# Windows Server – Setup and Configuration

# Section 3 – Organizational Units and Policies

## Part 1: Organizational Units

Group polices are a mechanism that allows control of both users and computers in the Active Directory network. In this lab you will learn to work with OUs and Group Policy Objects (GPOs) for your organization.

Organization units have several purposes. They allow users and computers to be grouped in a logical manner for administration, they allow delegation of control so certain individuals can provide administration to a subgroup of users and computers without having wider administrative capabilities and they provide the primary method of applying group policies to user and computer accounts.

Group Policies can be applied at the Site, Domain or OU level. Most polices are linked at the OU level because that give the most granular control of policy settings. Polices linked to the Site will be inherited by all users and computer in any domain contained in that site. Polices liked to the domain will be inherited by any uses and computers is OUs within that domain. Policies liked to an OU will be applied to all uses and computers in that OU and any child OUs under that OU.

Therefore, one of the important considerations in the design of a domain is the OU structure because that will determine how group polices can be linked and applied. There is no single preferred method of designing an OU hierarchy. Designing the OU hierarchy is part of the art of Active Directory design.

We will design OUs based on departmental structure, with each department in the company given an individual branch of the OU hierarchy. Whether User and Computer objects are put the same OU or in separate OUs is another decision an administrator must make, and there is no single best option for all designs.

**In the following steps you will create an Organization Unit structure for your organization and place user accounts in the appropriate OUs.**

* Start **SRV16** and log on with your personal administrative account.
* Open Active Directory Users and Computers (ADUC) from the Tools menu of Server Manager.

Under the domain you will see a number of folder icons. Most of the icons you see here are not OUs but are simple containers. Simple containers have a blank folder icon. Organization Units have a folder icon that isn’t blank; you will see another small image within the folder icon. You cannot link GPOs directly to simple containers, and you cannot create sub containers under them, so they do not serve well for our GPO requirements. For that you need OUs.

* Take not of the OUs in the default domain configuration.
* **Highlight** the Domain container then right click on it and select first **New** then **Organizational Unit** form the cascading menus.

Graphical user interface, timeline

Description automatically generated with medium confidence

* Give the OU the name of TEST and leave the check mark checked to protect the OU from accidental deletion.
* After creating the new OU, right click on it in the left pane of ADUC and click **Delete**.

Take note of the warning message.

* Right click on the **Test** OU and select Properties. Take note of the tabs you see.
* Close the **Properties** window.
* Locate the Menu bar at the top of the ACUC window and click on the **View** title, then click on **Advanced Features** under View.
* Return to the **Test** OU, right click on it and select **Properties** again. You will see new tabs now that you are in Advanced View mode.
* Click on the **Object** tab and uncheck the box for **Protect object from accidental** deletion and then click OK.

Graphical user interface, text, application, email

Description automatically generated

* Return to the left pane of ADUC and delete the Test OU. Don’t continue until you can delete the OU.
* Click on the View menu and uncheck the **Advanced Features** selection.
* Right click on the domain icon and create a new OU.
* Give the first OU the name All Departments.

Graphical user interface, application, timeline

Description automatically generated with medium confidence

* After creating the All Departments OU, right click on it and select New and then OU to create a child OU under All Departments. Name the new organizational unit **HR Dept**.
* Create child OUs under HR Department called **HR Users** and **HR Computers** as shown below.

Graphical user interface, text

Description automatically generated with medium confidence

* In the **Users** container of the domain (note that it is not an OU) locate the three member accounts of the HR Department and move them to the HR Users OU. You can use the mouse pointer to drag the user icons to the new OU, or you can right click on an account and select the **Move**… option from the menu. You can use the Ctrl or Shift keys to select multiple accounts to move at the same time.
* This is exactly where the user ‘Description’ from earlier comes in handy. You entered the ‘Description’ for each user, right?
* Next create OUs directly under the **All Departments** OU in the Widgets organization. Create separate OUs under each departmental OU for **users** and **computers** as you did with the HR department. Shown below.

