Windows Server Intro – Setup and Configuration

Section 1 – Configuration, Promotion, and Users

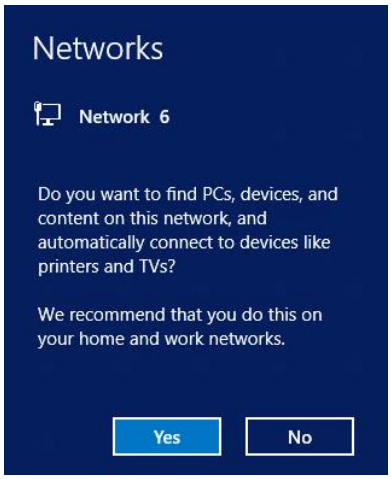
Machines:

- 1 Windows Server 2016
- 1 Windows 10 Client Machine

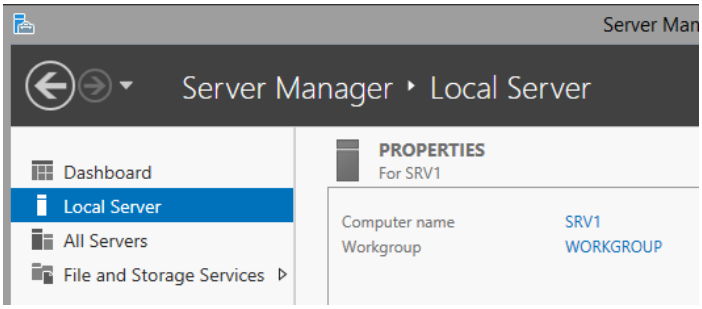
Part 1: Setup and Configure Your Server Image

****HARDWARE, OS INSTALL, INIT SETUP INFO HERE****

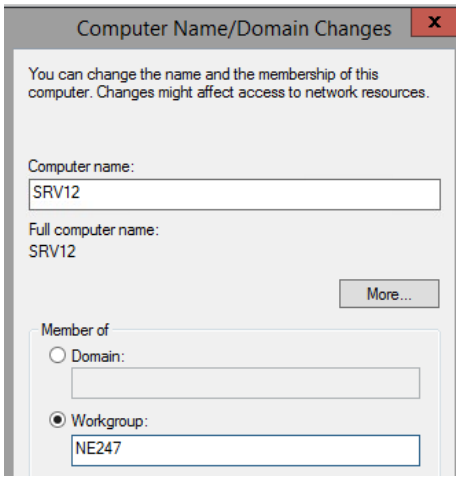
- If you get a box asking about connecting to the network, click Yes.



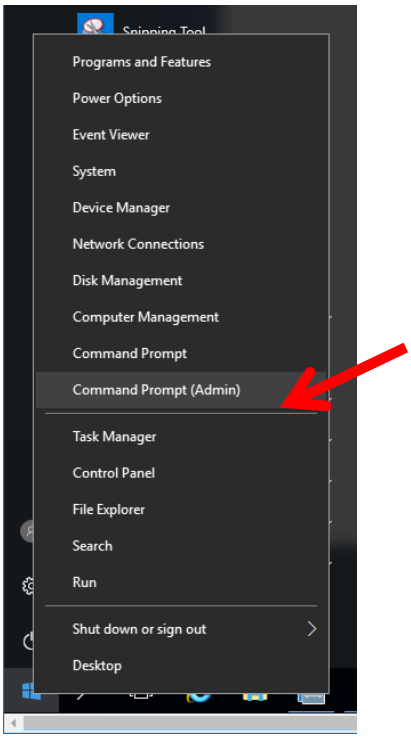
- **First**, do this. Server Manager > Tools > Computer Management > Local Users & Groups > Users > Administrator > **Uncheck 'User must change password at next login'** and set **Password never expires for the Administrator account**.
- Now go back to the Server Manager select **Local Server**, and then click on the current computer name to open the **System Properties** window.



