# Overview

Delegation of administrative control is done to distribute the load of managing an Active Directory domain. This is normally done to allow administrators in remote locations to administer the users and workstations at their location. It can also be used to give a group permission to manage a specific type of object like users or computers. In this lab, you will explore Active Directory permissions and use the delegation of administrative control wizard to assign permissions to groups.

# Objectives

* Be able to view and explain the security descriptor for and AD object.
* Be able to configure security for AD objects.

## Skills Reviewed

* Viewing security descriptors.
* Using AD Users and computers.
* Creating AD groups.
* Adding AD users to groups.

## New Skills

* Using the delegation of administrative control wizard.

## References

**Delegating Administration by Using OU Objects** - <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/delegating-administration-by-using-ou-objects#:~:text=To%20delegate%20administration%20by%20using,the%20OU%20to%20that%20group>.

# Initial Conditions

Your virtual machine should be in this state prior to beginning this guided practice:

* Guided Practice – Creating Active Directory Objects complete

# Final Conditions

At the end of this exercise:

* **GV-Admin** group created and given full control of the Greenville OU.
* **CO-Admin** group created and given full control of the Columbia OU.
* **GV-PassAdmin** group created and delegated permission to reset passwords for users in the Greenville OU.

## Viewing AD object SEcurity descriptors

To determine which users have permission to view or modify Active Directory objects, you need to be able to view the security for these objects. In this step, you will use AD Users and Computers to view the permissions on an AD object.

View the security descriptor for the domain object in AD by performing the following:

1. Login to the **Server-01** virtual machine
2. Open **Active Directory Users and Computers.**
3. Configure **Active Directory Users and Computers** so that you can view the **Advanced Features.**
4. Open the **Properties** for the **KMW.local** domain object.
5. Select the **Security** tab **to** **view** its **discretionary access control list (DACL).**
6. Use the **DACL** to fill in the table below.

|  |  |
| --- | --- |
| Group | Permissions |
| Everyone |  |
| Authenticated Users |  |
| System |  |
| Domain Admins |  |
| Enterprise Admins |  |
| Administrators |  |

1. When you are done, close the dialog box.

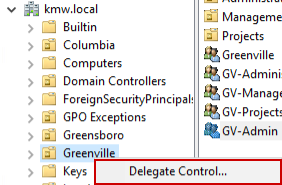
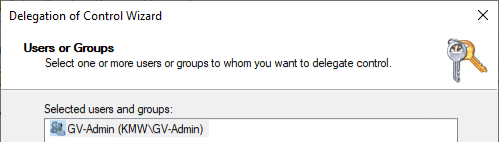
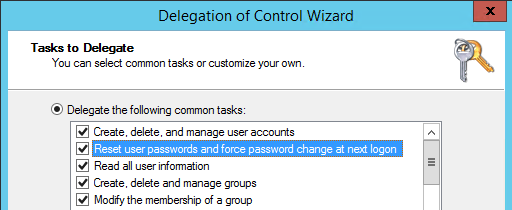
## Using the Delegation of Administrative Control wizard

The Delegation of Administrative Control Wizard is the easiest way to assign granular permissions to objects in the domain or OU.

### Granting Full Control Permissions to the objects in an OU

Your organization would like to give the GV-Admin group permissions to manage all the objects in the Greenville location.

Delegate administrative control of **Greenville** to the **GV-Admin** group, perform the following:

1. In **Active Directory Users and Computers**, create a new global group named **GV-Admin** in the **Users** container.
2. Browse to the **Greenville** OU and select **Delegate Control…** from the **context menu** to launch the **Delegation of Control** wizard as shown in the figure.
3. On the **Welcome to the Delegation of Control Wizard** page of the wizard, read the page and click the **Next** button.
4. On the **Users or Groups** page of the wizard, click the **Add…** button and add the **GV-Admin** group and then click the **Next** button.
5. On the **Tasks to Delegate** page of the wizard, **select** the following tasks and **click** the **Next** button:
   1. Create, delete, and manage user accounts.
   2. Reset user passwords and force password change at next logon.
   3. Read all user information.
   4. Create, delete, and manage groups.
   5. Modify the membership of a group.
6. On the **Completing the Delegation of Control Wizard** page of the wizard, **review** the results and click the **Finish** button.
7. Verify the settings by viewing the security tab in the properties for the **Greenville** OU object and verifying the permissions.
8. Create a **CO-Admin** group and **Repeat** the procedure above to give **CO-Admin** group control of the **Columbia** OU.
9. Add **Albert Carr** to the **GV-Admin** group.
10. Add **Mary Freeman** to the **CO-Admin** group.

### Granting Password Reset Permissions for Objects

Your organization would like to delegate the task of resetting passwords in the Greenville location to a group called **GV-PassAdmin**. To do this, perform the following:

1. Create a group in the **Greenville** OU called **GV-PassAdmin.**
2. Select **Delegate Control…** from the context menu for the **Greenville OU.**
3. Complete the wizard using the information below
   1. Users or Groups: **GV-PassAdmin.**
   2. Tasks to Delegate: **Reset user passwords and force password change at next logon.**
4. Addthe user **Sara Galloway** (sagalloway) in the Greenville Management department to the **GV-PassAdmin** and verify the user can **reset** **passwords** for users in the Greenville OU.

## Testing Delegation of Administrative Control

1. Login to **Client-01** as **Sara Galloway.**
2. Download and install the **RSAT** tools. Starting with Windows 10 October 2018 Update (Build 1809), RSAT is included as a set of **Features on Demand** in Windows 10 itself. The **Remote Server Administration Tools**, RSAT, must be added using **DISM.exe**. Execute the following command to add RSAT for Active Directory

dism /online /add-capability /CapabilityName:RSAT.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0

1. Open an **MMC** console and **add** the **Active Directory Users and Computers** Snap-In.
2. Reset the **password** of a **user** in the **Greenville** OU.

## Submission Requirements

1. **Download** the **grading** **script** from the assignment page to the **C:\Scripts** folder.
2. Check your lab by running the following command:

Invoke-Pester -Path C:\Scripts\GP21-Delegating\_ Administrative\_Control.test.ps1

**Note**: You will see a security warning when running the script. Enter **R** to run the script.

If you want to see more detail, add **-Output Detailed** to the command. This may assist you with troubleshooting

Invoke-Pester -Path C:\Scripts\GP21-Delegating\_ Administrative\_Control.test.ps1 -Output Detailed

1. You should not see any red in the output. Red in the PowerShell way of telling you that an error condition exists. Most of the time, the output will tell you what is wrong. If it is not obvious, contact your teacher and ask for assistance. You will be learning PowerShell during this term. **Correct** any **errors** you may have and run the script until all the output has no red. You should see the output like the images below

Text, chat or text message

Description automatically generated

1. Capture a snippet that shows the PowerShell Command and all its output. If you must use more than one snippet to capture the output, you must have at least **one line of overlap** in the snippets. The text in the snippets **must be legible** when pasted into the Word document. Paste the snippet(s) into a **new** **Word** **document**
2. **Upload** the **document** in the submission area of the assignment.