System Hardening

Activity 1: Active Directory Domain Services and Domain Connectivity

Right now, your Windows Server 2019 system is just a virtual machine (VM) running an operating system (OS) that is specialized to respond to requests from clients for authentication, resources, files, and more. Most people call machines (physical or virtual) "servers," but in reality, a server is actually a software program. Specifically, a server is a service that runs in the background as a process, independent of a sign-in, to provide a service or resource upon request, as long as the authentication and authorization check out. A server operating system is also known as a network operating system (NOS). Microsoft's Windows Server brand of server operating systems groups services into roles and features. You can install the Domain Name

System (DNS) role and/or the Dynamic Host Configuration Protocol (DHCP) role on a Windows Server 2019 system, which would turn the machine into a member server. A member server is a machine running a server operating system, connected to a domain, which has at least one role (server service) installed. If the machine is not connected to a domain, it would simply be known as a stand-alone server.

When the Active Directory Domain Services (AD DS) role is installed on a server operating system connected to a domain, that machine is now known as a domain controller (or DC for short), performing authentication and authorization for clients domain-wide. Even if the machine has other roles besides AD DS installed, it is just called a DC. Each DC is on the same level as the other DCs, containing the entire range of objects. This allows for easy and efficient replication (for consistency purposes) between the DCs.

If there is no existing DNS server when the AD DS role is installed, the DNS role must be installed at the same time. You will be prompted to install DNS during the AD DS installation. The reason why DNS must be in place for a domain to exist is very simple. When clients sign in to a domain, they sign in to a domain by the domain's name. DNS needs to be in place to resolve the query along the form of "Who is the domain controller for the mhs.net domain?" so the clients can send their requests to that specific machine. The initial query is for an DNS SRV (service) resource record that identifies a machine by its fully qualified domain name (FQDN), running Lightweight Directory Access Protocol (LDAP). Then, that machine's DNS A (IPv4 host address) or AAAA (IPv6 host address) resource record will resolve the server's FQDN to its corresponding IP address. Other SRV records are used to find global catalog servers, servers that can perform Kerberos authentication and password changes, and more. DNS is also needed on a domain for other reasons, like resolving computer object hostnames or FQDNs into their corresponding IPv4 addresses (through A resource records) or IPv6 addresses (through AAAA resource records).

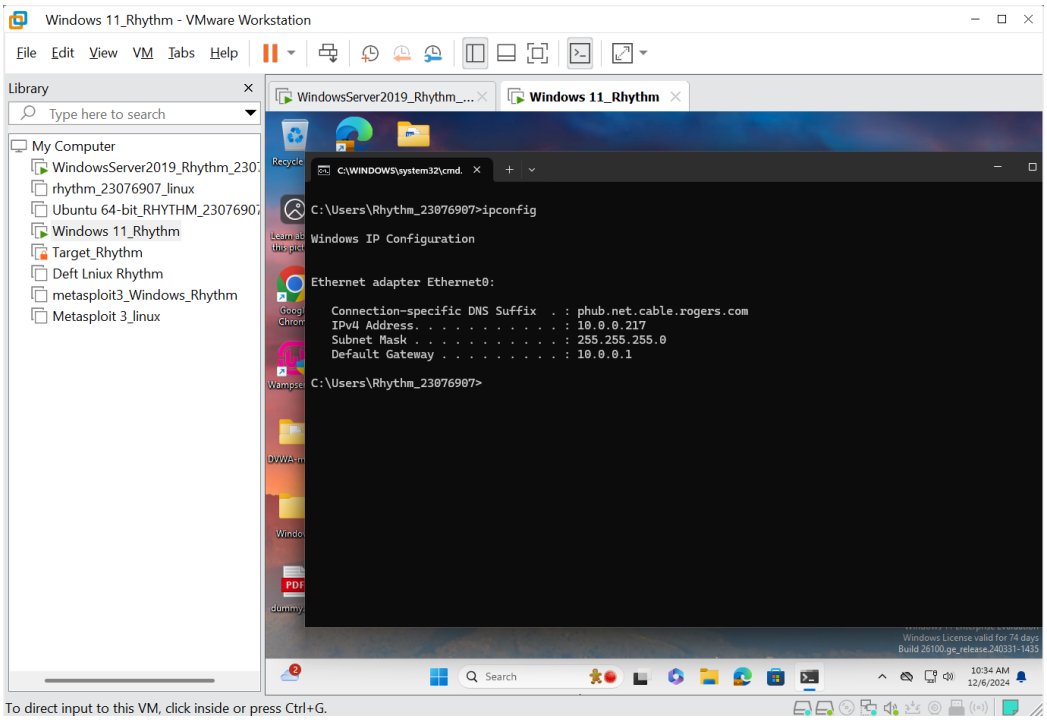
In this lab exercise, you will get started on your journey of hardening a domain while performing the following:

- Install AD DS
- Connect a client system to the domain

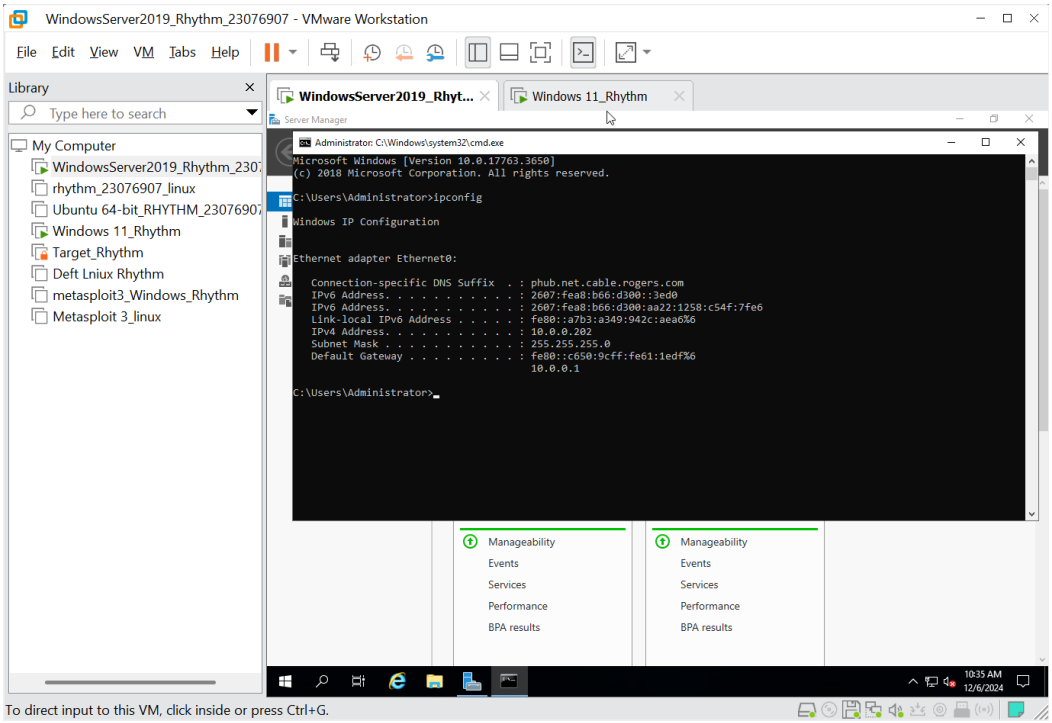
When you installed the Windows Server 2019 VM and the Windows 10 VM in initial Lab., you configured the network adapter to be in bridged mode, which puts those VMs on the same network as your host machine. Power on each VM, each in its own separate instance of VMware Workstation Player. Sign in with the credentials you used previously. Initially, you will sign in to the Windows