- In Server Properties, click on **Change** to change the computer name. NOTE: The **Computer Description** box is NOT for the computer name. You have to click **Change** to get to the proper place to actually change the name of the computer. Set the computer name and the Workgroup name to YOUR DOMAIN. You will be required to restart the image after changing the name.



- After rebooting, log back on as Administrator and close Server Manager when it starts. (You can always reopen Server Manger later by using the icon next to the start button.)
- Right click on the **Start Menu** button and select **Command Prompt/Powershell.** Be sure to open as admin.



- In the Command Prompt, issue the **ipconfig /all** command and record what you see. You will need to refer to this later. (Note: The DNS entries you see won't be labeled Preferred and Alternate, but that is what they represent, so the table below shows those names.)

IPV4 Address: _____

Default Gateway: _____

Subnet Mask: _____

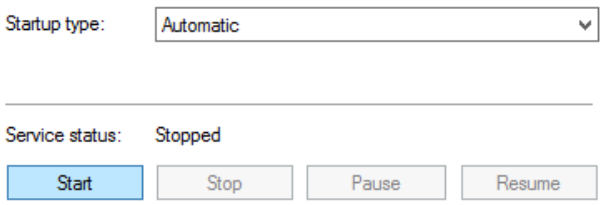
Preferred DNS _____

Alternate DNS _____

- You will need to set your server's IP information based on your organization's network.
- Right click on the clock in the lower right corner of the Task Bar, select Adjust Date/Time and then verify the Time Zone to your given time zone. During a standard installation, Windows sets the Time Zone to Pacific Standard time.

In the next section you will set or verify that certain services are set to run every time the server boots up. This is done to be sure that the server will be visible to other computers on the network when they browse the network.

- On SRV16 go to Start -> Server Manager -> **Tools** menu in Server Manager and select the Services option.
- In the list of services, scroll down to the **Function Discover Resource Publication** service and double click on it. (*There are two different Function Discovery services; be sure to pick the correct one.*)
- Verify that the server is set to Automatic and click the Start button



- After the service starts, click OK.
- Locate the **SSDP Discovery** service, set it to start automatically and start it and click OK.
- Repeat the process for the **UPnP Device Host** service.
- Using Server Manager > Tools > Computer Management > Disk Management to review disk configuration.

Part 2: Prepare Windows 10 Client Image

HARDWARE, OS INSTALL, SETUP GOES HERE

Setup with a local account and password

- Computer Management > Disk Management to review disk configuration.

Open System settings by clicking on the **File Explorer** [Folder] icon on the Taskbar, then right clicking on **This PC** and select **Properties**.

Across from **Computer Name** click on **Change settings.**

Click the **Change Settings** button and set the workgroup name to the domain as you did on your server image. Also verify the computer name here.

After clicking on OK you will have to restart your client computer and log back in again.

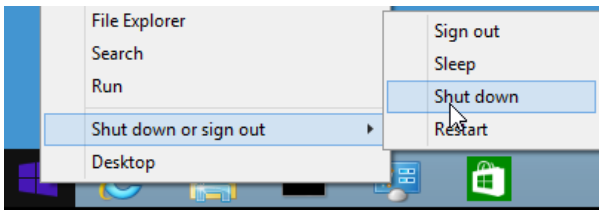
Open a command prompt and issue the IPCONFIG command, then record what you see. (You may want to pin the Command prompt to the taskbar as you did with the server.)

IPV4 Address: _____

Default Gateway: _____

Subnet Mask: _____

Shut the client computer down by first right clicking on the Start menu then selecting Shut down or sign out and choosing Shut down.



In the next part you will create and examine local user accounts as used on individual computers and computer workgroups (peer-to-peer networks). In the second part you will set the IP configuration.

Then, you will promote your server image from being a stand-alone server to be a domain controller for a new domain in a new forest. After promoting your DC, you will create and examine your domain user accounts.

