**NE259 – Windows Server – Lab2**

**Points will be deducted if All Answers Are Not In:**

**Ariel, 14pt, Bold, Red!**

This lab consists of four distinct sections. In the first 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. In the third part, 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. And in the final section you will create and examine domain user accounts.

Required Materials:

Server 2016 VMware image configured as a stand-alone server

Windows 10 VMware image configured as a stand-alone workstation

**Part 1: 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 **SRV16** and **WIN10** images.
* Log on to **SRV16** as the built-in **Administrator** account and to **WIN10** as **Student**.

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

* On **SRV16** open Server Manager if is not already open.
* AT the top right, click on Tools and select Computer Management.
* In the left pane of Computer Management, open Local Users and Groups and then click on **Users**.

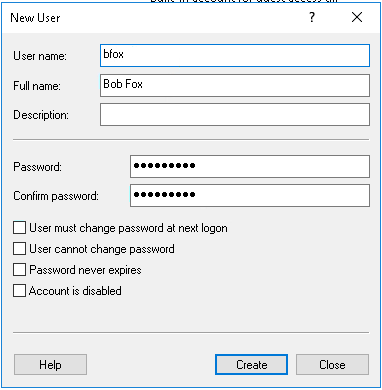
List the default accounts.

**Administrator**

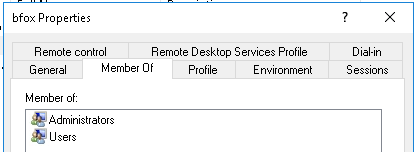
**DefaultAccount**

**Guest**

* First, set **Password never expires for the Administrator account**.
* Next, Right click on Users in the left pane and select New User.
* Create a user account for Bob fox with a username of **BFox** and password of **Password1**
* **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 **bfox** 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.



Bob Fox is now a local user with administrative rights and permissions. **Click OK** to save the bfox settings.

* **Log off SRV16** and log back on with the **Bob Fox** account.

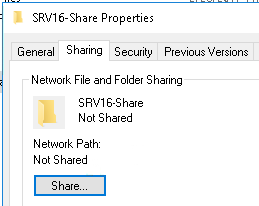
What display name does Windows show you? **Bob Fox**

**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 **SRV16-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 **SRV16-Share** and select Properties from the menu.
* Click on the Sharing tab, then click on Share



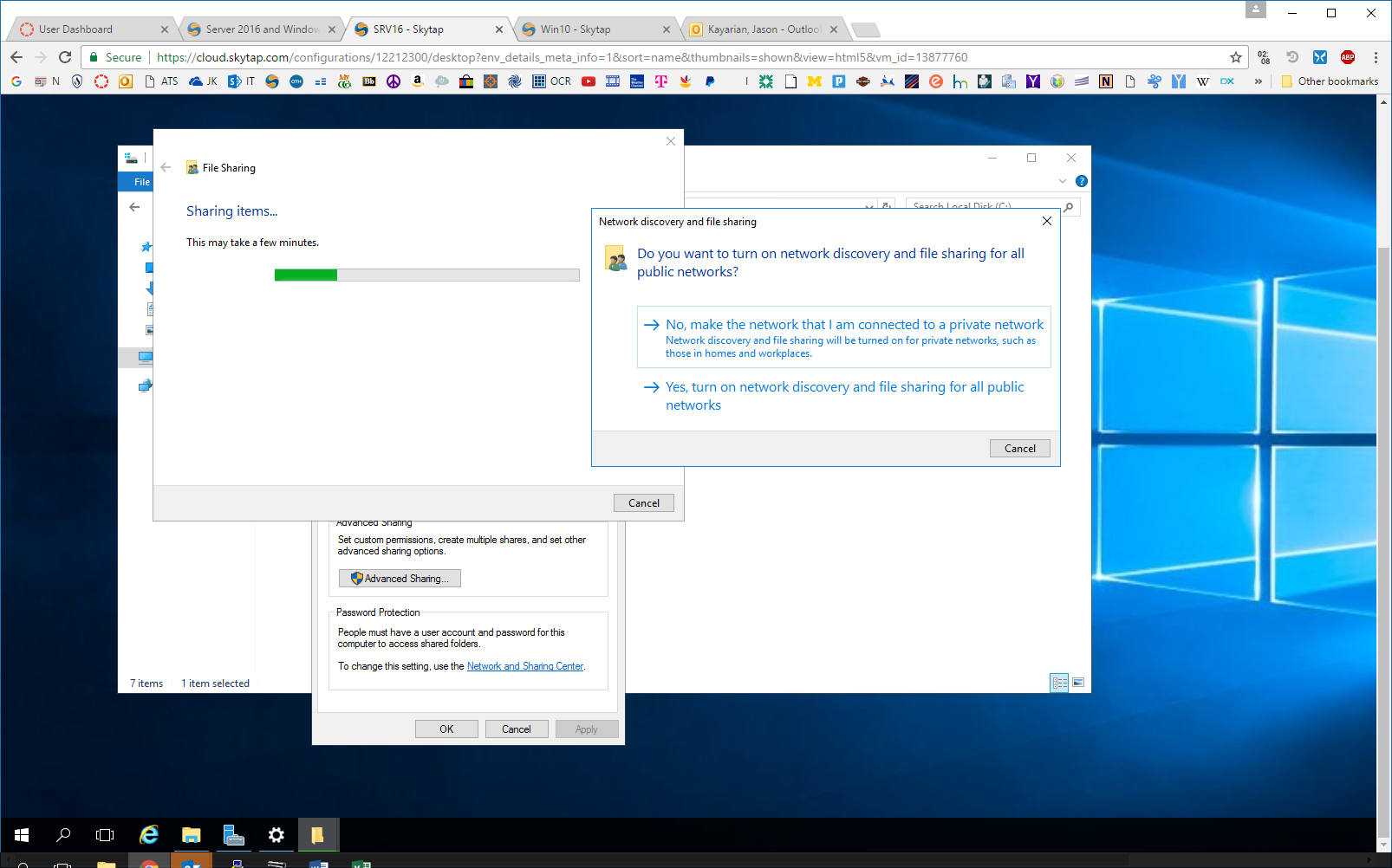
* List the accounts you see below and their permissions. (You probably won’t need all the spaced provided.)