Server 2019 VM as Administrator, but that will change later. On the Windows Server 2019 VM, Server Manager will open by default, along with a popup. Click the **X** in the upper-right corner to close each. On each VM, click the **Start** button or in the search box, type **cmd**, and then click **Command Prompt**. Next type ipconfig and press **ENTER**. You should see that the VMs are on the same network as your host machine, based on the IP addresses given by your network's DHCP server.

Windows 11

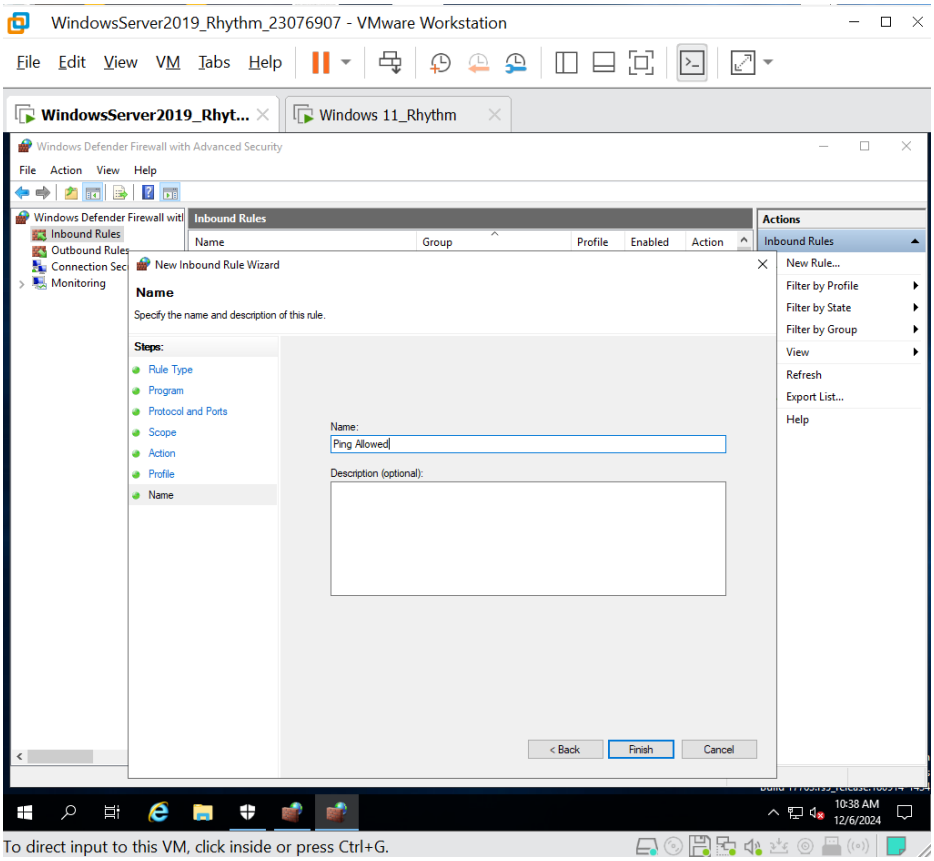


Windows server 2019

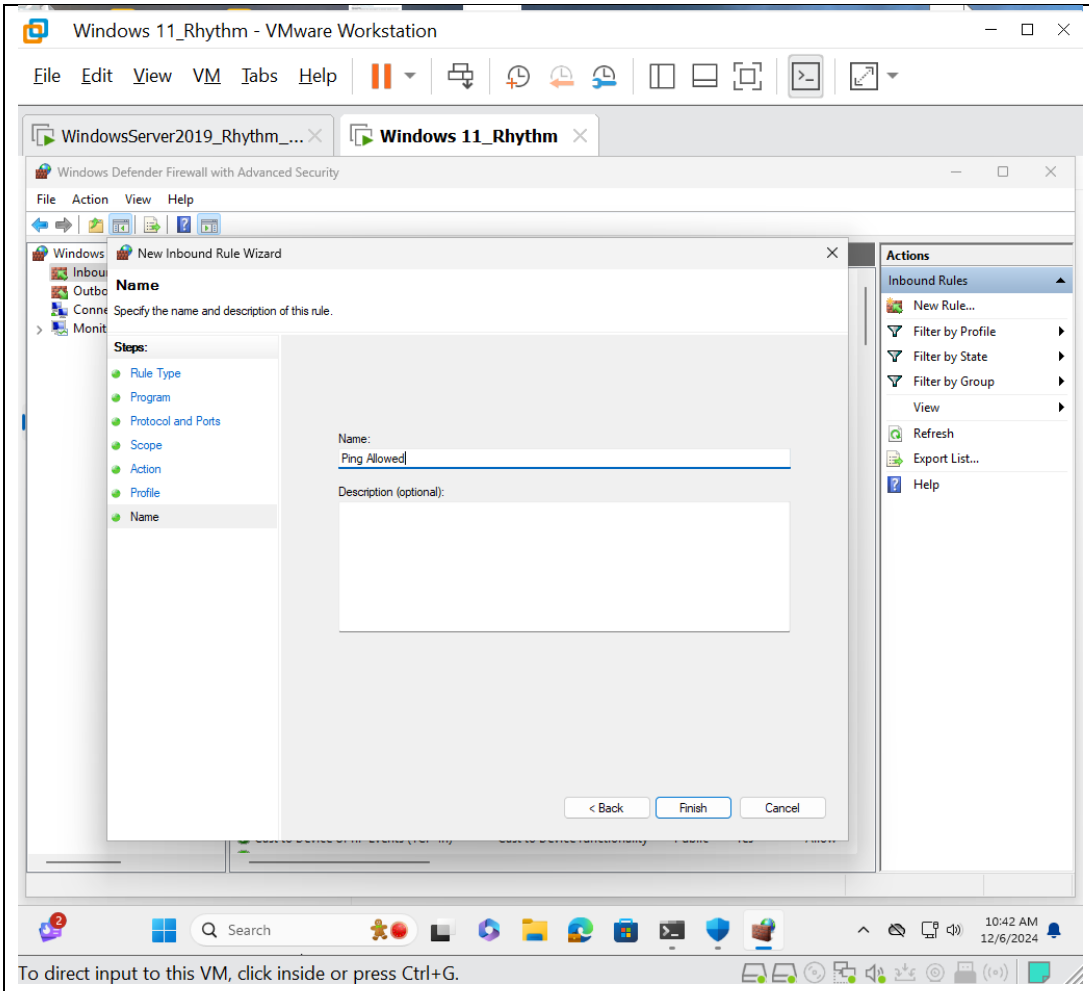


On each VM, click the **Start** button or in the search box, type firewall, and then select **Firewall & Network Protection**. Select **Advanced Settings** towards the bottom of the screen and then click the **Yes** button. In the left pane, click **Inbound Rules**. Next, right-click **Inbound Rules** and select **New Rul**…. Click the **Custom** radio button in the Rule Type screen and click the **Next** button. Click the **Next** button in the Program screen. In the Protocol Type: dropdown in the Protocol and Ports screen, select **ICMPv4** and click the **Next** button. Click the **Next** button in the Scope screen. Click the **Next** button in the Action screen. Click the **Next** button in the Profile screen. In the Name: box, type **Ping Allowed** and click the **Finish** button.

WINDOWS SERVER 2019



WINDOWS 10



Ping each VM from the other by typing **ping**, followed by the IP address of the other VM, in a command prompt and pressing **ENTER** on each VM. You should see four replies in each command prompt from the other VM that was pinged.

Servers should always have static IP addresses. You do not want the server's IP address to potentially change, as is the case with DHCP. Even though DHCP allows reservations, where the same Media Access Control (MAC) address always gets the same IP address, you do not want your server to depend on another server. If, for whatever reason, your DHCP servers are down or unreachable, when another server's lease expires or if it reboots, it will not be able to get an IP address and will be unreachable itself. Furthermore, you cannot install the AD DS role on a system that does not have a statically configured IP address.