Part 2: Local User Accounts

Local user accounts are available on all Windows computers except for those servers that are configured as Domain Controllers. Local user accounts can only be used on the local computer where they are created. No account that is not a local account can log onto the computer or access any resources on the computer. For example, to connect to a shared folder on a workgroup computer over the network, the incoming computer must provide the name and password of a local account on the target computer to gain access This is referred to as a decentralized administrative and security model because each computer maintains its own list of valid users and groups to control its own access and security.

To make workgroups function a little bit like a domain, a trick can be used by creating identical user accounts on each computer in the workgroup. This allows you to log onto one computer in a workgroup and access shared resources on another computer in the workgroup without manually authenticating with the remote computer. (The target computer sees that the incoming user account matches a local user account and allows access to what it believes is the local user account.) This technique, while effective, requires a considerable amount of administrative work and results in a network with poor internal security. **It is only appropriate for very small networks where security isn't a high priority.**

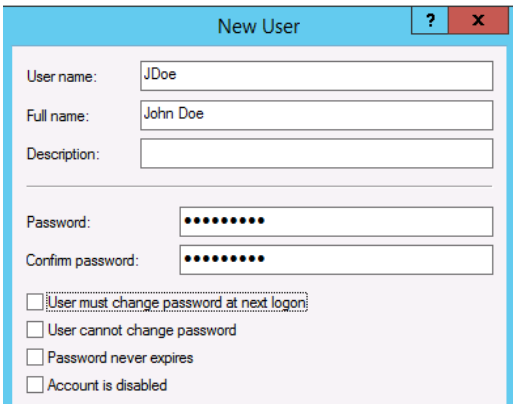
- If they aren't already running, start your **server** and **client** machines.
- Log on to **the server** as the built-in **Administrator** account and to **the client** as **a local user**.

In the following steps you will create a new local user account.

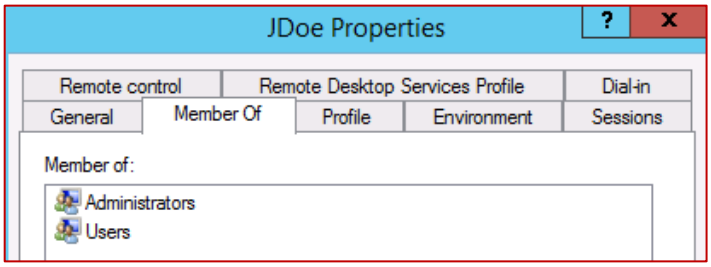
- On **your server** open **Server Manager** if is not already open.
- Tools > Services > Windows Update > Startup Type: Disabled > Stop service if running > OK.
- Back to Server Manager, click on Tools and select Computer Management.
- In the left pane of Computer Management, open Local Users and Groups and then click on **Users**.

Take note of the default accounts.

- Next, Right click on Users in the left pane and select New User.
- Create a user account for John Doe with a username of **jdoe** and password of **Password 1**.
- Uncheck the [ ]User must change password at next login option.
- Fill in the information as shown in the following screen shot.

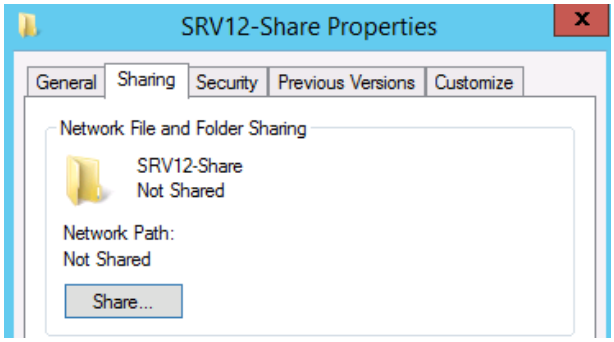


- After creating the account, right click on the account in the right pane of Computer Management and select Properties.
- Add the **jdoe** account to the **Administrators** group by clicking the **Member Of** tab, then click the **Add** button and type **Administrators** in the box provided. Be sure to use the plural form before clicking on **OK**.
- When completed you should see the following.