Graphical user interface

Description automatically generated with medium confidence

* Move the Widgets users to the appropriate OUs as you did with the HR department.
* Close ADUC

## Part 2: Group Policy Management Console

* On your server logged on as your personal account open the Group Policy Management Console (GPMC) from the Tools menu of Server Manager.

Graphical user interface, text, application

Description automatically generated

* Expand the Forest, Domains, you domain, and finally the Group Policy Objects containers in the left pane of the application.

Graphical user interface, text, application, chat or text message

Description automatically generated

* Take note of Group Policy Objects (GPOs) that exist by default in your domain. (There will be only two.)
* Highlight (left click on) the domain’s icon. Below the icon you will see the **Default Domain Policy** icon. Note the small arrow in the icon in front of the printed name. The arrow indicates that this is a link to the policy, not the actual policy itself. Deleting the link will not delete the policy but editing the link will cause the main policy to change.
* Left click on the Default Domain Policy link and read the notice that appears. You can check the box, so you don’t see this message every time you click on a policy link.
* You should now see that the **Scope** tab is open in the right pane. Security filtering specifies the group membership needed for a user or computer to receive the settings from this policy (assuming the user or computer is in a container that receives the policy).

**What group is listed under Security Filtering?**

* Remember that the Authenticated Users group contains all security principles that log on with a username and password. This includes computer accounts!
* Click on the Details tab.
* After examining the information offered in this section, click on the arrow to expose the alterntives for **GPO Status.** Take note of the default.
* Next, click on the Settings tab.
* Click the **show all** link. This will show you all the settings in this policy. You should see that there are many settings in the Computer Configuration section.

If there are no settings in a GPO for one of the two sections (Computer and User Configurations) you can disable the unused section to improve system performance (if there are many GPOs)

* Under **Account Policies/Password Policy** settings record the defaults you see.

Enforce password history \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Maximum password age \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Minimum password age \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Minimum password length \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Password must meet complexity requirements \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Store passwords using reversible encryption \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* In the left pane of GPMC click on the **Domain Controllers** icon.
* In the right pane you should see three tabs. The first, Linked Group Policy Objects, should already be selected. This tab shows the polices linked directly to this container.
* Next, open the **Group Policy Inheritance** tab.

This shows all policies that will have an effect on users and/or computers in this OU and their order of precedence. The higher the level of precedence (the lower the precedence number) the more powerful the policy will be. Any conflicting settings between policies will result in the policy with the lowest precedence number taking priority over all others.

* Note the two default policies and their precedence numbers. The lower precedence number takes priority.
* In the left pane, **expand all the OUs under All Departments**. You should see all the OUs that you created in a previous lab exercise. If you do not see the correct OUs, many any necessary adjustments before proceeding.

Graphical user interface, application

Description automatically generated

* **Highlight on the OU for the HR Dept** and in the right pane click on Linked Group Policy Objects (the first tab).
* Linking a policy to this container will affect any users and/or computers in this container as well as any child containers (as long as none are set to Block Policy Inheritance).

## Part 3: Applying a Desktop Background with a GPO

In the next section, you will create and work with GPOs. However, you first need to do some preparation. In the next steps, you will prepare a shared folder for desktop background images.

* On **your server** use File Explorer to navigate to the root of the C: drive and create a folder called **wallpaper**.
* **Share** the **wallpaper** folder with the **Everyone**, Allow **Read** share permission.
* Move your desktop image file to the wallpaper folder.