On the Windows Server 2019 VM, click the **Start** button or in the search box, type **sharing**, select **Manage Advanced Sharing Settings**, click **Network And Sharing Center** in the address bar at the top of the screen, click **Change Adapter Settings** in the left pane, right-click the **Ethernet0** interface, select **Properties**, and double-click **Internet Protocol Version 4 (TCP/IPv4).** Select the **Use The Following IP Address:** radio button and put in either the IP address it currently has or another one on the same subnet in the IP Address: bar. Since my network ID is 192.168.1.0/24 (a subnet mask of 255.255.255.0 is simply /24 in Classless Inter-Domain Routing [CIDR] notation), I configured my Windows Server 2019 VM with an IP address of 192.168.1.19 (19 in the fourth octet was chosen on

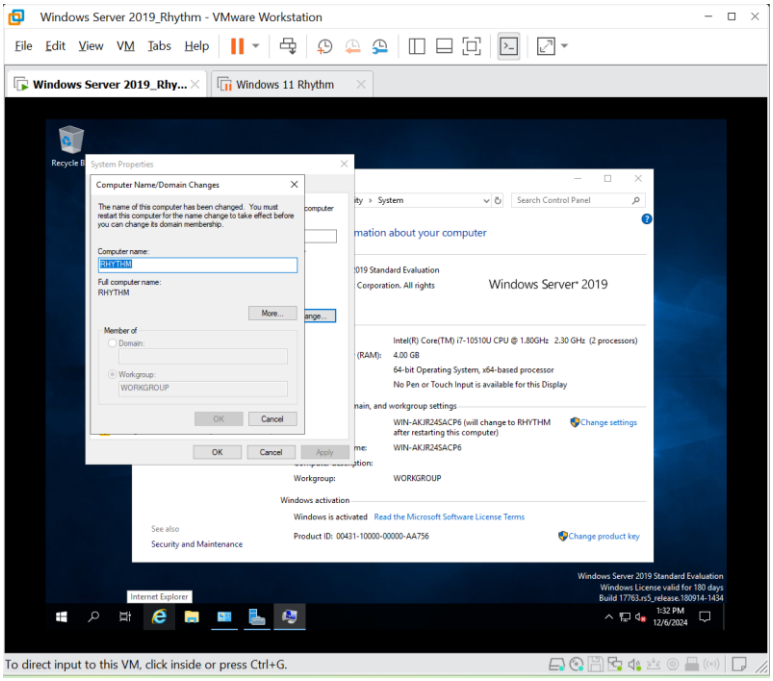
purpose, to match the 19 in Windows Server 2019). Put in the subnet mask of your network in the Subnet Mask: bar. In most cases, it will be 255.255.255.0, which can be confirmed with **ipconfig** in a command prompt on the VM or the host machine. Put in the IP address of the default gateway of your network in the Default Gateway: bar. In most cases, it will be 192.168.1.1, which can be confirmed with **ipconfig** on the VM or your host machine. In the Use the Following DNS Server Addresses: section, put 127.0.0.1 (the loopback address) in the Preferred DNS Server: bar, which means this machine will be its own primary DNS server (for the domain-related activities). Put 8.8.8.8 in the Alternate DNS Server: bar, to allow a Google Public DNS server to resolve queries for this machine if this machine's DNS service is not running. Click the **OK** button in the Internet Protocol Version 4 (TCP/IPv4) Properties box. Click the **OK** button in the Ethernet0 Properties box. It is a good idea to always "down" and "up" an interface after changes like these, to make sure the changes take effect. First, right-click the **Ethernet0** interface and select Disable. Then, right-click the **Ethernet0** interface and select Enable

