Security Lab

Lab 3: Enterprise Active Directory Configuration

Systems Security Management

Document Sections

Lab Purpose – General discussion of the purpose of the lab

Lab Goal – What completing this lab should impart to you

Lab Instructions – Instructions for carrying out the lab

Lab Deliverables – What you have to submit to your instructor

Lab Rubric – How this assignment will be graded

Lab Resources – Any useful resources for completing the lab deliverables

Lab Purpose

Microsoft's Active Directory (AD) platform is used as a security and authentication mechanism at businesses across the globe. Microsoft's AD uses various objects to define specific items within the directory database. These objects include User Objects (Accounts), Organizational Units (Folders), and Security Groups, among others. It will be these three objects you will learn more about and use to help Fortune Automotive develop their AD.

The purpose of this lab is to familiarize you with various aspects of a common enterprise authentication and authorization tool and aspects of account-based security. This lab has four (4) parts:

1. Active Directory Design
2. User and Group Creation
3. Assigning Group- or Organizational Unit-based Security
4. Systems Documentation

Active Directory Design

Designing an AD may seem like a simple matter: just create organizational units here, name them appropriately, and place user accounts within the folders. However, the truth is it can be a simple matter, but some thought must be put into how the AD should be designed. Some companies leave their AD as it is installed by default (e.g. user accounts are kept in the Users folder, etc.), while others will create a structure using organizational units to mimic department hierarchy. Ultimately, this decision is up to you and one you should consider as you assist Fortune Automotive in this endeavor. This is a critical thinking exercise. Use the information provided for the Fortune Automotive Corporation and consider your options for how to organize the company within the AD environment. You can use a hierarchy structure, a flat structure, or even a highly customized structure. The important thing to consider is the AD design you use will dictate how you apply group policies within the environment. In your next lab, you will be working with group policies and will their effect on an AD in action.

User and Group Creation

The primary purpose of Microsoft's Active Directory platform is to provide authentication services to those who need to access corporate resources. As you might expect, user account objects within AD play an important part in this service. User account objects can be assigned to resources (such as printers or network drives) and they are used to login to workstations and servers connected to the AD domain.

Groups come into the mix when you need to authorize more than one person to access shared resources. Instead of assigning specific people access to a resource, you can assign a group. Members of a security group can be changed at any time, granting or denying access to shared resources without the need to specifically modify the security permissions of the resource itself. Groups are a vital option to help the systems administrator manage shared resources more efficiently.

Assigning Group- or Organizational Unit-based Security

What happens when you want to apply specific security permissions or access rights to groups of people? Security groups are a good way to assign permissions or access rights to shared resources; however, in some cases a single group might not cover all of the people who need access. Of course, you can create a new group to do this, or assign multiple groups as necessary; however, you can also assign permissions or rights to Organizational Units (OUs) as well.

By assigning security permissions at the OU level, you can set certain rights to those objects contained within the OU. For example, if you want everyone in the Accounting OU to have access to specific network drives that other departments do not need, you can create a login script assigned directly to the Accounting OU. Then anyone whose user account object resides in the Accounting OU will automatically have that script run on their next login.

The decision to how a system administrator should assign security permissions and access rights within AD *will* affect how the AD is designed. It is important to keep in mind these options for security within AD are not an either/or scenario. Both options can and are used by companies to secure shared resources.

Systems Documentation

What happens in the event of a critical failure of a system? What happens if you were to discover the backup or disaster recovery solution the company has in-place is not working as expected, or just simply is not viable? Companies should (and most do) have a disaster recovery or business continuity plan ready should a critical failure occur; however, not everyone observes best practices when it comes to Information Technology. So, what do you do when you have a failed system with no backup available to restore services from?

In most cases, the systems administrator will need to re-install the server software and manually re-create the services. This is one reason why accurate and up-to-date systems documentation is a vital tool in the systems administrator’s arsenal. The simple fact of the matter is that no one should expect (or be expected) to remember every minute detail of a server configuration. This is where systems documentation comes into the picture; however, the documentation itself is only a good resource if it is kept up-to-date. Inaccurate information contained within systems documentation will lead to wasted time and effort on the part of the systems administrator and lead to extended system downtime as the server is recovered from the memory of anyone who has worked on it.