In the next section you will create and link GPOs

* Return to GPMC on **the server** and left click on the HR Users OU to highlight it.
* **Right click on the HR Users** container and select the option to **Create a GPO in this domain….**
* In the New GPO dialog box give the policy the name **HR Desktops** and click OK. You will not make any changes in the Source Starter GPO box.
* **Expand the HR Users OU** and you should see a link for the new policy name. Right click on the **HR Desktops** link and select **Edit** from the menu.
* You will now be in the Group Policy Management Editor where you can make changes to the new policy. You should see two main sections, Computer Configuration and User Configuration. As you should know, setting placed in the Computer Configuration section apply to all computers no matter who is logged in to them. Settings in the User Configuration section apply to all users regardless of what computers they log onto.
* You will also see separate folders for **Policies** and **Preferences**. Polices are always enforced and users cannot change them. Preferences can be changed by uses one they are in place.
* In the left pane **expand User Configuration** > **Policies** > **Administrative Templates** > **Desktop** and then click on the **Desktop** folder underneath.

Graphical user interface, application

Description automatically generated

* In the right pane left click on the **Desktop Wallpaper** icon. You will see that the left pane is now divided onto two panes, one for explanations and one for settings. Near the bottom of the pane, you will see two tabs. Click on the **Standard** tab to remove the explanation section.
* **Double click on the Desktop Wallpaper option**.
* You will need to make three choices in this window. First you will click the **Enabled** radio button near the top. This will activate the policy setting.
* In the Wallpaper Name box, you will need to type in a network accessible location for the wallpaper file. You can’t use a designation like C: because this would point clients to their local C: drive. Instead, you need to **use the UNC name and path**. You will use the following:

**\\<servername>\wallpaper\hr\_wallpaper.jpg**

Graphical user interface, application

Description automatically generated

* When finish, click on OK at the bottom of the window and close the GPM Editor.
* Open a CMD Prompt on the **server** machine and run the **gpupdate /force** command to ensure the latest group policies are updated.

You have now created a user policy that will affect all users in the HR Users OU. In the next steps you will test the policy to see if it works.

* Switch to **the client**, log off your personal account and log on to an account that is a member of the HR Department, Cotton Malone. Verify the background change.
* In the next steps, you will create a computer policy and see how it applies to computers, no matter who logs on.
* At **SRV16** open GPMC and locate the Acct Computers OU. Create and link a new GPO to this OU called **Restrict Acct Computers**.
* Edit the new policy and navigate under the **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**

Graphical user interface, text, application

Description automatically generated

* Locate the policy for Allow Log on locally and double click on the setting.
* Check the box to Define these policy settings: then click on the box for Add User or Group.
* Click **Browse** then at the next window click **Advanced** and then click **Find Now**.
* Locate the **two Global groups** you created for the **Accounting Department (Managers and Staff) and add them to the list.** (Your group name may be different than those shown below.)
* after adding the two global groups, add the Administrators group. (The system won’t let you finish unless you add the Administrators.)
* Open a CMD Prompt on the **server** machine and run the **gpupdate /force** command to ensure the latest group policies are updated.

Graphical user interface, text, application

Description automatically generated Graphical user interface, text, application, email

Description automatically generated

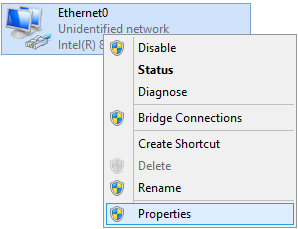
You have now created a policy that will only allow members of the Accounting Department and Administrators to log onto any computers in the Acct Computers OU. In the next steps, you will test the policy to see if it works.

* In **Active Directory Users and Computers**, locate the **client** computer icon in the Computers container and **move it to the Acct Computers OU**.
* Restart the client. When it restarts, try to log on as the cmalone account. This should fail.
* Now try to log on to **the client** with the jstone account. This should succeed because the jstone account should be a member of the AcctUsers group.
* Now try to logon with your personal account. You should be able to as a Domain Admin.

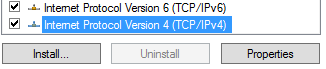
## Part 3: Set or Verify the Static IP Addresses

A Domain Controller must have a static IP address, so you must check this before the actual promotion process. In this section we will also check the static IP address for the **client** workstation computer to be sure they will be on the same subnet and can easily communicate.

