# Week 5 Windows Server Activities - Active Directory

Activities

[Week 5 Windows Server Activities - Active Directory 1](#_Toc177451313)

[Activity 5-1: Creating an OU Structure 1](#_Toc177451314)

[Activity 5-2: Creating Domain Local and Global Security Groups 2](#_Toc177451315)

[Activity 5-3: Locating Objects with Active Directory Users and Computers 5](#_Toc177451316)

[Activity 5-4: Exploring Default GPOs 6](#_Toc177451317)

[Activity 5-5: Working with Group Policies 8](#_Toc177451318)

[Activity 5-6: Creating User Accounts in Active Directory Administrative Center 10](#_Toc177451319)

[Activity 5-7: Editing Multiple Accounts 11](#_Toc177451320)

[Activity 5-8: Working with Default Groups 12](#_Toc177451321)

**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 5-1: Creating an OU Structure

Time Required: 10 minutes

Objective: Create OUs to reflect a company’s departmental structure.

Required Tools and Equipment: Server1

Description: You have been asked to finish creating the OU structure for a business with five main departments: Accounting, Administration, Sales, Research, and Operations. You create an OU structure based on these requirements, using Active Directory Administrative Center for this task.

1. Log on to Server1 as your administrator account, if necessary.
2. Open **Active Directory Users and Computers**.
3. In the left pane, right-click the Employees OU, which was created earlier, point to New, and click Organizational Unit.
4. In the Name text box, type **Administration**. Leave the other settings at their defaults and click OK.
5. Repeat Steps 3 and 4 to create the **Research** and **Operations** OUs. When finished, click the domain node in the left pane to display the folders and OUs in the middle pane, if necessary. You should have Accounting, Administration, Operations, Research, and Sales.
6. **Insert a screenshot:**
7. Click or tap here to enter text.
8. Close Active Directory Administrative Center. If you’re continuing to the next activity, stay logged on; otherwise, log off or shut down Server1.

# Activity 5-2: Creating Domain Local and Global Security Groups

Time Required: Approximately 15 minutes

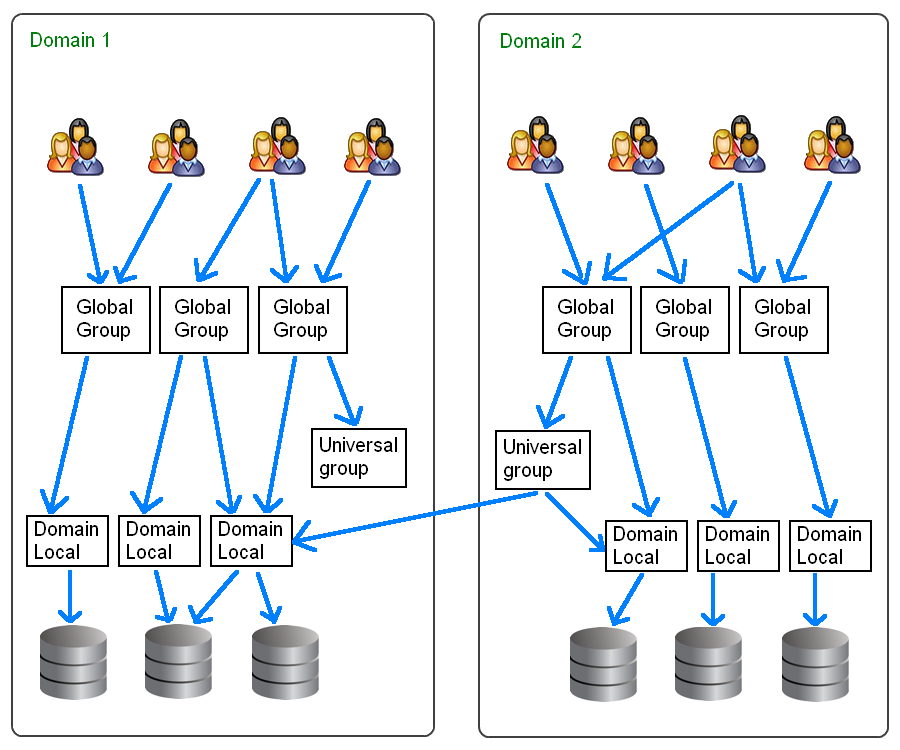
Objective: Create a domain local and a global security group and make the global group a member of the domain local group.