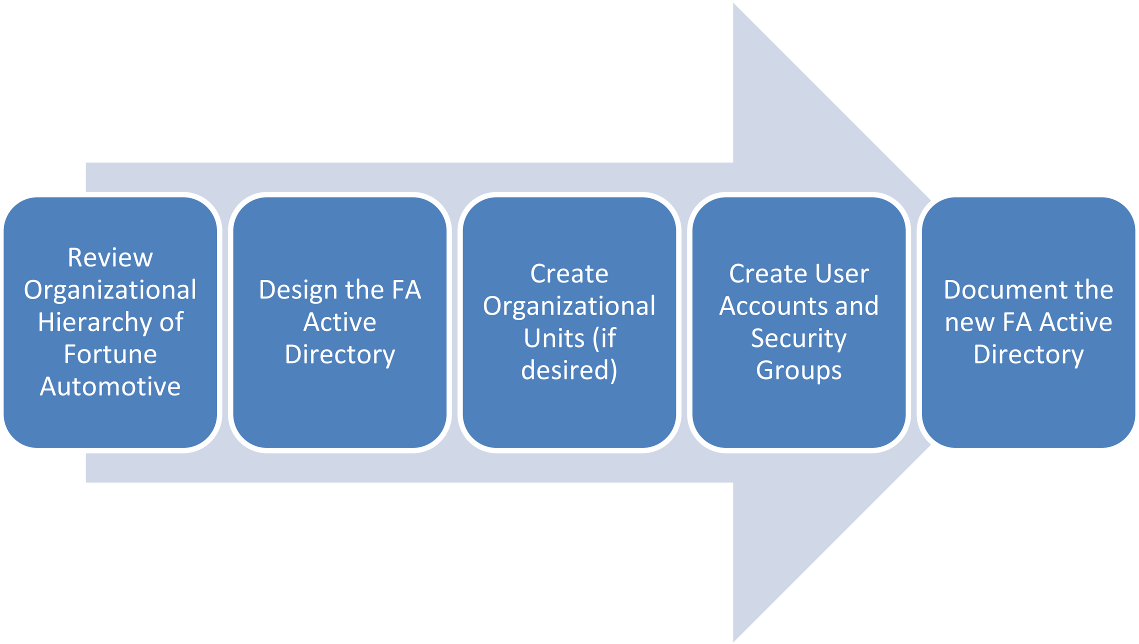
So, what is the bottom line? As a systems administrator, part of your responsibilities will involve keeping accurate up-to-date documentation on every system you maintain.

Lab Goal

Upon completion of this lab, you should have:

- Introduced you to Microsoft's Active Directory Services
- Increased your understanding of why designing logic and security into AD is important.
- Increased your understanding user, group, and OU security.
- Provide hands-on experience interacting with an enterprise-level authentication and security platform.
- Provide experience with systems documentation.

Lab Instructions


Review Organizational Hierarchy of Fortune Automotive
Design the FA Active Directory
Create Organizational Units (if desired)
Create User Accounts and Security Groups
Document the new FA Active Directory

1. Review Organizational Hierarchy of Fortune Automotive

1) Open a web browser to:
    a. http://d2l.arizona.edu
2) Log-in and access this course.
3) Attached to the Lab Assignment for Lab #3 you will find a .PDF file that contains the organizational chart for Fortune Automotive. This information will be necessary in order to complete the lab.

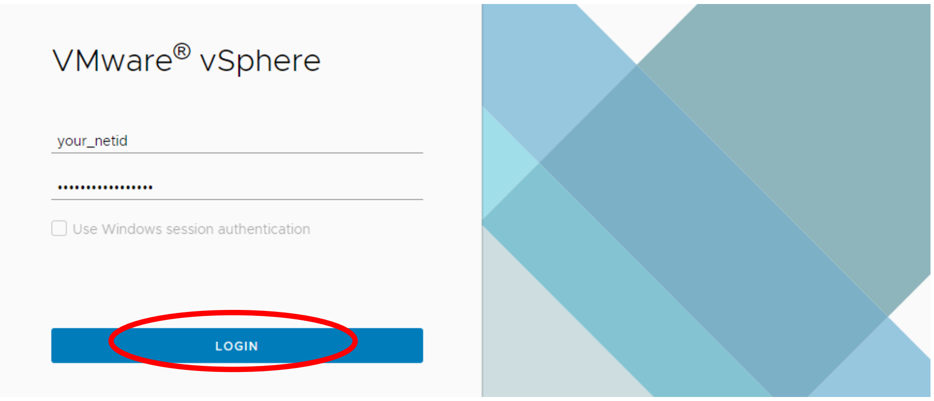
2. Design the FA Active Directory

1) Taking the information you have gleaned from the FA Organizational Hierarchy, create a design for your Active Directory. You may use any of the objects within AD to accomplish your design (including users, computers, groups, organizational units, etc.).

2) This is a critical thinking and creativity assignment. There are no right or wrong answers; however, there are better designs than others. Make use of Module 10 and research information on Google to help with your design.
3) Document the design using Microsoft Word and/or Excel or Visio. This will be one of the deliverables you submit for this lab. Keep in mind you will likely make changes to this documentation as you implement the design, so make changes as you go through the lab. What is contained within the provided document will be matched with how you modify the AD itself.

3. Create Organizational Units (if desired)

1) Connect to the UA VPN, then open a web browser to:
   a. https://plumvcsa.artg.arizona.edu/ui