* Login to **the server** as the Administrator and locate the computer network icon in to the left of the clock on the Task Bar, then right click on it and select **Network and Sharing Center**.
* Once in Network and Sharing Center, left click on **Change Adapter Settings** in the left pane.
* Right click on the **Ethernet** Icon and select **Properties**.



* Select (left click on) **Internet Protocol Version 4** and then click on **Properties**



* Verify and set the static IP info for **the server**

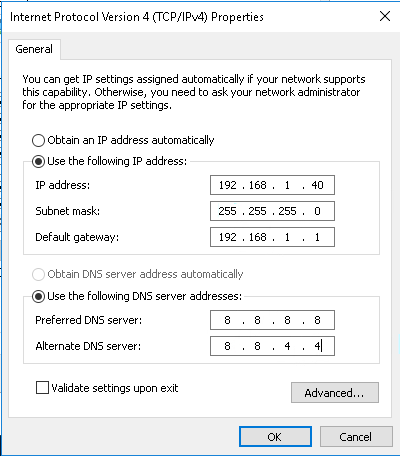
IP address: **<Pre Determined>**

Subnet mask: **<Pre Determined>**

Default gateway: **<Pre Determined>**

Preferred DNS Server: **<Pre Determined>**

Alternate DNS Server : **<Pre Determined>**



* Click OK and the close the various windows you opened.
* To verify that your settings are correct, open a command prompt and issue the IPCONFIG /ALL command.
* Verify you can connect to the default gateway by issuing the following command. (The command is not case sensitive: you could use upper or lower case.) You will need to fill in the values for xxx from your settings because various computers in the labs may have different values for the third octet.

PING <defaultgateway> (You may need to turn off the firewall)

* If this is successful, you should receive four successful connection messages
* Verify you can connect reach the public Internet by pinging one of the public DNS servers run by Google.

PING 8.8.8.8

* If this is successful, you should receive four successful connection messages
* Now switch to the **the client** computer and go to Control Panel and turn off the Firewall. Configure the **client** machine for a static IP address where the last octet is different. The result should be an address that differs from the server’s IP address only in the last octet.
* Configure the subnet mask, default gateway and DNS server addresses the same as you did for **the server**.
* Run IPCONFIG /All on both **the server** and **the client** and note the values for future reference below.

**server client**

IP Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Default Gateway: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Subnet Mask: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Preferred DNS \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Alternate DNS \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Use the PING command to verify that you can connect to the **client** IP address from the **server** computer.
* Use the PING command to verify that you can connect to the **server** IP address from the **client** computer.

Do not proceed until you can ping each of your computers from the other and can ping the Google DNS server at 8.8.8.8.

Now that you have a valid static IP address, you can promote your server to be a Domain Controller as described in the next part of the lab.

## Part 4: Promote Stand-Alone Server to Domain Controller

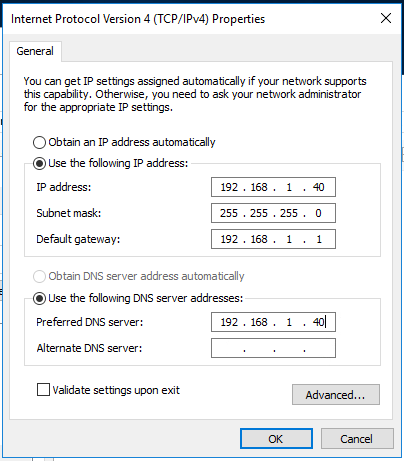
Domain Controllers allow for a central database of user and computer account information that greatly simplifies administration and security for all but the smallest networks. Domain controllers in the same domain maintain identical copies of the data base (through a process called replication) so that any domain controller in a domain can handle any authentication requests within that domain and can be used to make changes to the Active Directory (AD) data base.

Any Windows server can be promoted from a stand-alone server to a Domain Controller (DC). The actual steps in the process vary somewhat from one version of Windows to another, but the result is the same.