Although it is fine to leave the IP address of the Windows 10 machine dynamic, assigned to it from your DHCP server, we can statically configure the Windows 10 VM with an IP address for consistency and troubleshooting purposes. On the Windows 10 VM, click the **Start** button or in the search box, type **sharing**, select **Manage Advanced Sharing Settings**, click **Network and Sharing Center** in the address bar at the top, click **Change Adapter Settings** in the left pane, right-click the **Ethernet0** interface, select **Properties**, and double-click **Internet Protocol Version 4 (TCP/IPv4)**. Select the **Use the Following IP Address:** radio button and then put in either the currently used IP address or another one on the same subnet in the IP Address: bar. Since my network ID is 192.168.1.0/24 (a subnet mask of 255.255.255.0 is simply /24 in CIDR notation), I configured my Windows 10 VM with an IP address of 192.168.1.10 (10 in the fourth octet was chosen on purpose, to match the 10 in Windows 10). Put in the subnet mask of your network in the Subnet Mask: bar. In most cases, it will be 255.255.255.0, which can be confirmed with **ipconfig** on the VM or the host machine. Put in the IP address of the default gateway of your network in the Default Gateway: bar. In most cases, it will be 192.168.1.1, which can be confirmed with **ipconfig** on the VM or your host machine.

In the Windows 10 VM adapter settings, in the Preferred DNS Server: bar, enter the IP address of your Windows Server 2019 VM (which you just configured), and set the value for Alternate DNS Server: to 8.8.8.8. Now the Windows Server 2019 VM will be the Windows 10 VM's DNS server and, eventually, its domain controller.

Step 1: The default hostname for the Windows Server 2019 VM is not a great hostname. Rename the Windows Server 2019 VM.

a) Click the **Start** button or in the search box, type This PC, right-click **This PC**, and select **Properties**.
b) In the Computer Name, Domain, and Workgroup Settings section, click **Change Settings**.
c) In the System Properties window, click the **Change…** button.
d) In the Computer Name/Domain Changes window, in the Computer Name: box, enter something more meaningful than the default name of this computer (I called mine MHS-SERVER) and then click the **OK** button.
e) In the Computer Name/Domain Changes popup, click the **OK** button.
f) In the System Properties window, click the **Close** button.
g) In the Microsoft Windows popup, click the **Restart Now** button to restart the VM.



Step 2: Configure a password for the Administrator account. The system will not be able to install the AD DS role if the Administrator account does not have a complex password.

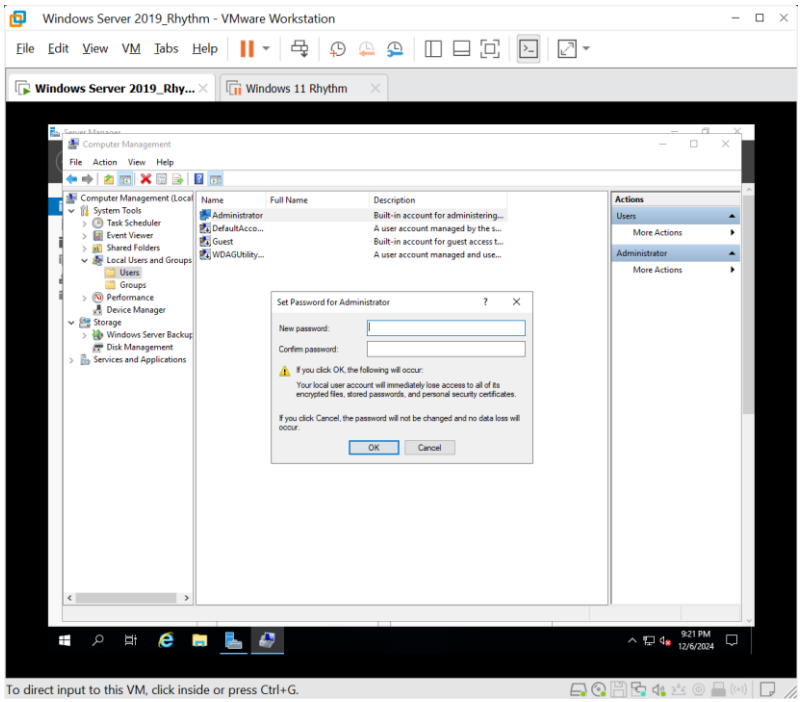
a) Click the Start button or in the search box, type **Computer Management**, and then click **Computer Management**.

b) In the Computer Management window, in the left pane, click **Local Users and Groups**.

c) In the middle pane, double-click the Users folder.

d) Right-click the **Administrator** account and select **Set Password….**

e) Click the **Proceed** button.



f) In the New Password: and Confirm Password: textboxes, enter a password of at least eight characters, using at least three characters from the following groups: uppercase letters, lowercase letters, numbers, and symbols. Click the **OK** button.

g) Close the Computer Management window.

Step 3 Install the AD DS role.

a) Click the Start button and then click the Server Manager tile. In the Server Manager popup, put a check in the box next to Don't Show This Message Again and then click the **X** at the top right of the popup.

b) Click **Manage hyperlink** at the top of the screen and then click **Add Roles and Features**.

c) At the Before You Begin screen, click the **Next** button.

d) At the Installation Type screen, with Role-based or Feature-based Installation selected, click the **Next** button.

e) At the Server Selection screen, with Select a Server from the Server Pool selected and the VM highlighted below, click the **Next** button.