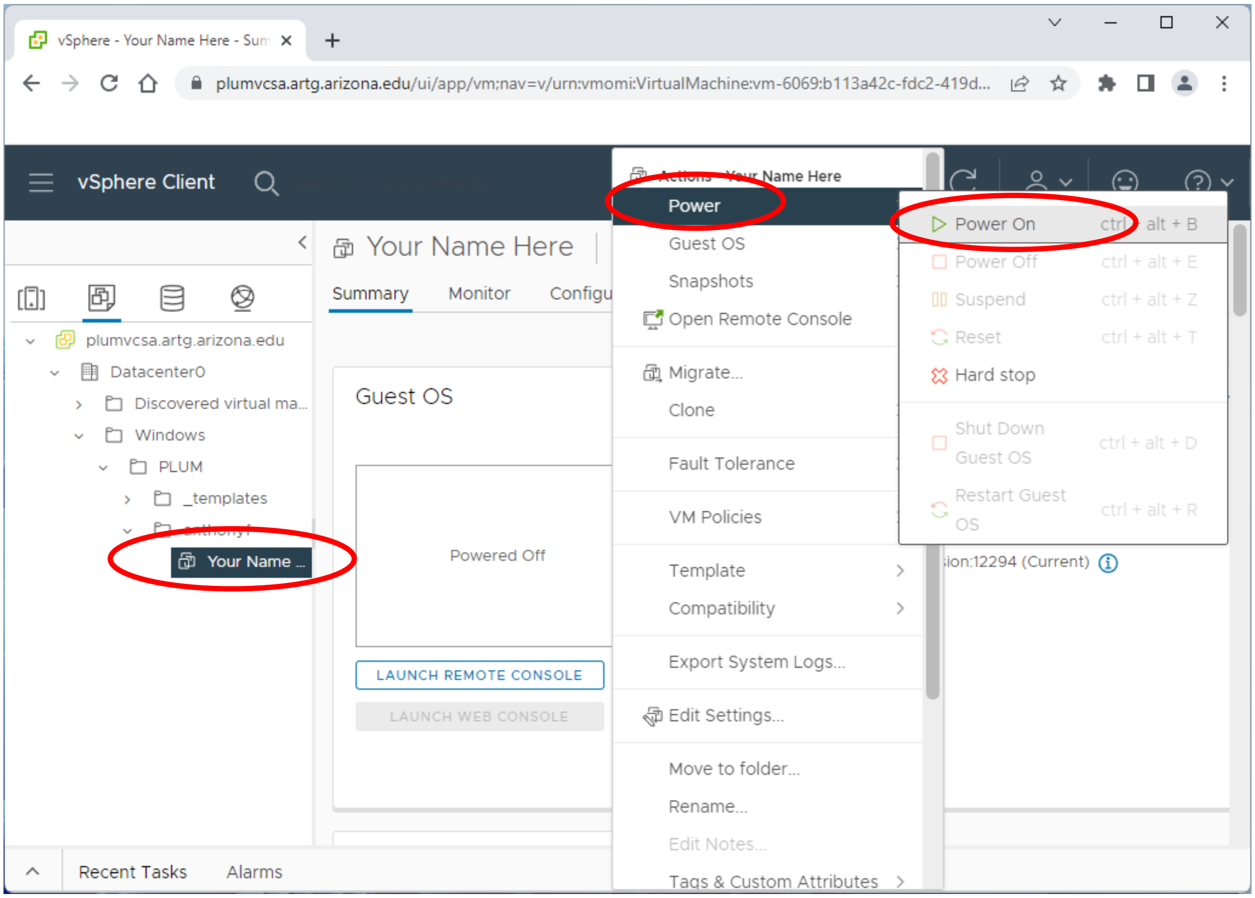
VMware® vSphere

your_netid

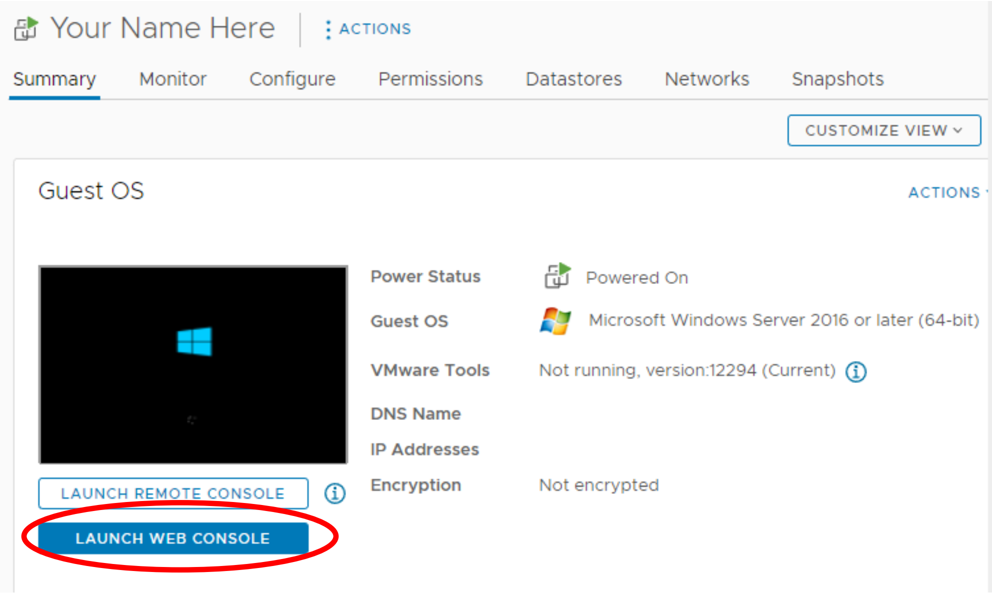
••••••••••••••••

□ Use Windows session authentication

2) On the login page, you will enter your NetID and password.
3) Click **Login** to continue.