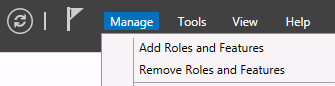
A Domain Controller can only hold data for a single domain. In other words, a Windows server can only be a DC for one Active Directory domain. To create a second domain, you need another domain controller. Domains within a Forest are connected with logical Trusts that allow users in one domain to be given access to resources in another domain.

When you decide to promote a server to become a DC you have to make a decision about the DC. Will it be the first domain in a new forest, a new domain in an existing forest, or a new Domain Controller in an existing domain? If you don’t have an Active Directory forest yet, there is only one valid answer: a new domain in a new forest.

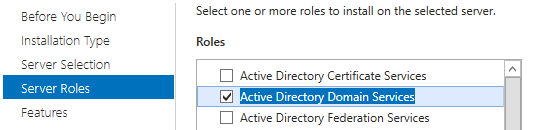
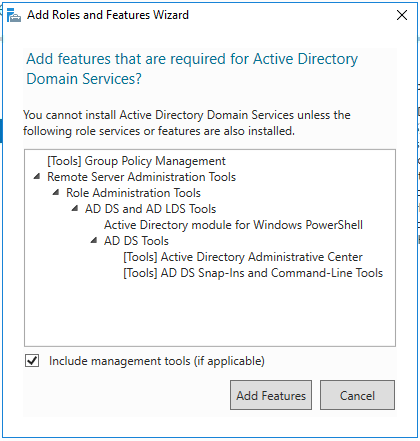
* If **the server** isn’t running, start it.
* Log on to the server as Administrator.
* Before making this computer a DC, you should CHANGE the IP setting of the Preferred DNS server to the ACTUAL IP address of your server computer. You should then remove the values for the Alternate DNS server so that there is only the Preferred DNS server. This will prevent your server from trying to set up its DNS zone file on an outside DNS server.  
  For Example:



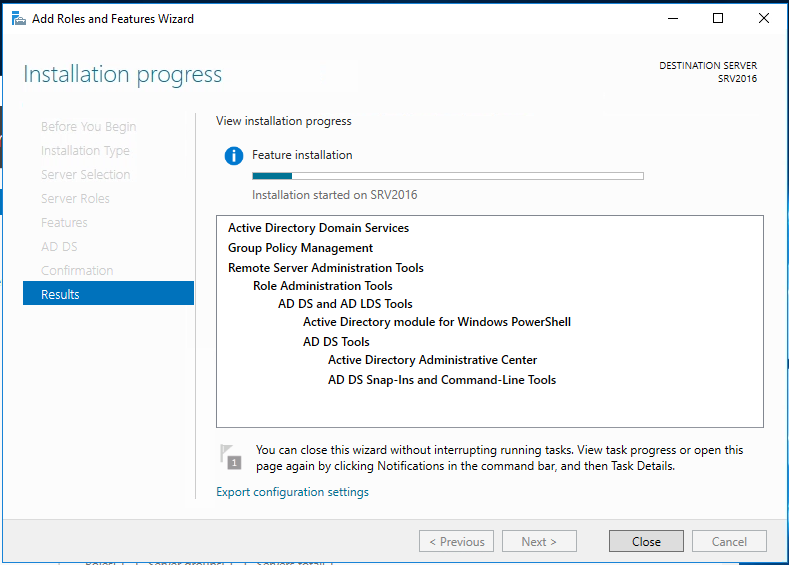
* Open Serve Manager if it isn’t already open, click on the Manage menu title in the top right and select Add Roles and Features.



* Click Next through the Wizard until you get to the Select server roles page, then check the box for Active Directory Domain Services (often just abbreviated to AD DS). When you do this you will get the option to also add related services. You want to do this, so click on Add Features when prompted.