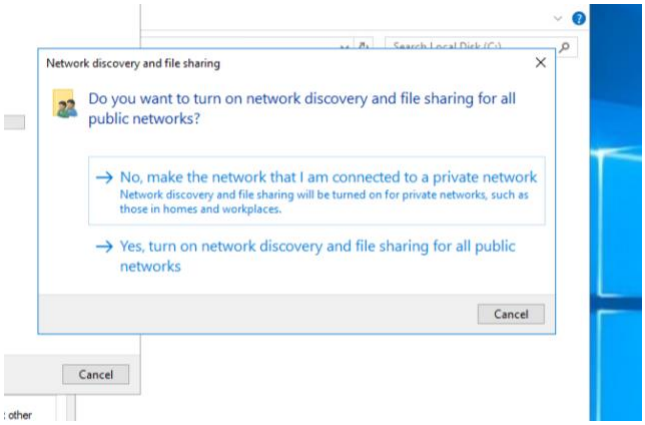


John Doe is now a local user with administrative rights and permissions. **Click OK** to save the jdoe settings.

- **Log off the server** and log back on with the **John Doe** (JDoe) account.
- Next you will create a Shared Folder for Workgroup Access
- On **SRV16**, close the Server Manager if it open and then open the File Explorer (the folder icon on the Task Bar.
- Navigate to 'This PC' and open the hard drive 'Local Disk C:' then right click on an open space in the right pane and select New then Folder to create a new folder on your C: drive.
- Call the folder <ServerName>-Share
- Open the new folder and create a new text document by first right clicking in the right pane then selecting New and Text Document.
- Call the new document **TestData.**
- Open the file and put your name in the file and save it.
- In the left pane, right click on **<ServerName>-Share** and select Properties from the menu.
- Click on the Sharing tab, then click on Share



- Click Share at the bottom of the window then click Done.
  If prompted to turn on network discovery, Choose 'Yes'



- Close the share properties window.

Next you will connect to the share on SRV16

- Switch to the **client** computer.
- Go to Search option and type **File Explorer**, right-click and pin to the taskbar
- Click on the Network icon in the left pane
- You should see at least your **server** computer and your **client** computers listed. If you do not see them after a minute or so, double check your configurations.
- Left click on the **server's** icon and you should get a Windows Security dialog box because your Student account is not recognized by **the server.**
- Fill in **jdoe** for the username and **Password1** for the password. DO NOT check the box to remember credentials.
- You should now see the **<ServerName>-Share** folder. Double click on it and then double click on the file to open it.
- Add the date to the file and save it.
- Close the **<ServerName>-Share** window to return to the desktop.
- Log off **the client computer** and log back on as **your original local account** (you are doing this to clear the access token for **your server**).
- Open the Network icon again and click on **your server**.

- You should get a login screen again
- Do NOT put in any credentials, just click Cancel
- Log off the client.
- Switch back to **the server**
- Create a new user account on **the server** with the same username as your original local client account with the same password. Be sure to UNCHECK the box for changing the password at next logon. *[Hint: use Computer Management as you did before.] It does not matter if you fill in a Full name or description.*
- Open File Explorer, open Local Disk, right click on **<ServerName>-Share** and select Properties.
- Click the Sharing tab, click on Share and the add **your local account** to the sharing list
- Click on Share at the bottom of the screen to complete the addition, then click Done and close.

Next you will test the new account you just created. Remember, although it has the same user name and password as the account on the client, it is a local account on the server.

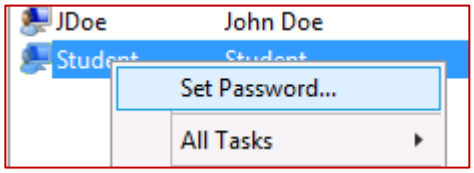
- Switch back to **the client**
- Log on as the original local account
- Go to the Desktop, open File Explorer and open the Network Browser and find **<ServerName>-Share**
- If the share does not appear, re-check your configurations
- Open the **<ServerName>-Share** folder and open the TestData file
- Add the date and try to save the changes.

Instead of saving the changes, you should get the Save As window because the Student account only has the Read permission to the file on **the server**.