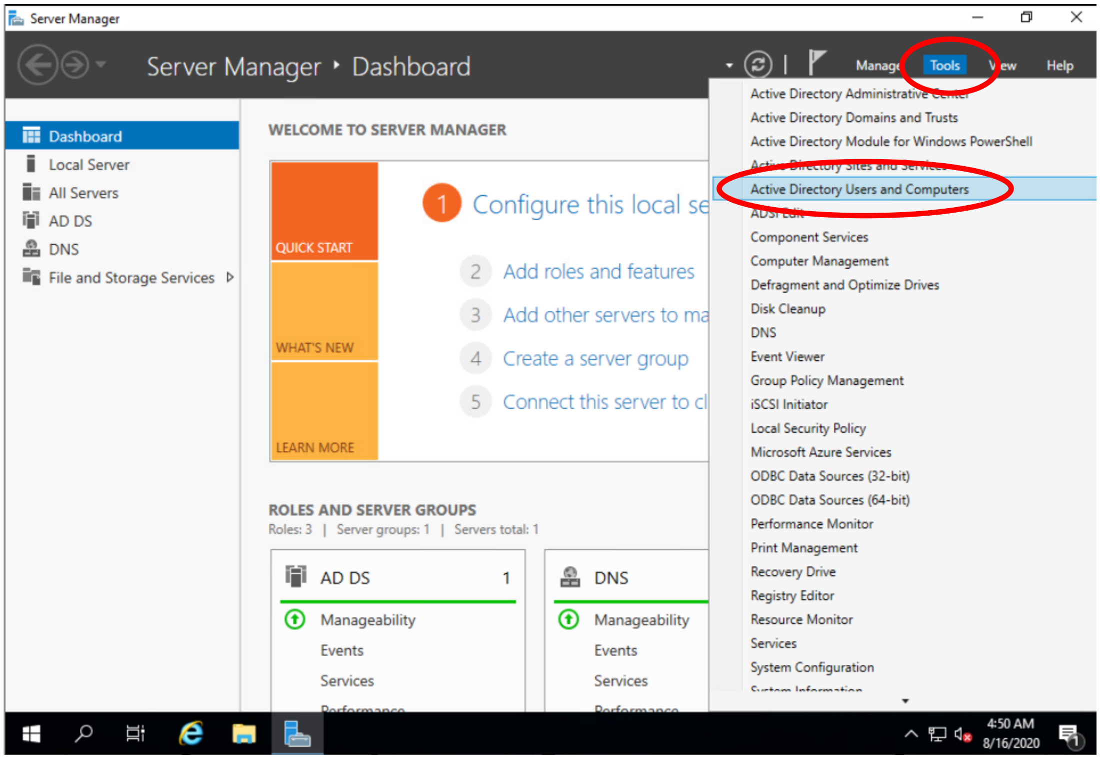
4) Click on the **name of your server**, then click on the **Actions** menu and choose **Power**, then **Power On** to boot up your server.



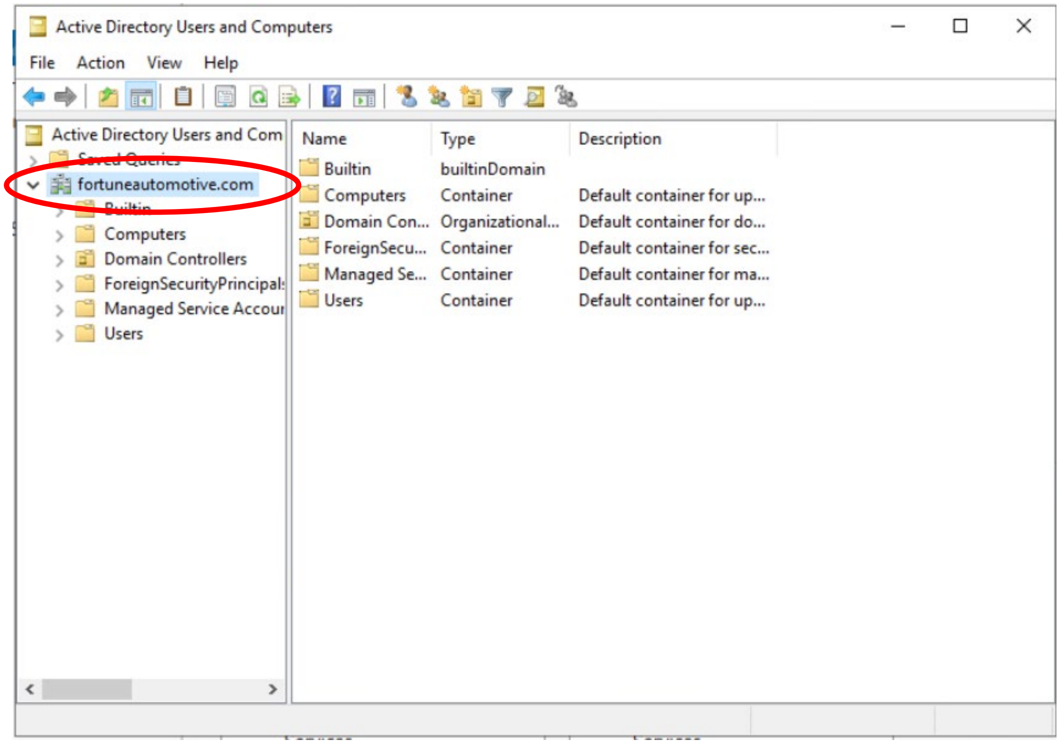
Power Status Powered On
Guest OS Microsoft Windows Server 2016 or later (64-bit)
VMware Tools Not running, version:12294 (Current)
DNS Name
IP Addresses
Encryption Not encrypted

5) As your server is powering up, click on the **Launch Web Console** link. This will open the server console window in a new browser tab.