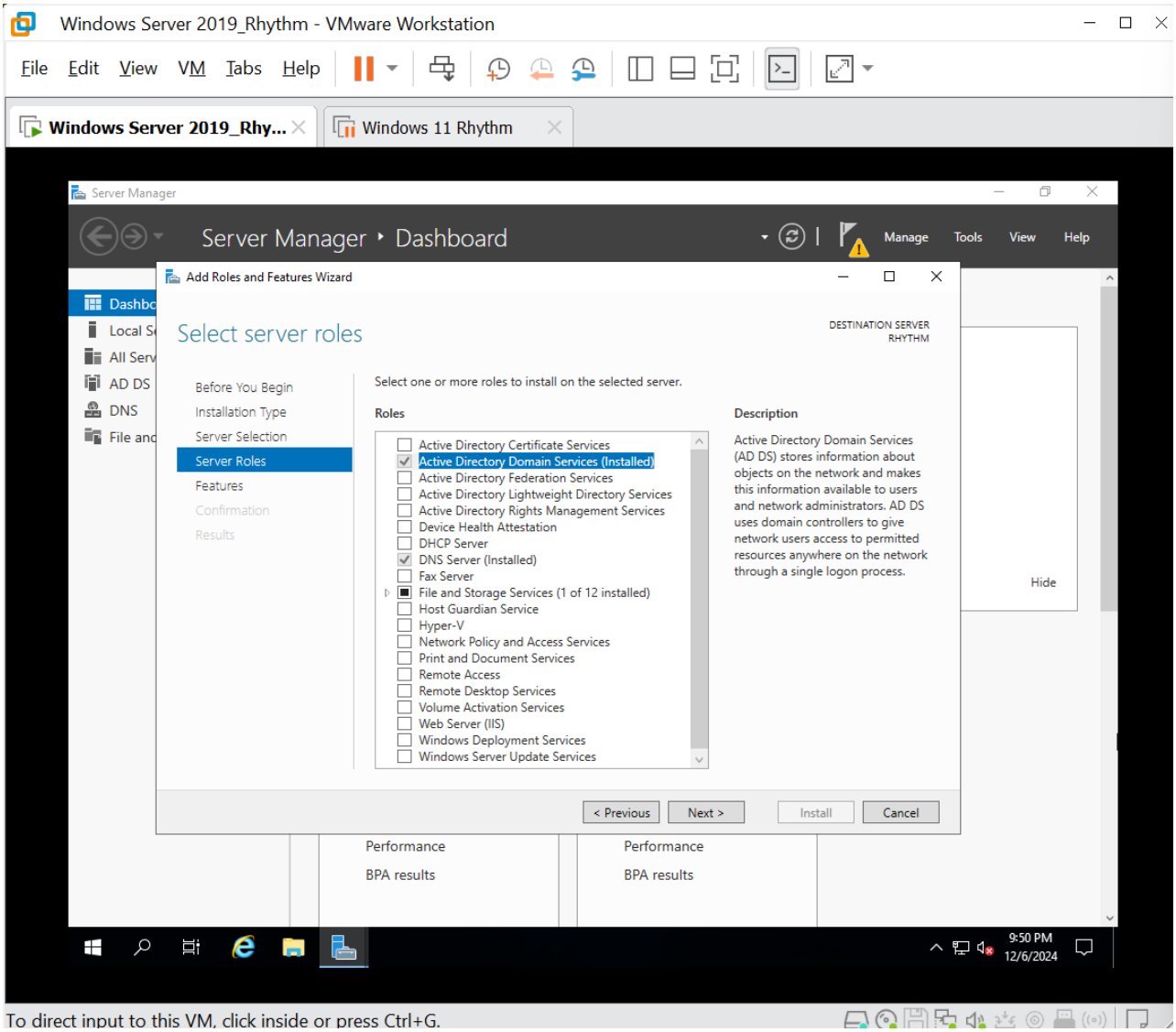
f) At the Server Roles screen, put a check in the box next to Active Directory Domain Services. After you put a check in the box, a popup will ask, "Add features that are required for Active Directory Domain Services?" With the check in the Include Management Tools (If Applicable) box, click the **Add Features** button. Then click the **Next** button.

g) At the Features screen, leave the default selections and click the **Next** button.

h) At the AD DS screen, read the information and click the **Next** button.

i) At the Confirmation screen, put a check in the box next to Restart the Destination Server Automatically If Required. In the popup, click the **Yes** button and then click the **Install** button. You will notice a progress bar showing the progression of the installation.

j) When the installation completes, you will see the message "Configuration required. Installation succeeded on," followed by the name of your computer. Click the **Close** button. Already Installed