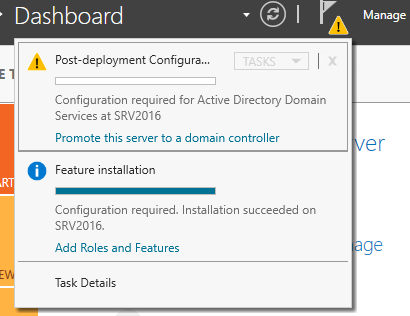


* Click **Next** to accept the defaults **until** you get to the Confirmation where you should click on **Install**.
* The results windows will show you a progress bar near the top.



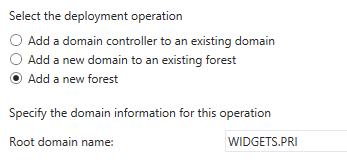
The process should only take a few minutes. When it is complete you should get the message that configuration is required, and that Installation succeeded. When you get this message, click Close.

* Near the top of Server Manager you should now see a yellow triangle. When you click on it you will see the option to Promote this server to a domain controller. Click on the link provided.

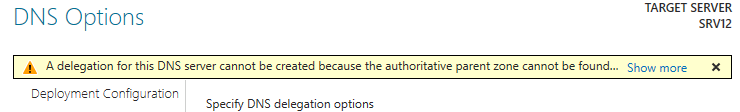


* You will next get the AD DS Configuration Wizard. Examine the radio button options.
* Select **(\*) Add a new forest**. You must do this since you don’t have a forest yet. This DC will be the first DC in a new forest.
* After doing this you will have to input the name of the Root domain. This is also the name of the forest. You must choose this name with care because changing it in the future can cause considerable administrative work.

**Name you used**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* The next screen offers the option to change to functional levels which you should leave Default
* Input a DSRM password. This can be anything and should be **secure**.
* On the DNS Options screen you will get a warning about delegation. This is normal and should be ignored. The warning just means that there is no zone file for your domain name yet. Click Next to proceed past the warning.



* On the next page, wait for & accept the supplied default NetBIOS name for the domain.
* **Continue through the wizard accepting all the defaults** until you get to the Prerequisites Check. You will see two warnings, but when you scroll to the bottom of the warnings you should see the message that Prerequisites Check was completed. **Click Install.**

The process will again display the warnings about cryptography algorithms and delegation. These are normal and expected. You can ignore them because you will have no Windows NT machines in your network and you will be using your own server for DNS. The system will automatically reboot during the installation process.

* If everything went well, the server would reboot. If it takes a long time (more than 5 minutes) this may indicate a problem with the DNS configuration.
* When you get the **logon screen** you will see that you are being asked to log onto the domain. You will see the NetBIOS name for the domain followed by a slash and the name of the account. **Log in as the built in Administrator. *This is now the default Administrator for the domain, not a local account.*** The local Administrator account was converted to a domain account during the promotion process.

## Part 5: Domain User Accounts

In order **to access Active Directory network resources,** and computers that are members of an Active Directory domain, **users must authenticate** (prove their identity) **with a domain controller** that holds their account information. This means they must provide a username and the appropriate password for that username or they can’t access domain computers and their resources. The usernames must be the usernames associated with domain user accounts held in the domain controller’s Active Directory database. Local user accounts, even if they exist on domain joined computers, are not stored in Active Directory and therefore cannot be used to authenticate with a domain controller or access resources within the network.

Domain user accounts are created on domain controllers and are held within that domain. A user can log in at any computer in any domain in the forest, but the user account authentication information must be accepted and approved by a domain controller in the user’s home domain. This makes the domain the Authentication Boundary in Active Directory.