6) When the Windows Server OS has finished booting, login to the server using the Administrator account you created during Lab #2. **NOTE: The Username will appear as FA\Administrator OR FA_YOURINITIALS\Administrator depending on how you created your AD in lab 2**. Also note that if you see FA\instructor, you can change this by clicking on **Other User** and entering **administrator** for the username and your password.

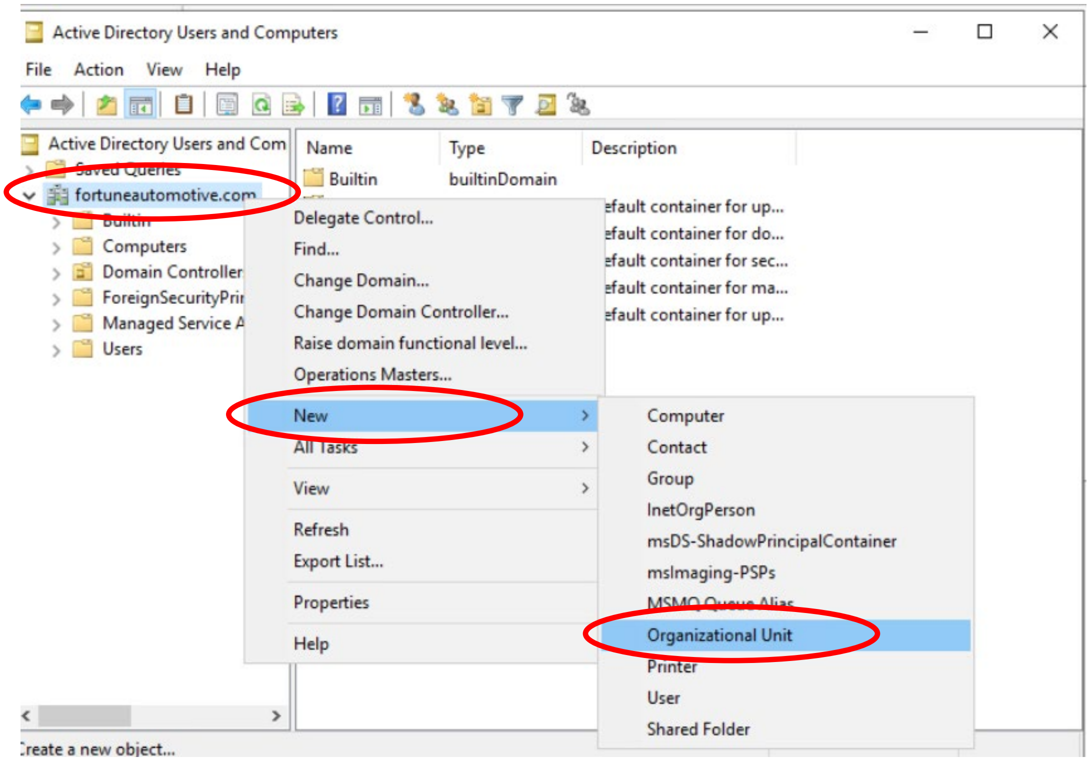


7) Once logged into the server you will need to run the Active Directory Users and Computers tool. This can be done from the Server Manager application. Click on the **Tools** Menu and select **Active Directory Users and Computers**.



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

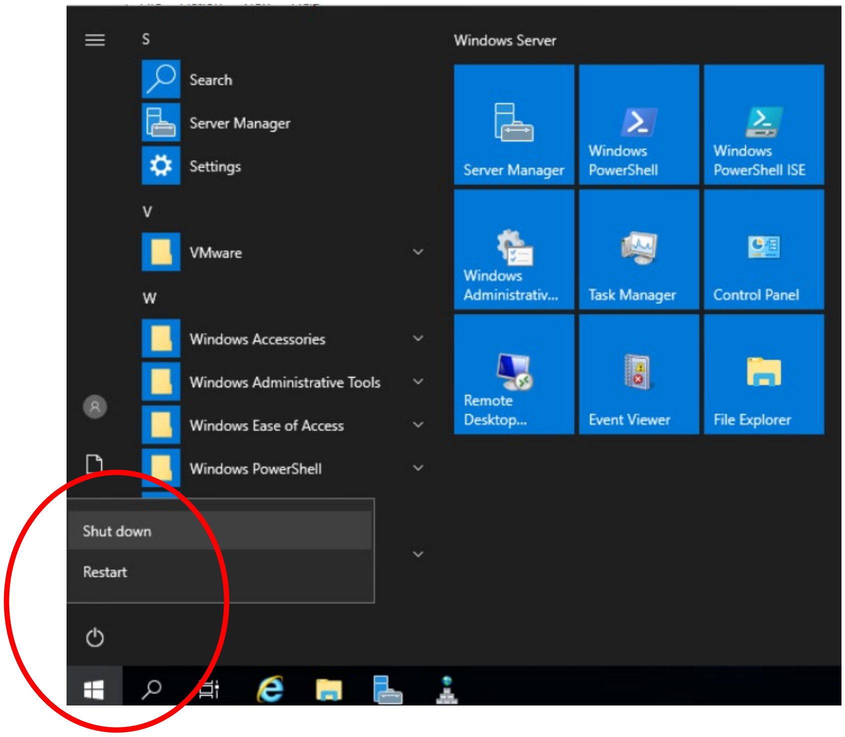
8) From this point you can begin to implement your AD design. OUs are created by first left-clicking on the domain (fortuneautomotive.com) to select it, then right clicking on folder contained on the left side of the window or anywhere in the right side of the window and choosing Organizational Unit from the menu.