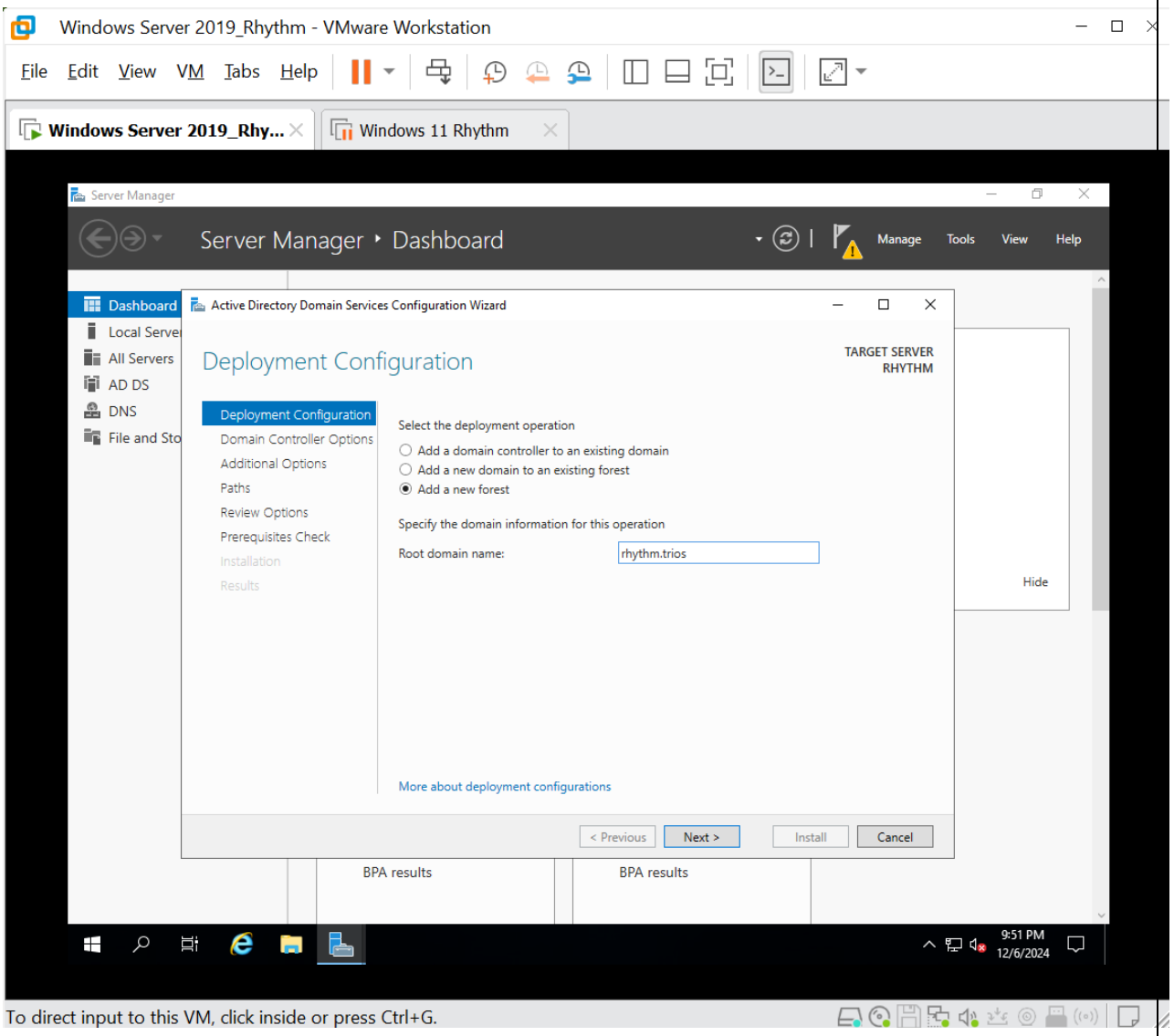


Step 4: Promote the machine to a domain controller.

a) Click the yellow triangle with the black exclamation mark in it, under the flag next to Manage. In the Post-deployment Configuration section, click **Promote This Server to a Domain Controller**.

b) At the Deployment Configuration screen, select the radio button for **Add a New Forest**, enter a domain name into the Root Domain Name box (I chose mhs.net), and click the **Next** button.

c) At the Domain Controller Options screen, notice that the Domain Name System (DNS) server checkbox is checked as well as the Global Catalog (GC) checkbox (which cannot be unchecked). Enter a password in the Password: and Confirm Password: textboxes and then click the **Next** button, leaving the Forest Functional Level: and Domain Function Level: values at their defaults.



d)

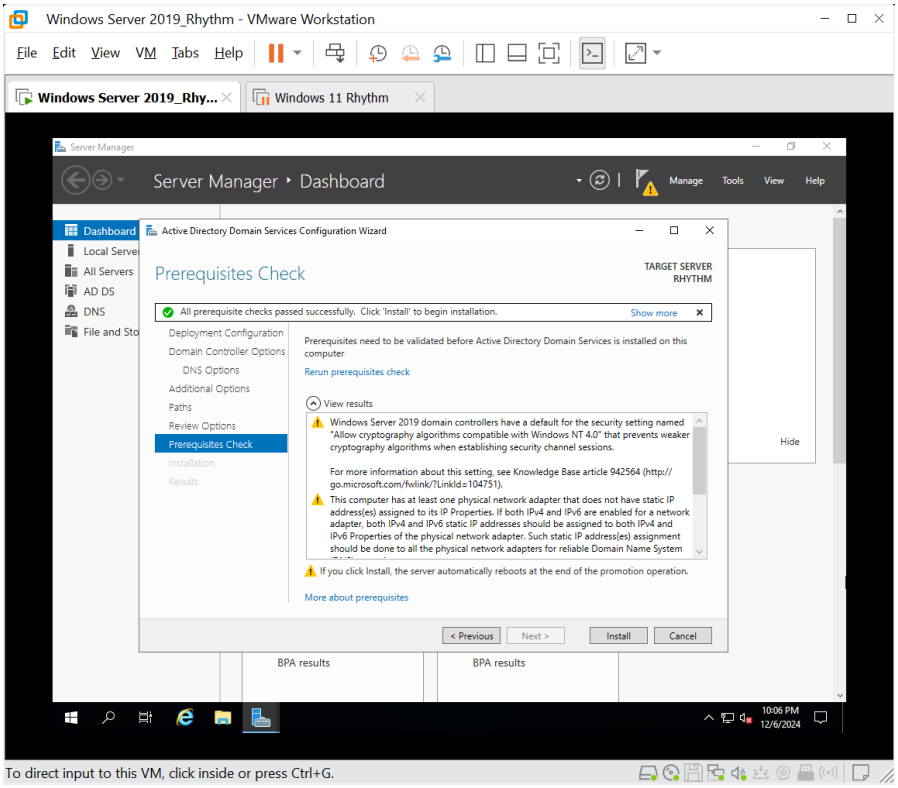
e) At the DNS Options screen, you will see a message stating “A delegation for the DNS server cannot be created because the authoritative parent zone cannot be found….” Click **Show More** and read the last words of the paragraph, “Otherwise, no action is required” (which applies here), and click the **OK** button. Click the **Next** button.

f) At the Additional Options screen, let a default name populate into the textbox and click the **Next** button.

g) At the Paths screen, leave the default selections and click the **Next** button.

h) At the Review Options screen, review your selections and click the **Next** button.