A domain local group is the main security principal recommended for assigning rights and permissions to domain resources. Although both global and universal groups can also be used for this purpose, Microsoft best practices recommend using these groups to aggregate users with similar access or rights requirements. Global and universal groups should then be added as members of domain local groups, which are added to a resource’s DACL. The process can be summarized with the abbreviations AGDLP and AGGUDLP. In single-domain environments or when users from only one domain are assigned access to a resource, use AGDLP:

1. **A**ccounts are made members of
2. **G**lobal groups, which are made members of
3. **D**omain **L**ocal groups, which are assigned
4. **P**ermissions to resources

Description: In this activity, assume that you have been asked to set up groups to manage access for the managers in an Active Directory that has four domains. You will practice beginning the setup by creating a domain local group that will be used to manage resources and a global group of accounts. Last, you will add the global group to the domain local group. Use the administrator level account you created earlier.

**Users >> Global >> Domain Local >> Resources**



1. Open Active Directory Users and Computers that you have been using.
2. In the tree in the left pane, display the contents under the domain, MyDomain.local
3. Create 2 new users in the Administration OU, Administration1 and Administration2. Use Test as their last names. Ensure the box is checked for User must change password at next logon.
4. Create 2 new users in the Sales OU, Sales1 and Sales2. Ensure the box is checked for User must change password at next logon.
5. Do the same for Research and Operations.
6. In the Sales OU, Click the **Action** menu 🡪 **New** 🡪 **Group**.
7. In the Group name box, enter **DL\_Sales**
8. Click Domain local under Group scope, and click Security (if it is not already selected) under Group type.
9. Click OK and then look for the group you just created in the right pane within the Sales OU.
10. Click the Create a new group in the current container icon on the button bar (with two heads).
11. In the Group name box, type **G\_Sales**
12. Ensure Global is selected under Group scope and that Security is selected under Group type.
13. Click OK and then look for the group you just created in the right pane.
14. Use the same instructions to create groups for Administration, Research, and Operations.
15. In the **Sales OU**, Double-click **G\_Sales**.
16. Click the Members tab. Notice that no members are currently associated with this group.
17. Click the Add button.
18. Click the Advanced button in the Select Users, Contacts, Computers, Service Accounts, or Groups dialog box.
19. Click Find Now.
20. Click Sales1, then hold down the CTRL key and click Sales2. Click OK.
21. Make sure that the users you selected are shown in the Select Users, Contacts, Computers, Service Accounts, or Groups dialog box. Click OK.
22. Be sure that both accounts are shown in the global group’s Properties box on the Members tab.
23. **Insert a screenshot:**
24. Click or tap here to enter text.
25. Click OK.
26. Do this same process for the other OU’s.
27. Add each Global Group to the corresponding Domain Local Group.
28. Double Click **DL\_Sales**, and show the Member tab.
29. **Insert a screenshot:**
30. Click or tap here to enter text.
31. Close the MMC console window and click Yes to save the console settings, if you have not done this previously. If you are saving the settings, click Desktop in the left portion of the dialog box. Enter a name for the console, such as Manage Accounts, and click Save.

# Activity 5-3: Locating Objects with Active Directory Users and Computers

Time Required: 5 minutes

Objective: Search for user and group objects with Active Directory Users and Computers.

Required Tools and Equipment: Server1

Description: Before Active Directory grows too large, you need to experiment with the search feature in Active Directory Users and Computers so that you’re comfortable finding objects.

1. If necessary, log on to Server1 as your administrator account, and open Active Directory Users and Computers.
2. Right-click the domain node in the left pane and click Find.
3. Click the Find list arrow and verify that Users, Contacts, and Groups is selected. In the In text box, make sure the domain is selected. You could click Find Now, but if you do, all users, contacts, and groups in the entire domain are displayed. You want to narrow down the choices first.
4. In the Name text box, type **user**. By specifying this name, all users, groups and contacts containing the word “user” are displayed. Click the Find Now button.
5. **Insert a screenshot:**

Click or tap here to enter text.

1. In the Search results section, you can double-click any entry to access its properties.
2. Close the Find Users, Contacts, and Groups dialog box and Active Directory Users and Computers

# Activity 5-4: Exploring Default GPOs

Time Required: 15 minutes

Objective: Explore the two default GPOs in Active Directory.