Name Permission Level

**Bob Fox Owner**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* 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 **WIN10** 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 **SRV16** computer and your **WIN10** computers listed. If you do not see them after a minute or so, ask for assistance.
* Left click on the **SRV16** icon and you should get a Windows Security dialog box because your Student account is not recognized by **SRV16**
* Fill in **bfox** for the user name and **Password1** for the password. DO NOT check the box to remember credentials.
* You should now see the **SRV16**-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 **SRV16**-Share window to return to the desktop.
* Log off **WIN10** and log back on as **Student** (you are doing this to clear the access token for **SRV16**).
* Open the Network icon again and click on **SRV16**.
* Do you get the logon screen again?  **[Y / N]** (you should) **Y**
* Do NOT put in any credentials, just click Cancel
* Log off **WIN10**.
* Switch back to **SRV16**
* Create a new user account on **SRV16** with the username of **Student** with the password of **Password10**. 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 **SRV16-Share** and select Properties.
* Click the Sharing tab, click on Share and the add **Student** to the sharing list
* What permission does Student get by default? **Read**
* 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 WIN10, it is a local account on SRV16.**

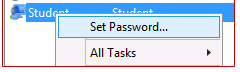
* Switch back to **WIN10**
* Log on as Student
* Go to the Desktop, open File Explorer and open the Network Browser and find **SRV16-Share**
* Does the share appear? **[Y / N]** (if it doesn’t, ask for help.) **Yes**
* Open the **SRV16**-Share folder and open the TestData file
* Add the date and try 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 **SRV16**. We will cover permissions later in the course, but this is instructive to witness.

* Click cancel and don’t try to save the file changes.
* Log off **WIN10**

**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 **SRV16**
* Open Computer Management and locate the Student 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 **SRV16** 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 **SRV16** with the new password, switch to **WIN10** and log on with the **WIN10** Student account (the password is still Password10).
* Switch to the Desktop, open File Explorer and open Network

What happens when you click on the **SRV16** icon?

**File explorer loads, and then says “Windows cannot access \\SRV16”**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

It should now be obvious that the two Student accounts are different account controlled by different computers.

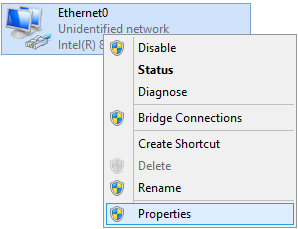
* Close all the open windows and **Logout of SRV16 & WIN10**

Continue on to Part 2 …..

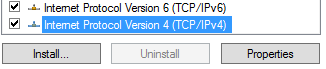
**Part 2: Set or Verify the Static IP Addresses**

A Domain Controller must have a static IP address, so you must check this before the actual promotion process. In this lab we will also check the static IP address for the **WIN10** workstation computer to be sure they will be on the same subnet and can easily communicate. Your images are located on a private network segment on Skytap and will already have static IP addresses set.