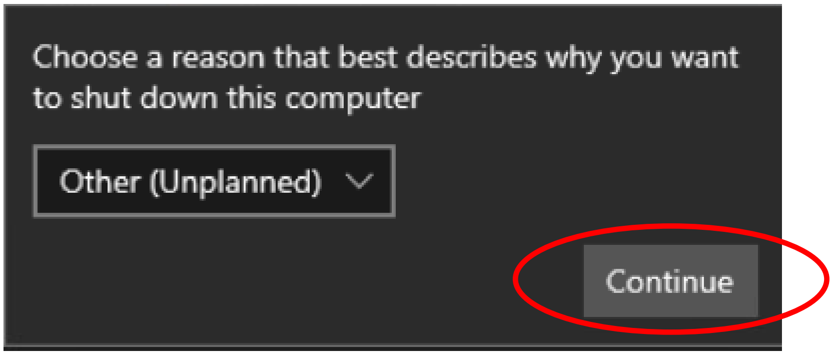
9) You can then name the OU and then add other OUs if your design calls for them. While you are not required to create and use OUs, they are very important with regard to the use of group policy (you will work with group policy in lab 4).

4. Create User Accounts and Security Groups

1) From within the AD Users and Computers tool you will need to create user account objects for all of the Fortune Automotive personnel contained within the Organizational Hierarchy. This is done the same way as it is when you create an Organizational Unit in Part 3, Steps 7-8 (simply choose User or Groups instead of Organizational Units from the menu).
2) You will need to populate the User Account object with the following information:
   a. Full Name
   b. Email
   c. Department
   d. Manager
3) As you create User Accounts, you will assign usernames and passwords to each user. **This needs to be documented within your design deliverable**.
4) If you created OUs within the AD make sure you are placing the User Account objects in their appropriate locations.
5) Once the User Accounts have been setup, create Security Groups containing those users who need to be grouped together for a specific purpose. For example, will all users within the Human Resources department need to access the same network resources (e.g. a printer or network drive)?



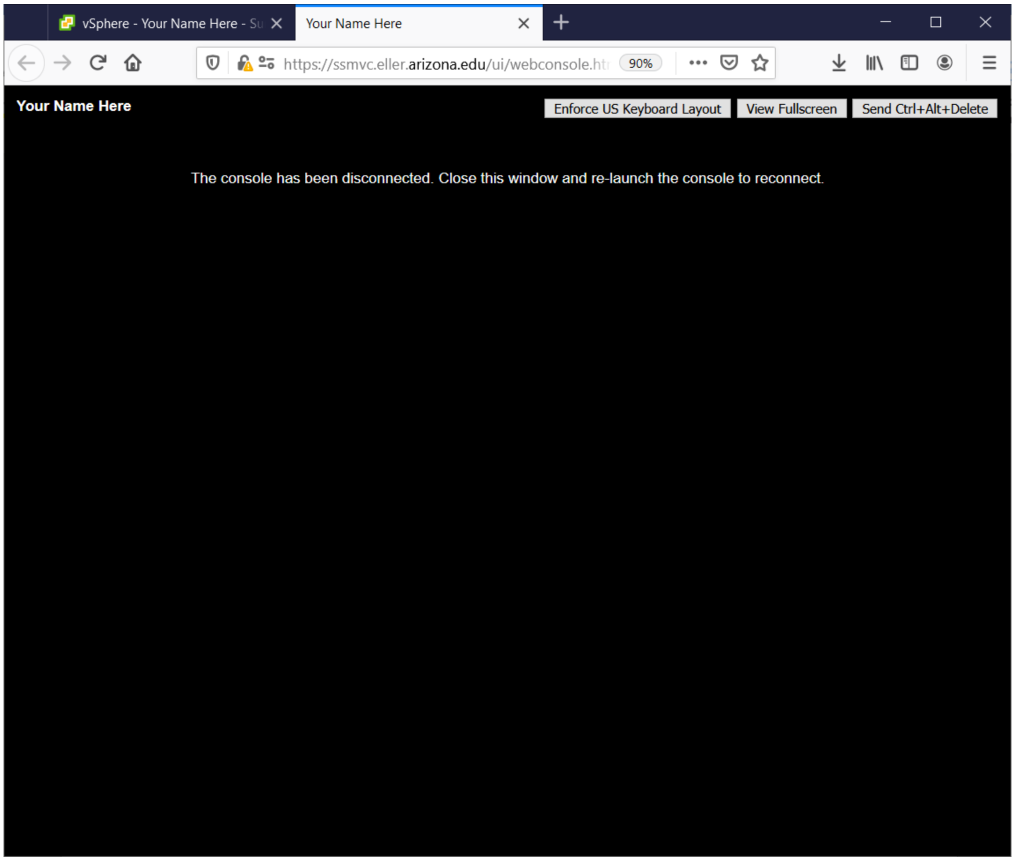
1) Now you can shut off your server. Click on the **Start** button in the lower left corner of the screen to bring up the Start screen. In the lower left corner you will see a power button. Click on the **power** button and choose **Shut down** from the menu.