Required Tools and Equipment: Server1

Description: You want to begin using GPOs to manage users and computers in your network, so as a first step, you decide to familiarize yourself with the default GPOs linked to the domain and the Domain Controllers OU.

1. Log on to **Server1** with your administrator account, if necessary.
2. In Server Manager 🡪 **Tools** 🡪 **Group Policy Management**.
3. In the left pane, click to expand the Forest and Domains nodes, if necessary. Click to expand **MyDomain.local** under the Domains node, if necessary.
4. Click **Default Domain Policy**. If a Group Policy Management console message is displayed, read the message, click the Do not show this message again check box, and then click OK.
5. In the right pane, click the Scope tab, if necessary. The Links section shows you which container objects are linked to this GPO. In this case, your domain should be the only container linked. All objects in a container linked to the GPO are affected by that GPO.
6. Click the Settings tab. (The settings might take a few seconds to be displayed.) You can view GPO settings here, but you can’t change them.
7. **Insert a screenshot of the expanded settings tab:**

Click or tap here to enter text.

1. The two main nodes are highlighted: Computer Configuration and User Configuration. Click the show all link to expand the settings. Only nodes that have configured settings are shown.
2. Scroll through the settings for the Default Domain Policy, which pertain to user account settings, such as password policies, or security. Take some time to see how Windows initially configures security settings for the domain. You might want to make changes to the default security settings on your own domain. Notice that no settings are displayed under the User Configuration node because no settings have been configured.
3. **Insert a screenshot:**

Click or tap here to enter text.

1. Click to expand Domain Controllers in the left pane, and then click Default Domain Controllers Policy.
2. In the right pane, click the Settings tab, if necessary, and then click show all. Scroll through the settings for the Default Domain Controllers Policy. Most pertain to user rights assignments, such as which users are allowed to log on to the computer locally or change the system time. Again, take some time to see how Windows initially configures security settings for domain controllers.
3. **Insert a screenshot:**

Click or tap here to enter text.

1. Right-click Default Domain Policy in the left pane and click Edit to open the Group Policy Management Editor.
2. If necessary, click to expand Computer Configuration and User Configuration. Under Computer Configuration, click to expand the Policies folder. You see the three folders described earlier.
3. Click to expand Windows Settings and then Security Settings. Click to expand the Account Policies node and explore the settings in this node and the nodes under it. By default, account policies are defined only in the Default Domain Policy, and all domain users are subject to these settings.
4. **Insert a screenshot:**

Click or tap here to enter text.

1. Click to expand the Local Policies node and explore the three nodes under it. Most settings in Local Policies are displayed as Not Defined. In fact, only three policies in the Local Policies node are defined.
2. **What are these three policy groups?**

Click or tap here to enter text.

1. Browse through some nodes in the Policies folder under User Configuration. No policies are configured in this node. Configuration of user policies is up to the server administrator.
2. Close the Group Policy Management Editor. In the Group Policy Management console, click to expand Domain Controllers, if necessary, and then right-click Default Domain Controllers Policy and click Edit.
3. Under the Computer Configuration node, click to expand the Policies folder, if necessary, and then click to expand Windows Settings and then Security Settings. Click to expand Account Policies and Local Policies and explore the settings in these nodes. Notice that no account policies are defined, but a number of user rights assignments are. Default settings that apply to domain controllers focus on what types of actions users can perform on domain controllers. Most actions are limited to members of the Administrators, Backup Operators, and Server Operators groups.
4. **Insert a screenshot of one of the policies in this area:**

Click or tap here to enter text.

1. Take some time to explore several GPOs to familiarize yourself with what’s available. Leave the Group Policy Management console open for the next activity.

# Activity 5-5: Working with Group Policies

Time Required: 10 minutes

Objective: Create a GPO and see how policies you configure affect user objects in the OU to which the GPO is linked.

Required Tools and Equipment: Server1

Description: You want to see how some group policy settings affect users in your domain. You know that you want to restrict some users’ access to Control Panel, so you decide to start with this policy. Because you want the policy to affect certain users, you configure it in the User Configuration node.