* Login to **SRV16** 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 or set the static IP address for **SRV16** as shown below

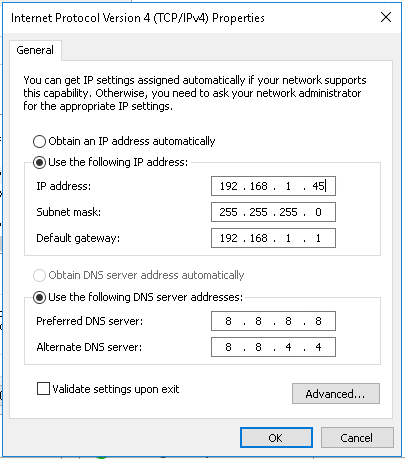
**IP address: 192.168.1.45**

Subnet mask: **255.255.255.0**

Default gateway: **192.168.1.1**

Preferred DNS Server: **8.8.8.8**

Alternate DNS Server : **8.8.4.4**



* 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 VMnet8 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 192.168.1.1 (You may need to turn off the firewall)**

* Was this this ping attempt successful?  **[Y / N] Y**
* Verify you can connect reach the public Internet by pinging one of the public DNS servers run by Google.

**PING 8.8.8.8**

* Was this this ping attempt successful?  **[Y / N] Y**

***DO NOT PROCEED UNTIL THE ABOVE PING ATTEMPS ARE SUCCESSFUL!!!***

* Now switch to the **WIN10** computer and go to Control Panel and turn off the Firewall. Configure the **WIN10** machine for a static IP address where the last octet is **55**. 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 **SRV16**.
* Run IPCONFIG /All on both **SRV16** and **WIN10** and record the values for future reference below.

**SRV16** **WIN10**

IP Address **192.168.1.45 192.168.1.55**

Default Gateway: **192.168.1.1 192.168.1.1**

Subnet Mask: **255.255.255.0 255.255.255.0**

Preferred DNS **192.168.1.1 192.168.1.1**

Alternate DNS **8.8.8.8 8.8.8.8**

* Use the PING command to verify that you can connect to the **WIN10** IP address from the **SRV16** computer.
* Use the PING command to verify that you can connect to the **SRV16** IP address from the **WIN10** 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.

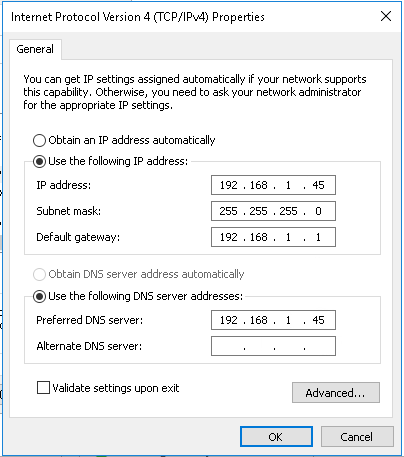
Part 3: Promote Stand-Alone Server to Domain Controller

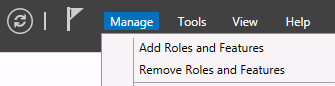
Domain Controllers allow for a central database of user and computer account information that greatly simplifies administration and security for all but the smallest networks. Domain controllers in the same domain maintain identical copies of the data base (through a process called replication) so that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

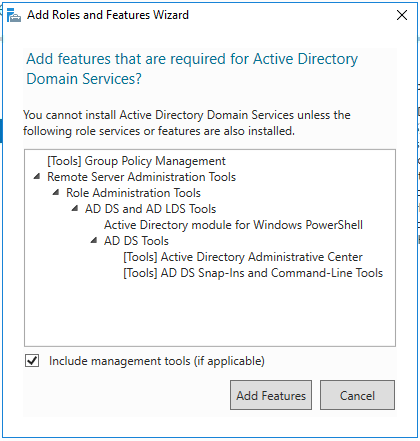
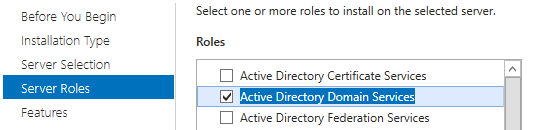
A Domain Controller can only hold data for a single domain. In other words, a Windows server can only be a DC for one Active Directory domain. To create a second domain, you need another domain controller. Domains within a Forest are connected with logical Trusts that allow users in one domain to be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