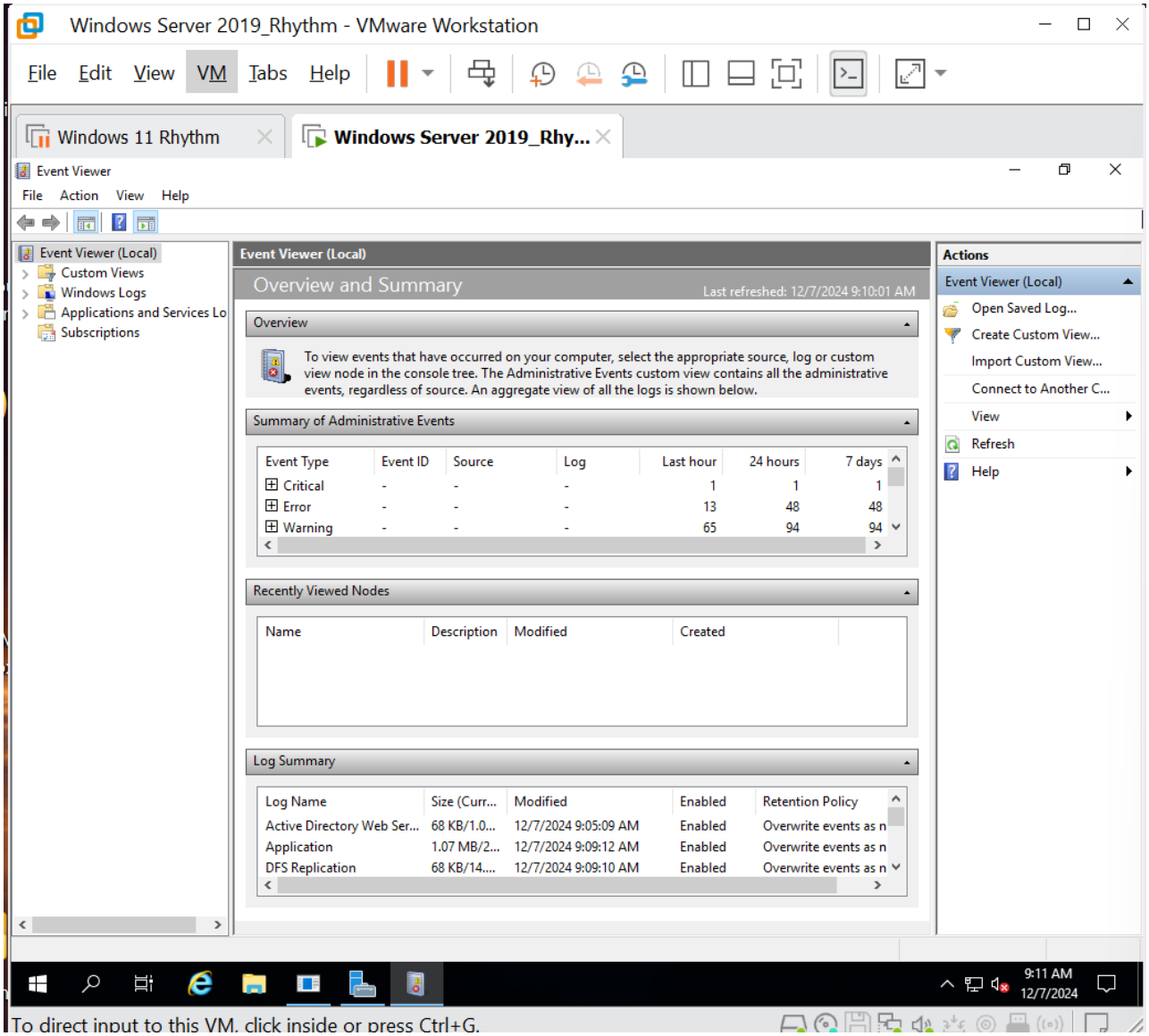
i) At the Prerequisites screen, you should see the message All Prerequisite Checks Passed Successfully. There will be some warnings. Read them, but do not worry about them. Click the **Install** button. You will notice various progress messages.



j) At the You're About to Be Signed Out box, click **Close**. You will see the blue Applying Computer Settings screen with dots going around in a circle for a while.

k) Press **CTRL+ALT+INSERT** to unlock the VM when you see the prompt. INSERT is used instead of DELETE to send this control signal to the VM, not the host machine. Alternatively, on the VMware menu, click **Player** and then click **Send Ctrl+Alt+Del**. Put in your password. You should see the desktop.

Step 5: Event Viewer, which is found on all versions of Windows, including client and server OSs, can be used for troubleshooting and verification. This helps ensure that any accidental, malicious, or simply unwanted changes are logged and able to be traced, which makes it easy to hold users accountable.



Event Viewer displays the following information to you in a GUI, aggregated from multiple log files:

- **Application** Contains events from programs running (for example, a backup of the database completed successfully).
- **Security** Contains security and audited events, including sign-in attempts, directories and files accessed, and privilege escalation.
- **System** Contains OS information and events, including services that were not able to start or the last reboot of the OS.
- **Directory Service** Contains events correlated to Active Directory functionality, like replication.
- **DNS Server** Contains events on the DNS service, which is convenient for troubleshooting name resolution issues.

There are other log files containing events on various features of Windows Server 2019 and its services.

Now, you will use Event Viewer to verify that the AD DS role installation succeeded. Open Server Manager and click **Tools** at the top of the screen. After the promotion to a domain controller, additional administrative tools will be available. Click **Event Viewer**.

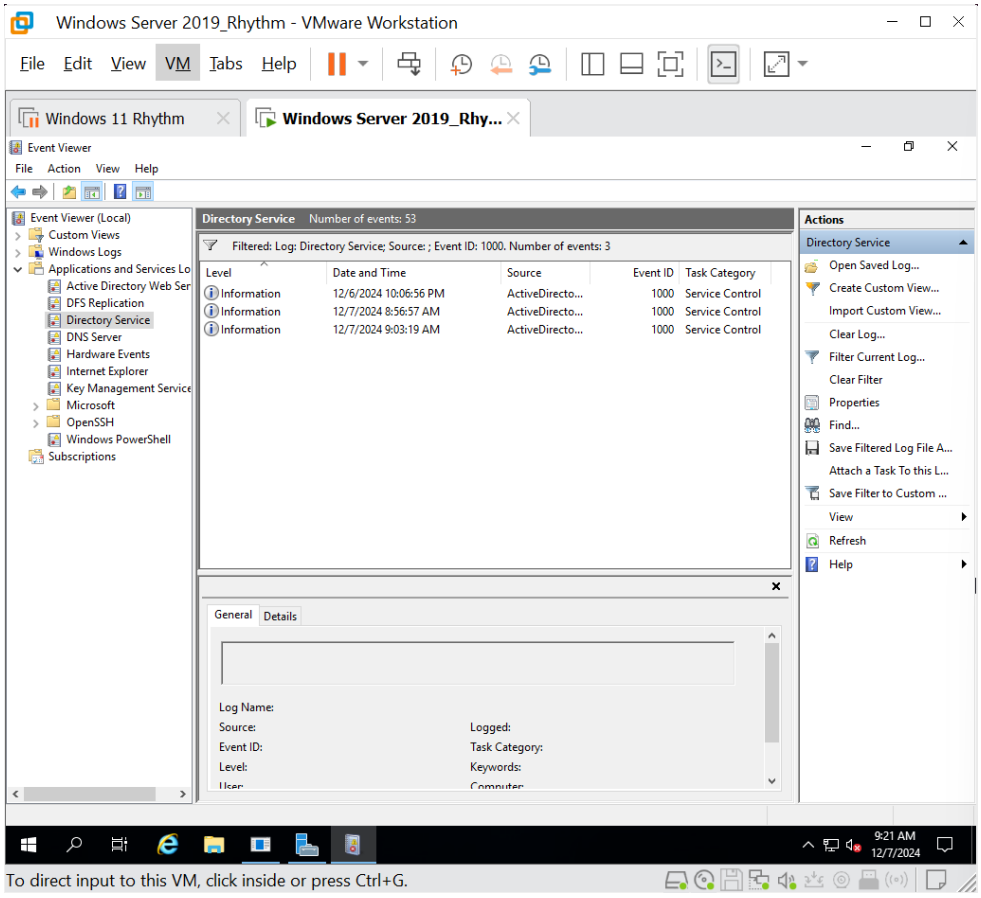
a) In the left pane, expand Applications and Services Logs by clicking on the arrow. Select Directory Service.