1. If necessary, log on to Server1 as your administrator account, and open the Group Policy Management console.
2. Click to expand the Forest and Domains nodes and then the domain node, if necessary.
3. Right-click the Sales OU (created earlier). Click Create a GPO in this domain and Link it here. In the New GPO dialog box, type **Remove Control Panel and Settings** in the Name text box, and then click OK.
4. In the left pane, click to expand the Sales OU, and then right-click **Remove Control Panel and Settings** and click Edit to open the Group Policy Management Editor.
5. Go to **User Configuration 🡪 Policies 🡪 Administrative Templates 🡪 Control Panel**. In the right pane, double-click the **Prohibit access to Control Panel and PC settings** policy to open the dialog box.
6. Read the description of the policy in the Help box, and then click the Enabled option button. Note that there are three possible settings: Enabled, Disabled, and Not Configured. If the policy is enabled, users affected by the policy are prohibited from accessing the Control Panel and PC settings. If the policy is disabled, users have access. If the policy is not configured, it has no effect on users’ access to the Control Panel and PC settings. Click OK. Notice that the State column in the Group Policy Management Editor for the policy you changed then shows “Enabled.”
7. **Insert a screenshot:**

Click or tap here to enter text.

1. Close the Group Policy Management Editor and Group Policy Management console.
2. Log on to Win11 as **Sales1**. To do so, after you press Ctrl+Alt+Delete, click Other user. Type sales1 in the User name text box and Password01 in the Password text box, and then press Enter.
3. After you’re logged on, Click Start, type in Control Panel, and try to access the Control Panel. In the Restrictions message box stating that the operation has been cancelled because of restrictions on the computer.
4. **Insert a screenshot:**

Click or tap here to enter text.

1. Click OK.
2. Right-click the desktop and click Screen Resolution. In the same Restrictions message box, click OK. Your policy has clearly taken effect. (If you see an Explorer.EXE message box stating “Unspecified error,” click OK.)
3. **Insert a screenshot:**

Click or tap here to enter text.

1. Log off Server1 and Win10. Shut down the server and the workstation unless you’re continuing to the next activities.

In this activity, you might have noticed a delay between setting a policy and the policy taking effect. You can run the command-line program gpupdate.exe, which applies group policies immediately to the computer on which gpupdate.exe is running and to the currently logged-on user. This program is an invaluable tool for testing GPOs because it saves considerable time. As mentioned, computer policies are applied when a computer restarts, which can take some time, and user policies are applied when a user logs on. GPOs are also updated on domain controllers every 5 minutes and on workstations and servers every 90 minutes, even if the computers don’t restart.

# Activity 5-6: Creating User Accounts in Active Directory Administrative Center

Time Required: 10 minutes

Objective: Create a user account in Active Directory Administrative Center.

Required Tools and Equipment: Server1

Description: You understand there are some differences in account creation when using ADAC, so you decide to create a test user with this tool.

1. Log on to Server1 with your administrator account, if necessary, and open Active Directory Administrative Center.
2. Click the domain node. In the middle pane, right-click Employees point to New, and click User.
3. In the Create User window, notice the two fields with asterisks next to them: Full name and User SamAccountName logon. In Active Directory Administrative Center, only these two fields are required to create a user. Type Test User7 in the Full name box and testuser7 in the User SamAccountName logon box.
4. Press the Enter key to create the user.
5. In Active Directory Administrative Center, double-click Employees and notice that Test User7 is grayed out and has a down arrow icon to indicate the account is disabled. (If you don’t see Test User7, refresh the view.) Right-click Test User7 and click Enable. In the message stating that the password doesn’t meet complexity requirements, click OK. You can’t enable the account until a suitable password has been set.
6. Right-click Test User7 and click Reset password. In the Reset Password dialog box, type Password01 in the Password and Confirm password text boxes, and then click OK.
7. Right-click Test User7 and click Enable. The account is enabled.
8. At the bottom of Active Directory Administrative Center, you see the Windows PowerShell History. Click the up arrow on the right to expand the Windows PowerShell History Viewer.
9. Scroll to the top of the history, if necessary, to see the **New-ADUser** command. Click to select New-ADUser and click Copy on the viewer’s menu bar.
10. Open Notepad and paste the Clipboard contents into Notepad. You see the full PowerShell command that was generated when you created Test User6. Close Notepad without saving the file.
11. Scroll through the PowerShell history to see other commands that were generated for setting the password and other account properties. It isn’t obvious which command enables the account. Find the last Set-ADObject command in the history. The userAccountControl=8389120 part of the command is what does the job. This parameter sets account properties that specify the account is a normal user and the password must be changed at next logon.
12. **Insert a screenshot:**

Click or tap here to enter text.