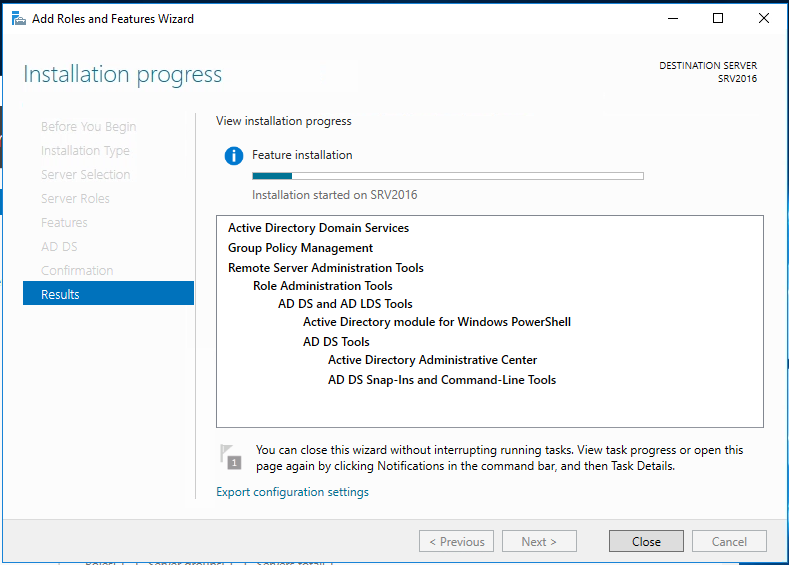
When you decide to promote a server to become a DC you have to make a decision about the DC. Will it be the first domain in a new forest, a new domain in an existing forest, or a new Domain Controller in an existing domain? If you don’t have an Active Directory forest yet, there is only one valid answer: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

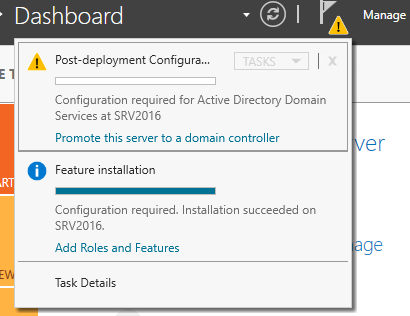
* If **SRV16** isn’t running, start it.
* Log on to **SRV16** as **Administrator**.
* **Before making this computer a DC, you should CHANGE the IP setting of the Preferred DNS server to the ACTUAL IP address of your SRV16 computer.** You should **then remove the values for the Alternate DNS server so 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.

What is the default option? **Add a domain controller to an existing configuration**

* 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. For this lab use the name **AVERY.PRI**

Name you used: **AVERY.PRI**

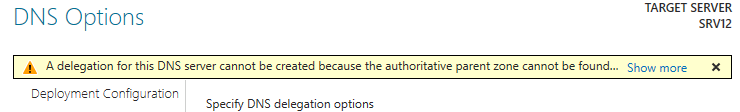
* The next screen offers the option to change to functional levels which you should leave Default

What check boxes are checked for domain controller capabilities?

**Domain Name System (DNS) Server**

**Global Catalog**

* Input a DSRM password. This can be anything, but for simplicity in a lab environment, use **Password1**
* 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.

What is the NetBIOS name? **AVERY**

* **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 will 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 with Password16**. ***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 4: Domain User Accounts

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.

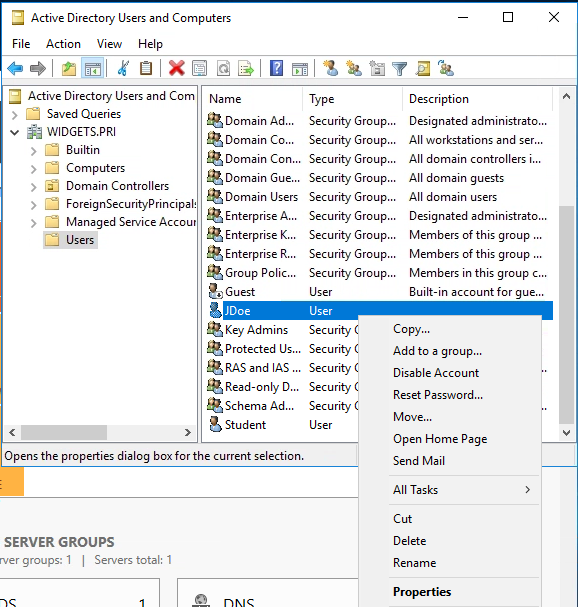
Domain user accounts are created by authorized administrative accounts and can be done manually or automated such as a PowerShell script. In this exercise, you’ll use the manual method of account creation. While a username can be anything, it is common practice to have a naming policy convention in place. 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 **SRV16** with the **Administrator** account and **Password16**. When Server Manager starts, click on the Tools menu at the top and select Computer Management. Look for Local Users and Computers.  
  Do you see it? [Y / N ] **N**
* This shows 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 Bfox 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 **bfox** account and select Properties (or double click on it).