- Click cancel and don't try to save the file changes.
- Log off the client.

In the next steps you will change the password for the Student account on SRV16 and see that the account is really different than the account on WIN10.

- Switch to **the server**
- Open Computer Management and locate the original local account in Local Users and Groups.
- Right click the account and select Set Password



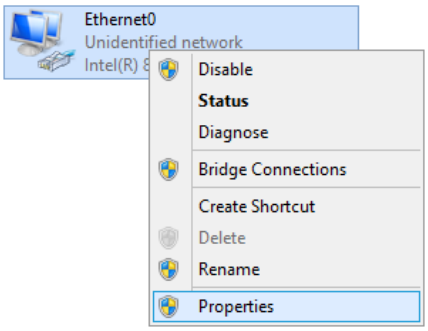
- Set the Password to **Swordfish1** (ignoring the warning message).
- Log off **the server** and log on as Student to make sure the password change worked as expected. (If logon failed, troubleshoot the problem before asking for assistance.)
- After you are sure the Student account works on **the server** with the new password, switch to **the client** and log on with the **original local account** (the password is still Password10).
- Switch to the Desktop, open File Explorer and open Network. Click the server's icon.
- It should now be obvious that the two Student accounts are different account controlled by different computers.

- Close all the open windows and **Logout of both machines.**

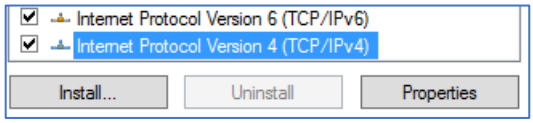
Part 3: Set or Verify the Static IP Addresses

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**.

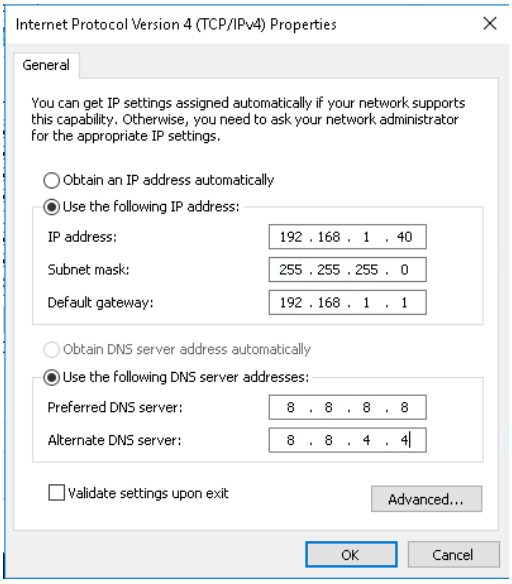


- Select (left click on) **Internet Protocol Version 4** and then click on **Properties**



- 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

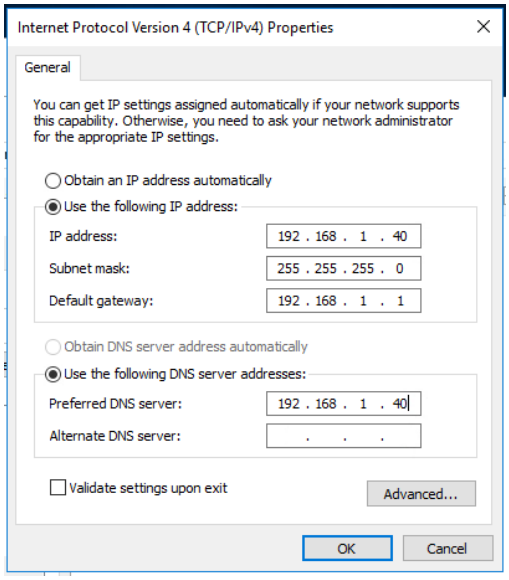
Domain Controllers allow for a central database of user and computer account information that greatly simplifies administration and security for all but the smallest networks. Domain controllers in the same domain maintain identical copies of the data base (through a process called replication) so that 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.