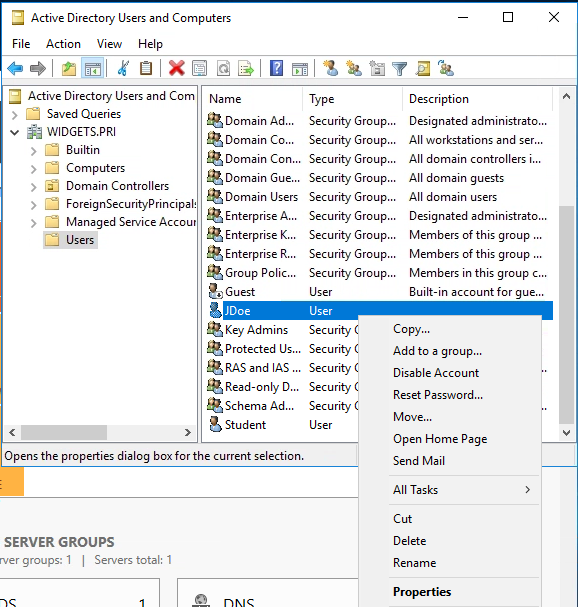
Domain user accounts are created by authorized administrative accounts and can be done manually or automated such as a PowerShell script. In this exercise you’ll use the manual method of account creation. While a username can be anything, it is common practice to have a naming policy convention in place. One very common naming policy is for a username to be a concatenation of the user’s first initial and last name. This is by no means required, nor is it the only useful naming convention, but is the one that will be used throughout these labs.

In the next steps you will examine the domain accounts that were converted from local account during promotion to a domain controller.

* If not already logon to **the server** with the **Administrator** account. When Server Manager starts, click on the Tools menu at the top and select Computer Management. Look for Local Users and Computers to verify that the SAM database has been disabled and that the Active Directory database must be used for user accounts.
* Close Computer Management.
* Click on the Tools menu again and select Active Directory Users and Computers (ADUC)
* Expand the name of your domain in the left pane, then left click once on Users.

In the right pane you should be able to find your JDoe account and the Student accounts that you created as local users. These accounts were converted to domain accounts in the promotion process.

* Right click on the **jdoe** account and select Properties (or double click on it).



* In **jdoe Properties**, click on the **Member of** tab and record what groups the account is a member of.

**Name Active Directory Domain Services Folder**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Now check the membership of the **client local** account and record what you see.

**Name Active Directory Domain Services Folder**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

In the next section you will create a new, personal administrative account that you will use for most of the work in the rest of this and the following guides.

* Still in **Active Directory Users and Computers (ADUC)** right click on the **Users icon** in the left panel and select **New** and then **User** from the cascading menus.
* Put in your first and last name and give yourself a logon name. It is suggested that you use your first initial and last name for the logon name, but you don’t have to.

Graphical user interface, text, application, email

Description automatically generated

* You should record the password below for reference in case you forget it later. Be sure to UNCHECK ‘[ ] User much change password at next login’ and also CHECK ‘ [X] Password never expires’.

**Username:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Password**:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* After the account has been created, locate it in the right pane in ADUC and double click on it.
* Click on the Member of tab and add **Domain Admins** to the membership. This will give you complete administrative control of the domain. When you have finished with this you should see that your new account is a member of two groups. Fill in the lines below.

**Name Active Directory Domain Services Folder**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Log off as Administrator and log on with your new personal administrative account.

Unless specified otherwise, you should always log onto your server with your personal domain admin account.

In the next steps you will set your new Domain Controller to allow other computers on the network to see it and access it.

* On **your server** in Server Manager use the Tools menu to select Services.
* Locate **Function Discovery Resource Publication**, double click on it and set it to **Automatic** startup type and then **Start** it. (There are two different Function Discovery services, be sure you have selected the correct one.)
* Repeat this process of setting Automatic startup and starting the SSDP Discovery service and the UPnP Device Host service.

Next you will verify that you can browse your network and see both of your computers.