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

Name Active Directory Domain Services Folder

**Administrators, Domain Users, Users**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

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

Name Active Directory Domain Services Folder

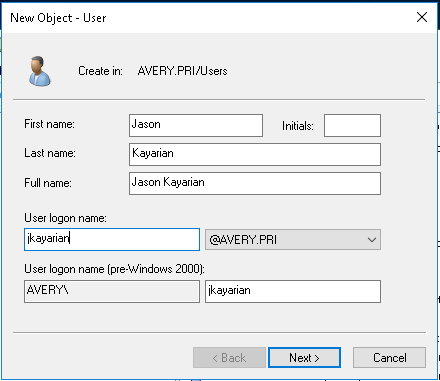
**Domain Users, Users**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

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

* 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.
* For this personal account use **Password247**. 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’.**

User Name: **WBain**

Password: **Password247**

* 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

**Domain Users, Domain Admins**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

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

***Unless specified otherwise, you should always log onto SRV16 with your personal domain admin account.***

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

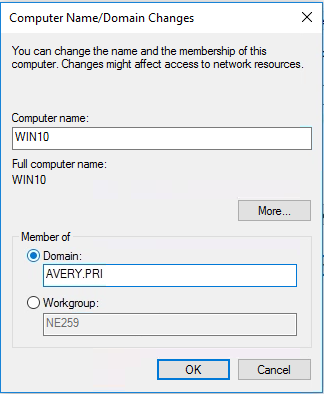
* On **SRV16** in Server Manager use the Tools menu to select Services.
* Locate **Function Discovery Resource Publication**, double click on it and set it to **Automatic** startup type and then **Start** it. (There are two different Function Discovery services, be sure you have selected the correct 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 **WIN10**, open File Explorer there and verify you can see both **SRV16** and **WIN10** 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 **WIN10** 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 SRV16. \*\*\*\***
* 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 (AVERY.PRI) 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 **WIN10** after changing the DNS suffix.
* If, after rebooting, log back onto **WIN10** as Student.
* 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 **WIN10** 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.

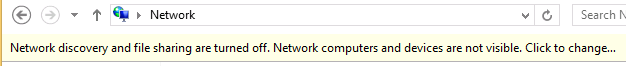


* **Click on the arrow, select Other User and then log on with your personal domain admin account.** Notice that just below the password box you will see a Sign in to field.

What are you signing into? **Personal domain account of AVERY.PRI**

Once you have logged into **WIN10** 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 **SRV16**.
* Open the **SRV16**-Share folder, open the TestData file, add the date and save the document.

Was this all successful? **[Y / N ] Y**

**Next you will create a series of user accounts for use in later labs.**

* Now on the **SRV16** Server, create domain user accounts (using Active Directory Users and Computers on the server) for each of these employees of Widgets 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 **Password1** and set the accounts so that the users don’t have to change their passwords at next logon and so they don’t expire. (You would not do this on a real network, but it simplifies laboratory exercises.)

Full Name Username Description

Woodrow Webb  **WWebb**  HR Manager

Julio Watkins **JWatkins**  HR Staff

Ivan Grant **IGrant**  HR Staff

Alyssa Cox  **ACox**  Accounting Department Manager

Lewis Pearson  **LPearson**  Accounting Department Staff

Raymond Sullivan  **RSullivan**  Accounting Department Staff

Melody Beck  **MBeck**  Marketing Department Manager

Cassandra Moran  **CMoran**  Marketing Department Staff

Lavern Keller  **LKeller**  Marketing Department Staff

Misty Burns  **MBurns**  MIS Senior Administrator

Tracy Oliver **TOliver**  MIS Administrator

Sean Santiago **SSantiago**  MIS Help Desk Staff

Pat Berry  **PBerry**  MIS Help Desk Staff

Jasmine Adams  **JAdams**  Senior Editor

Sheryl Hale  **SHale**  Editorial Staff

Edward Ortiz  **EOrtiz**  Editorial Staff Intern

Nick Perkins  **NPerkins**  Editorial Staff Intern

* Often installing Active Directory reverts the DNS of the server to the localhost 127.0.0.1 address. Re-check to ensure that SRV16 dns settings are set for its own ip address and not localhost.
* Shut down both images using the proper shut down procedure”

-END