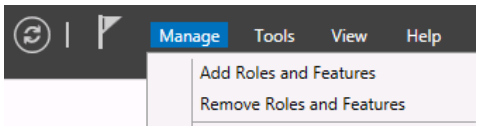
A Domain Controller can only hold data for a single domain. In other words, a Windows server can only be a DC for one Active Directory domain. To create a second domain, you need another domain controller. Domains within a Forest are connected with logical Trusts that allow users in one domain to be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

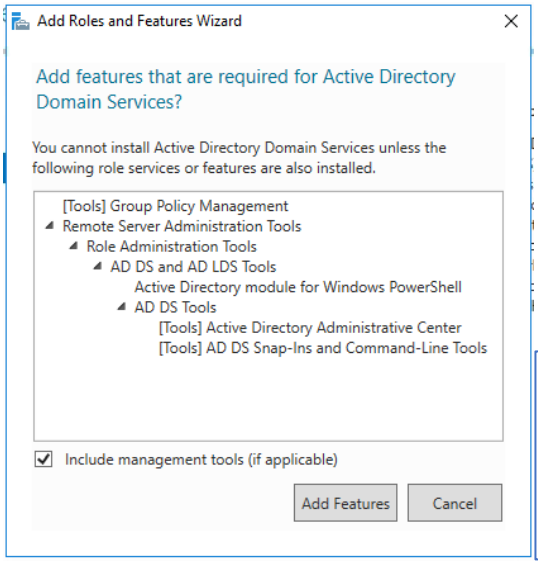
- If **the server** isn't running, start it.
- Log on to the server as Administrator.
- Before making this computer a DC, you should CHANGE the IP setting of the Preferred DNS server to the ACTUAL IP address of your server computer. You should then remove the values for the Alternate DNS server so that 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:

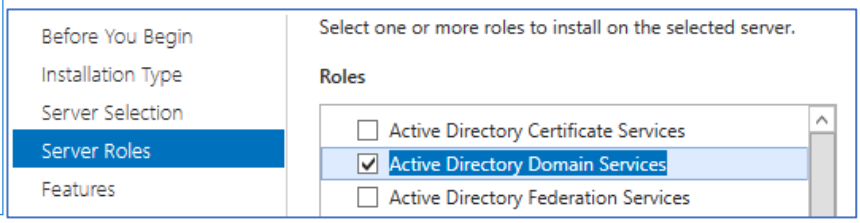


- Open Serve Manager if it isn't already open, click on the Manage menu title in the top right and select Add Roles and Features.

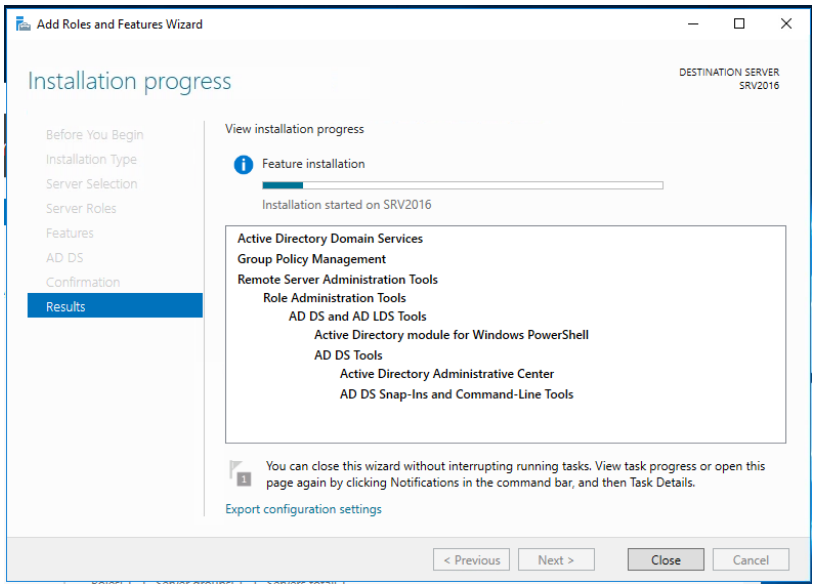


- Click Next through the Wizard until you get to the Select server roles page, then check the box for Active Directory Domain Services (often just abbreviated to AD DS). When you do this you will get the option to also add related services. You want to do this, so click on Add Features when prompted.