* On your client, open File Explorer there and verify you can see both your server and the client PC under Network. *Do not continue until you can browse to both machines.*

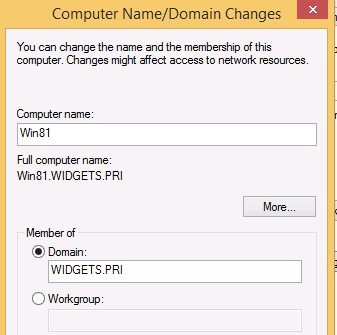
In the next steps you will join the WIN10 computer to the domain

* On **the client** open the IP properties for the network adapter as you did when you set the static IP address.
* Change the Preferred DNS server address to the IP address of **the server**.
* Delete any Alternate DNS server entry.
* Close all the open windows.
* Open File Explorer, right click on This PC in the left pane and select Properties

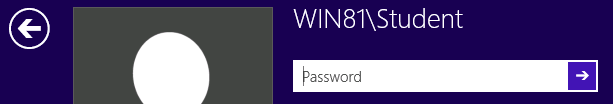
Graphical user interface, application

Description automatically generated

* In the System windows, click on Advanced system settings in the left pane.
* Click on the Computer Name tab, then click on the Change button
* In the Computer Name/Domain Changes windows, select the More button
* Put your domain name in the box for Primary DNS suffix for this computer. You are doing this so that when you try to join this computer to the domain, it will try to register with the correct DNS zone..
* Click OK and close the windows. You may be required to reboot **your client** after changing the DNS suffix.
* If, after rebooting, log back onto **your client** as your original local account.
* Return to the Computer Name windows (This PC / Properties / Advanced System Settings / Computer Name / Change).
* Click the radio button for Domain under Member of and put in your domain name, then click OK



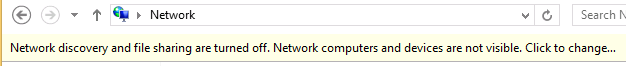
* You will then be asked for domain credentials that have the rights to add a computer to the domain. If you correctly added your personal account to the SRV16 Domain Admins group, you can use those credentials. A few seconds after entering the credentials you should get a screen welcoming you to the domain. After you click OK you will have to reboot again.
* After restarting, the system will offer to allow you to log into the client with a local account. If you do this you will not be able to access the domain properly. You can tell it is offering a local logon by the NetBIOS name of your computer rather than the domain at the logon screen.



* Click on the arrow, select Other User and then log on with your personal domain admin account. Notice that just below the password box you will see a Sign in to field.

Once you have logged into **the client** with domain credentials you will see that the very first logon takes longer because Windows 10 realizes this account hasn’t logged into this computer before.

* Go to the Desktop and open File Explorer (folder icon on the Taskbar).
* If you get the message about Network Discovery, Click to change



* After you have **turned on Network Discovery**, go to the Network icon and click on the **the server.**
* Open the **<ServerName>-Share** folder, open the TestData file, add the date and save the document.

Creating User Accounts

* Now on the Server, create domain user accounts (using Active Directory Users and Computers on the server) for each of these employees of your organization and use a consistent naming convention of first initial and last name; ex: **FLastName**. You will use these accounts in later labs. For simplicity, give them all the same password, requiring them to create a new one that meets complexity on their first login.

Here is an example list. This can be entered into a spreadsheet for use as a CSV file in powershell to expedite the process.

Full Name Username Description

Florence Horvath **FHorvath**  HR Manager

Cotton Malone **CMalone**  HR Staff

John Rebus **JRebus**  HR Staff

Gabriel Allon **GAllon**  Accounting Department Manager

Jeffrey Archer **JArcher**  Accounting Department Staff

Jesse Stone **JStone**  Accounting Department Staff

Steve Berry **SBerry**  Marketing Department Manager

David Baldacci **DBaldacci**  Marketing Department Staff

Jack Reacher **JReacher**  Marketing Department Staff

Jeffrey Deaver **JDeaver**  MIS Senior Administrator

Linda Fairstein **LFairstein**  MIS Administrator

Virgil Flowers **VFlowers**  MIS Help Desk Staff

Emma Peale **EPeale**  MIS Help Desk Staff

Robert Parker **Rparker**  Senior Editor

Claudia Plum **CPlum**  Editorial Staff

Ian Rankin **IRankin**  Editorial Staff Intern

Cassiopeia Vit **CVit**  Editorial Staff Intern

-END