1. Although the PowerShell commands generated by Active Directory Administrative Center aren’t always the most straightforward way to accomplish a task (the Enable-ADAccount cmdlet is more straightforward), they can help you learn how to use these commands for writing scripts. Close Active Directory Administrative Center.
2. If you’re continuing to the next activity, stay logged on; otherwise, log off or shut down the computer.

# Activity 5-7: Editing Multiple Accounts

Time Required: 10 minutes

Objective: Create users and change attributes on several accounts simultaneously.

Required Tools and Equipment: Server1

Description: You need to change some attributes on several users in your Sales OU, so you decide to use the Properties for Multiple Items dialog box to make this task easier.

1. If necessary, log on to Server1 as Your administrator account, and open Active Directory Users and Computers.
2. Click to expand the Marketing OU, if necessary, and then click the Sales OU.
3. Create two user accounts by using the \_Sales Template account. The accounts should have the first and last names Sales Person2 and Sales Person3 and logon names **SalesPerson2** and **SalesPerson3**. Enter Password01 for the password on both accounts. Make sure the Account is disabled check box is selected. Click to clear the User must change password at next logon check box so that these users don’t have to change their passwords.
4. After you have created the two users, click Sales Person1, and then hold down Shift and click Sales Person3. Release Shift, and then click Action, Properties from the menu to open the Properties for Multiple Items dialog box.
5. **Insert a screenshot showing multiple properties:**

Click or tap here to enter text.

1. Click the Description check box, and then type AACN Sales Person in the text box. Click the Web page check box, and then type www.allaboutcomputernetworks.com in the text box.
2. Click the Account tab. Scroll down in the Account options list box and click to select the Account is disabled check box on the far left. Click Apply.
3. Click the Address and Profile tabs to review which attributes you can change. Click the Organization tab. Click the Job Title check box, type Sales Associate in the text box, and then click OK.
4. Open the Properties dialog box for each Sales Person user to verify that the changes were made for all. When you’re finished with each one, click OK.
5. Leave Active Directory Users and Computers open if you’re continuing to the next activity; otherwise, log off or shut down the computer.

# Activity 5-8: Working with Default Groups

Time Required: 5 minutes

Objective: View properties of default groups.

Required Tools and Equipment: Server1

Description: You want to see the scope and membership of some default groups that Windows creates.

1. If necessary, log on to Server1 as Your administrator account, and open Active Directory Users and Computers.
2. Click the Builtin folder. Click the Administrators group and open its Properties dialog box. The options in the Group scope and Group type sections are disabled because you can’t change the scope or type of groups in the Builtin folder. Notice that the selected scope is Builtin local. These groups are considered domain local, but there are some differences between Builtin local and other domain local groups, as you’ll see.
3. Click the Members tab to see this group’s members, and then click Cancel.
4. Next, view the membership of the Guests and Users groups. Notice that the Users group has two special identities as members: Authenticated Users and Interactive. Close both Properties dialog boxes.
5. Click the Users folder. Click **Domain Admins** and open its Properties dialog box. Click the General tab, if necessary. Notice that you can’t change this group’s scope or type. Click the Members tab to view the group membership, and then click Cancel.
6. Next, view the membership of the **Domain Users** group. Notice that all the users you have created became members of this group automatically.
7. **Insert a screenshot of the members of the Domain Users group:**

Click or tap here to enter text.

1. Close this Properties dialog box.
2. View the membership of the Domain Computers group. There are currently no members, but after a computer is joined to the domain, the computer account is added to this group.
3. To see the groups your currently logged-on account is a member of, open a command prompt window. Type **whoami /groups** and press **Enter**. You see a long list of groups the local administrator is a member of, including several special identity groups, such as Everyone, Interactive, Authenticated Users, and Local. In the output, these groups are identified as well-known groups.
4. **Insert a screenshot of the results of the command.**

Click or tap here to enter text.

Attach this completed assignment and submit in Blackboard.