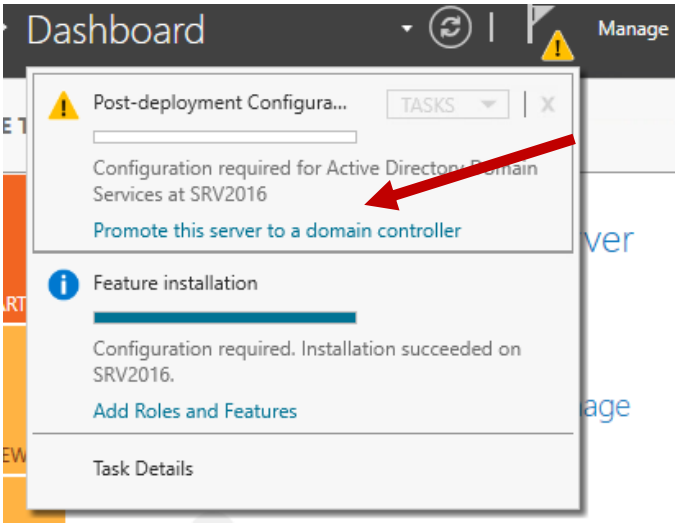


- Click **Next** to accept the defaults **until** you get to the Confirmation where you should click on **Install**.
- The results windows will show you a progress bar near the top.



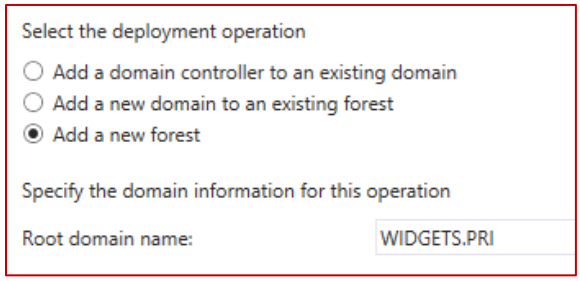
The process should only take a few minutes. When it is complete you should get the message that configuration is required, and that Installation succeeded. When you get this message, click Close.

- 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.

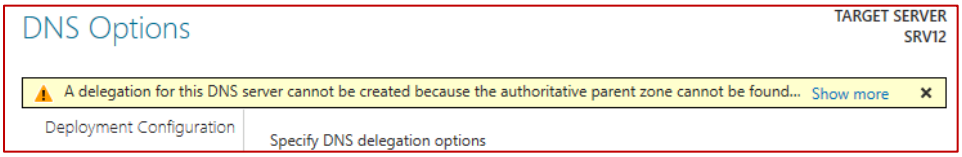


- You will next get the AD DS Configuration Wizard. Examine the radio button options.
- Select **(*) Add a new forest**. You must do this since you don't have a forest yet. This DC will be the first DC in a new forest.
- After doing this you will have to input the name of the Root domain. This is also 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.

