenshot:**

Click or tap here to enter text.

# Activity 4-4: Disabling, Renaming, and Enabling an Account

Time Required: Approximately 5 minutes

Objective: Practice disabling, renaming, and then enabling an account.

Description: In this activity, you learn how to disable an account, rename the account, and then enable that account.

1. Logon to **Server1**.
2. Access **Active Directory Users and Computers**, or if it is closed, open it.
3. Browse to find the account, **Sales1**, you created in the previous activity.
4. Right-click the account and click **Disable Account**.
5. Click OK when you see the informational dialog box that verifies you have disabled the account. The account icon will have a down arrow inside a white circle to show that it is disabled. No one can use the account until you enable it.
6. To rename the account, right-click it and click Rename. Enter a new name, **Sales2**, and then press Enter.
7. When you see the Rename User dialog box, change the First name and the Last name boxes to reflect the new name. Change the User logon name, **sales2**. Click OK.
8. Make sure the account is now listed as **Sales2** in the Sales OU.
9. **Insert a screenshot:**

Click or tap here to enter text.

# Activity 4-5: Moving an Account

Time Required: Approximately 5 minutes

Objective: Practice moving an account.

Description: If your organization uses OUs to reflect different departments, then you might need to move accounts between OUs as people are transferred to different departments. In this activity, you move the account you renamed to a different OU.

1. Access the MMC console window for Active Directory Users and Computers, or if it is closed, open it.
2. Right-click the account you renamed, **Sales2**.
3. Click Move.
4. In the Move dialog box, find the Accounting OU, and click it. Click OK.
5. In the tree of the left pane, click the OU to which you moved the account and verify that the account is moved (see the middle pane).
6. **Insert a screenshot:**

Click or tap here to enter text.

1. Drag **Sales2** back to the **Sales OU**.
2. Leave the Active Directory Users and Computers MMC console window open for the next activity.

# Activity 4-6: Changing an Account’s Password

Time Required: Approximately 5 minutes

Objective: Practice changing an account’s password.

Description: One of the most common account management tasks is resetting passwords. In this activity, you learn how to reset the password for a user.

1. Access the MMC console window for Active Directory Users and Computers, or open it if it is closed.
2. Open the **Sales OU**, if it is not already open, so that you can see the account you created and renamed.
3. Right-click the account for which you want to reset the password, **Sales2**.
4. Click Reset Password.
5. **Insert a** screenshot**:**

Click or tap here to enter text.

1. Enter the new password and then confirm it. Use Password01 as the new password.
2. Ensure that the box is checked for User must change password at next logon. Checking this box enables you to force the user to change the password by Microsoft and often a requirement of financial auditors who scrutinize networks that handle financial information. Notice that you can also unlock an account that has been locked. You might need to unlock an account when a user has unsuccessfully tried to sign in too many times and the account goes into a locked status for a prespecified interval.
3. Click OK in the Reset Password dialog box. Click OK in the information message box.
4. Leave the MMC console window for Active Directory Users and Computers open for the next activity.

# Activity 4-7: Deleting an Account

Time Required: Approximately 5 minutes

Objective: Practice deleting an account.

Description: In this project, you delete the account that you renamed.

1. Access the MMC console window for Active Directory Users and Computers, or open it if it is closed.
2. Open the **Sales OU**, if it is not already open, so that you can see the account you created and renamed.
3. Right-click the account you want to delete, **Sales2**, and click Delete.
4. **Insert a screenshot:**

Click or tap here to enter text.

1. Click Yes to verify that you want to delete this account.
2. Leave the MMC console window for Active Directory Users and Computers open for the next activity.

# Assignment Submission

Attach this completed document to the assignment in Blackboard.