Choose a reason that best describes why you want to shut down this computer

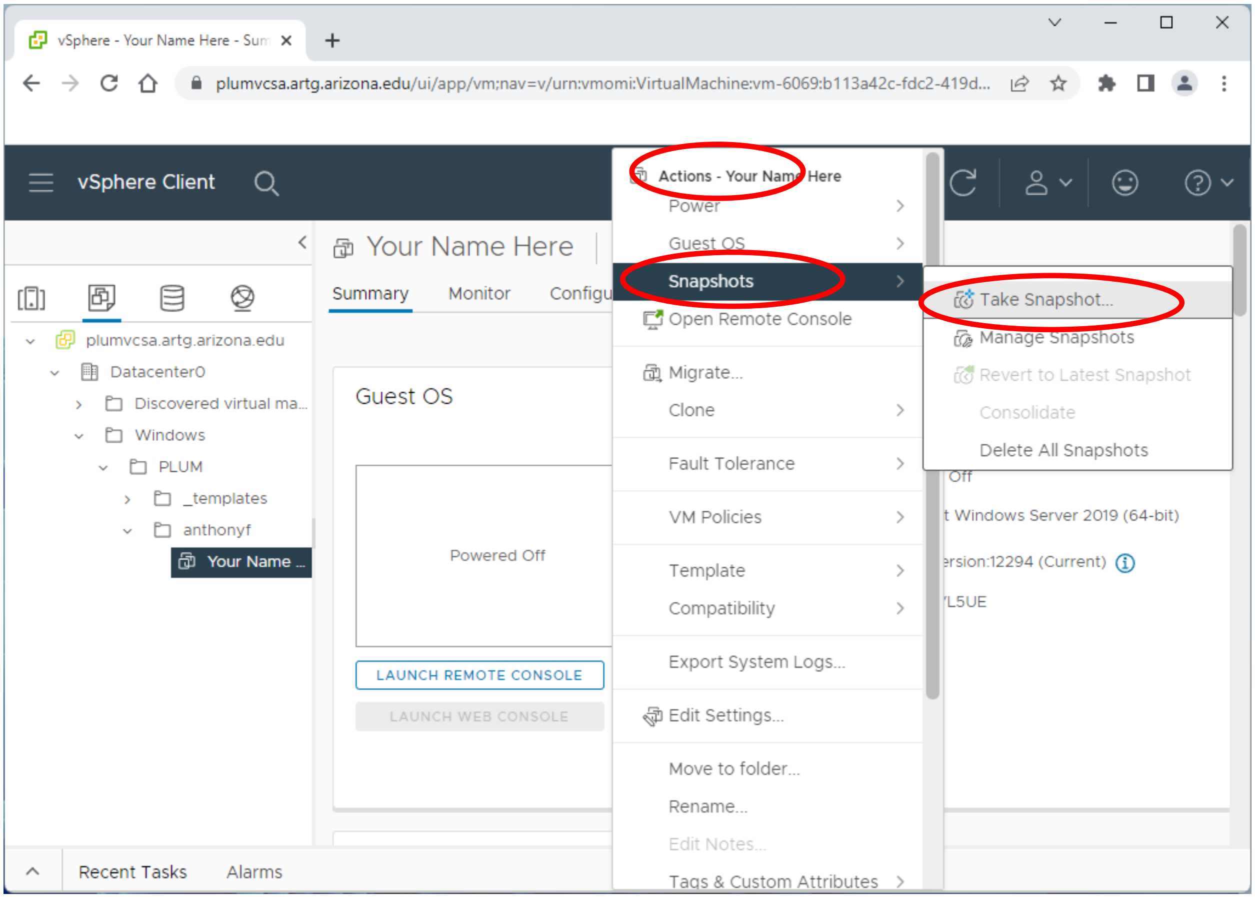
Other (Unplanned)

2) You will be asked to select a reason for the shutdown. **Choose any option** and click **Continue** to shut down the server.


vSphere - Your Name Here - Su
Your Name Here
https://ssmvc.eller.arizona.edu/ui/webconsole.ht
90%
Your Name Here
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

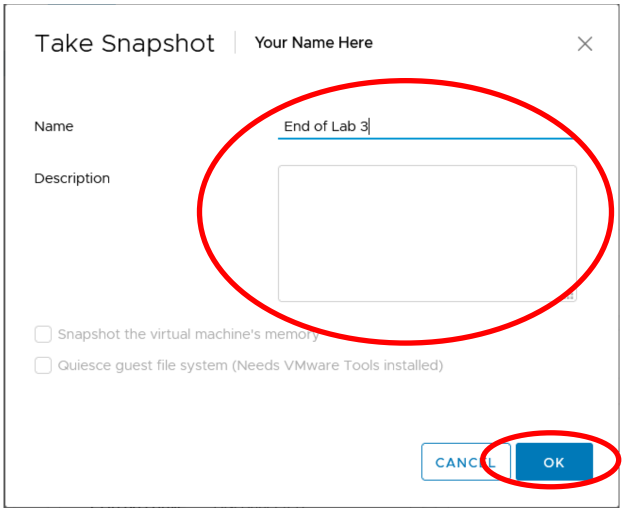
The console has been disconnected. Close this window and re-launch the console to reconnect.