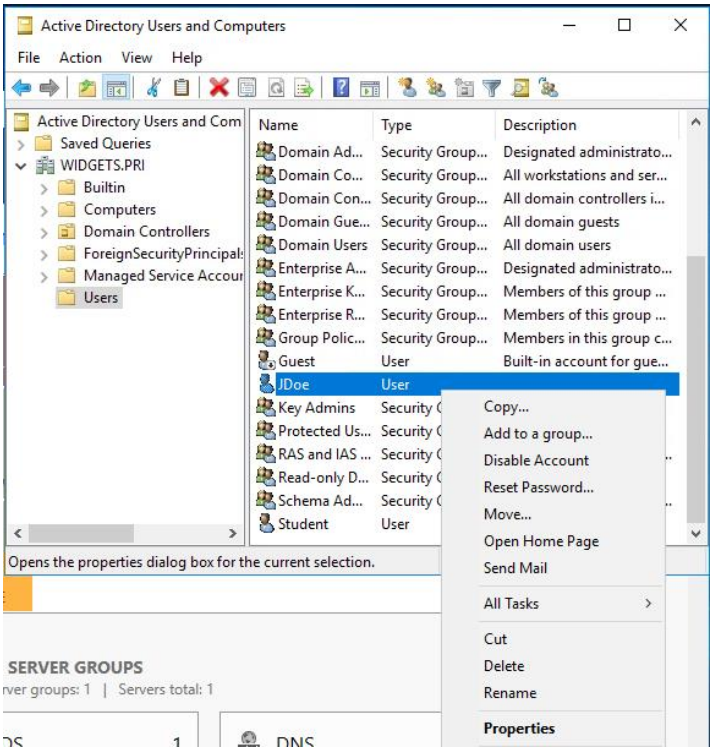
In the next steps you will examine the domain accounts that were converted from local account during promotion to a domain controller.

- 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.

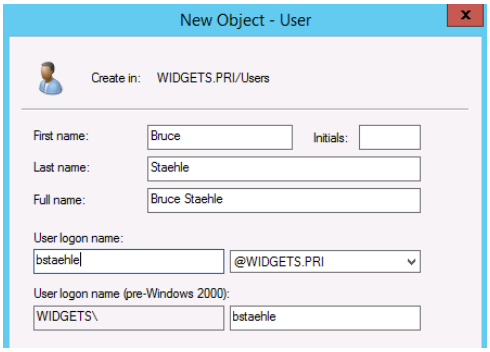
Name	**Active Directory Domain Services Folder**
_____	_____
_____	_____
_____	_____

- 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.



- 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.

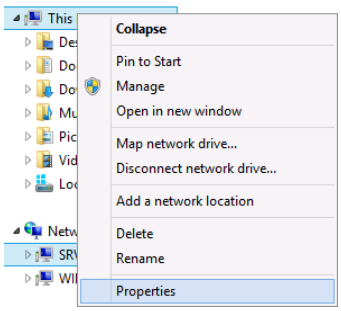
Next you will verify that you can browse your network and see both of your computers.

- 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.*

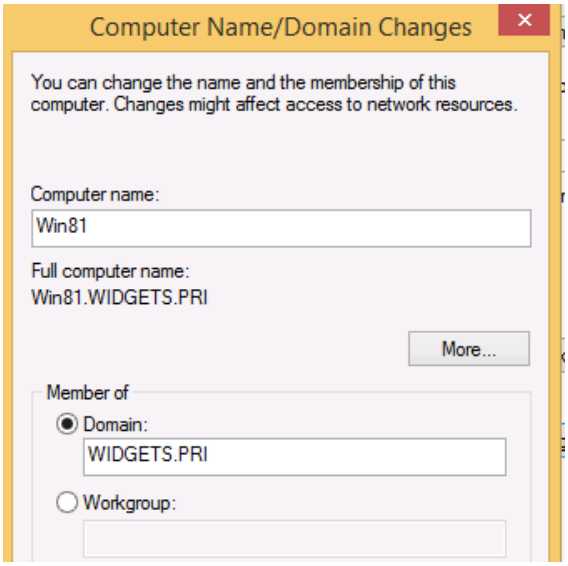
In the next steps you will join the WIN10 computer to the domain

- 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



- 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

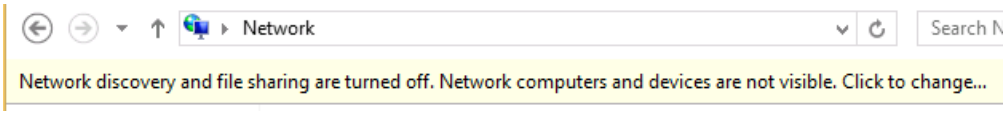
credentials. A few seconds after entering the credentials you should get a screen welcoming you to the domain. After you click OK you will have to reboot again.

- 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