3) When the server is completely shut down the screen will be black with the statement “The console has been disconnected”. Close the window for your server by clicking on the **X** in the upper right-hand corner of the open tab.



4) Now, go back to the web browser where the VMware web client is showing your server to take a snapshot of your server. This will create a point-in-time backup that will allow you to restore your server to the end of Lab 3 if you have problems when working on Lab 4.

5) Click on the **Actions** button, highlight the **Snapshots** option, and select **Take snapshot** from the menu.



Take Snapshot | Your Name Here

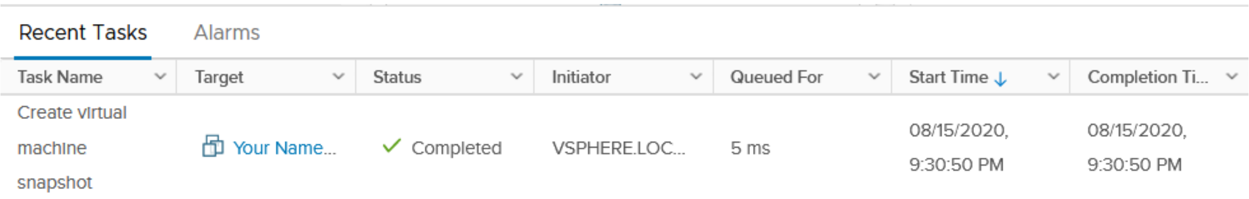
Name: End of Lab 3

Description:

□ Snapshot the virtual machine's memory

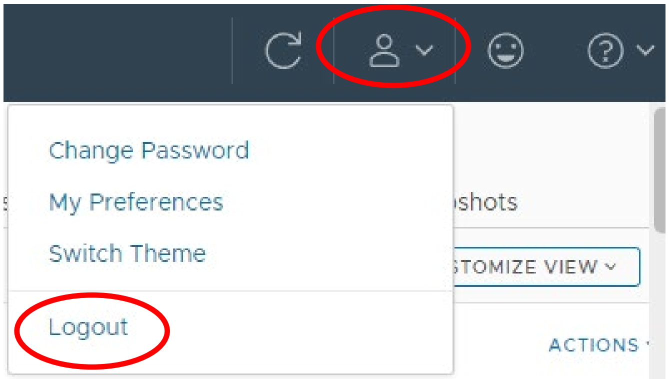
□ Quiesce guest file system (Needs VMware Tools installed)

6) Type in a name for this snapshot (**End of Lab 3** is recommended), provide a description if desired, then click **OK**.



Task Name	Target	Status	Initiator	Queued For	Start Time ↓	Completion Ti...
Create virtual machine snapshot	Your Name...	✓ Completed	VSPHERE.LOC...	5 ms	08/15/2020, 9:30:50 PM	08/15/2020, 9:30:50 PM

7) In the bottom of the screen, under the Recent Tasks section you will see a green check mark with Completed next to Create virtual machine snapshot.



8) Congratulations, you have completed Lab 3! To log out of the vCenter Web Client, **click on your username** in the upper portion of the screen and select **Logout** from the menu.

9) Close your web browser.

5. Document the new FA Active Directory

1) Throughout this process you should have been documenting the design of the new AD for Fortune Automotive. Once you have implemented the design you must make sure your design matches the documentation. ***If it does not, take this time to modify the documentation as necessary to complete this step***.
2) Please note: part of the document you submit will be compared to the implementation on your lab server during grading. So, make sure you provide accurate information for the user accounts you created and the overall design of your AD.
3) In addition, you will need to provide a written explanation of your design (what did you do and how) and a written justification for your design (why your design is a good one). These sections should be no more than 1-2 pages in length.

Lab Deliverables

At this point you should have the following:

a. An Active Directory design document containing the overall design of the new FA AD, and detailing user account and security group information.
    i. There is no overall requirement for how long your system documentation should be; however, the documentation must provide enough information to recreate the system in the event of system failure where no backups exist.
    ii. **Please use the Lab 3 Worksheet attached to this lab to provide your documentation**.
b. A completed AD matching the documented design on your lab server.

Submit the following via the D2L assignments section for the lab:

- Your design document

Lab Rubric

Lab #3 will be graded in two parts: your Active Directory design and your system documentation. Here is the breakdown for how your lab will be graded:

Sections	Additional Information
Following Instructions (10%)	Please make certain you follow the instructions for the Lab Deliverable.
Active Directory Design (25%)	You must make your design decisions and implement the design in the AD you are provided. Use the Fortune Automotive portal for information necessary to make your design decisions. The design ***must*** match your documentation.
Documentation (50%)	The content of your documentation is the most critical piece of your grade. Your documentation must match ***exactly*** with what you have designed in your Active Directory. This documentation will require filling out the documentation worksheet attached to the lab in D2L. Again, make certain your AD design is ***completely*** documented and your documentation matches the design ***exactly***.
Design Justification (15%)	You must justify your design. Explain why your design will meet the needs of the Fortune Automotive Corporation.

Lab Resources

- The Fortune Automotive Organizational Chart is attached to this assignment in D2L.