b) Click a column header to sort by that column. Click the column header a second time to reverse the order.

c) Navigate the entries with the UP ARROW and DOWN ARROW keys on the keyboard. The information displayed in the lower pane can be seen in its own window by double-clicking an entry. If you click the Copy button in the popup, you can copy the event information, which can be pasted into a file for future reference. From that popup, you can navigate the other entries by clicking the up- and down-arrow buttons on the popup. Click the **Close** button to close the popup.

d) To filter the results, in the Actions section on the right pane, click **Filter Current Log**… and then customize as desired. To remove the filter and see all results, again, click **Clear Filter** (which is only visible when a filter is in place) in the Actions section in the right pane. This is helpful for isolating something specific you might be looking for.

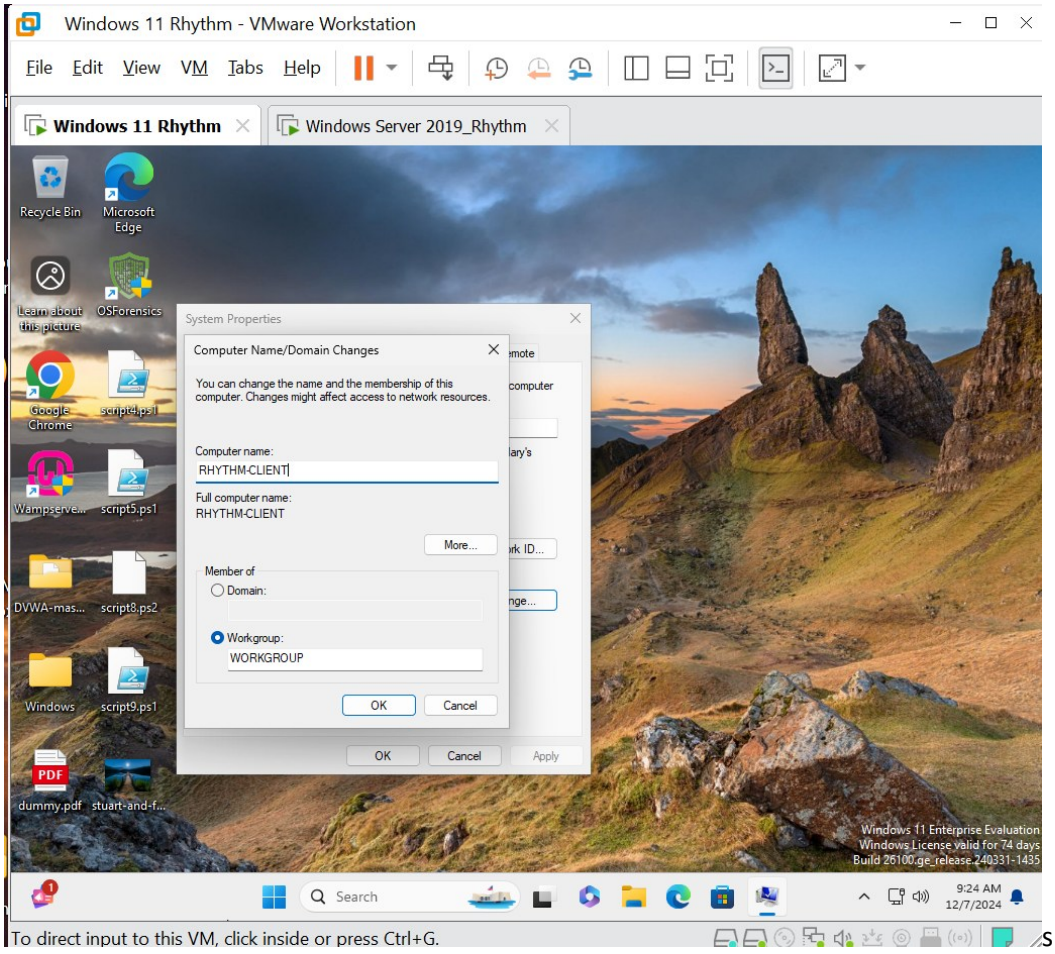
e) Filter by Event ID 1000, which corresponds to Microsoft Active Directory Domain Services startup complete.



Step 6: The default hostname for the Windows 10 VM is not a great hostname. Rename the Windows 10 VM.

a) Click the **Start** button or in the search box, type **This PC**, right-click **This PC**, and select **Properties** or click **Properties** in the right pane.

b) Click the **Rename This PC** button and then in the textbox type a more meaningful name than the default name of the computer (I called mine -MHS-CLIENT). **Take the screenshot.** Click the **Next** and then click the **Restart Now** button to restart the VM.



c) Sign in, after the reboot, to the Windows 10 VM.

Step 7: Join the Windows 10 VM to the Active Directory domain.

a) Click the **Start** button or in the search box, type **This PC**, right-click **This PC**, and select **Properties** or click **Properties** in the right pane.

b) In the Related Settings section, click **Rename This PC (Advanced)**. A System Properties window, with the Computer Name tab selected, will open.

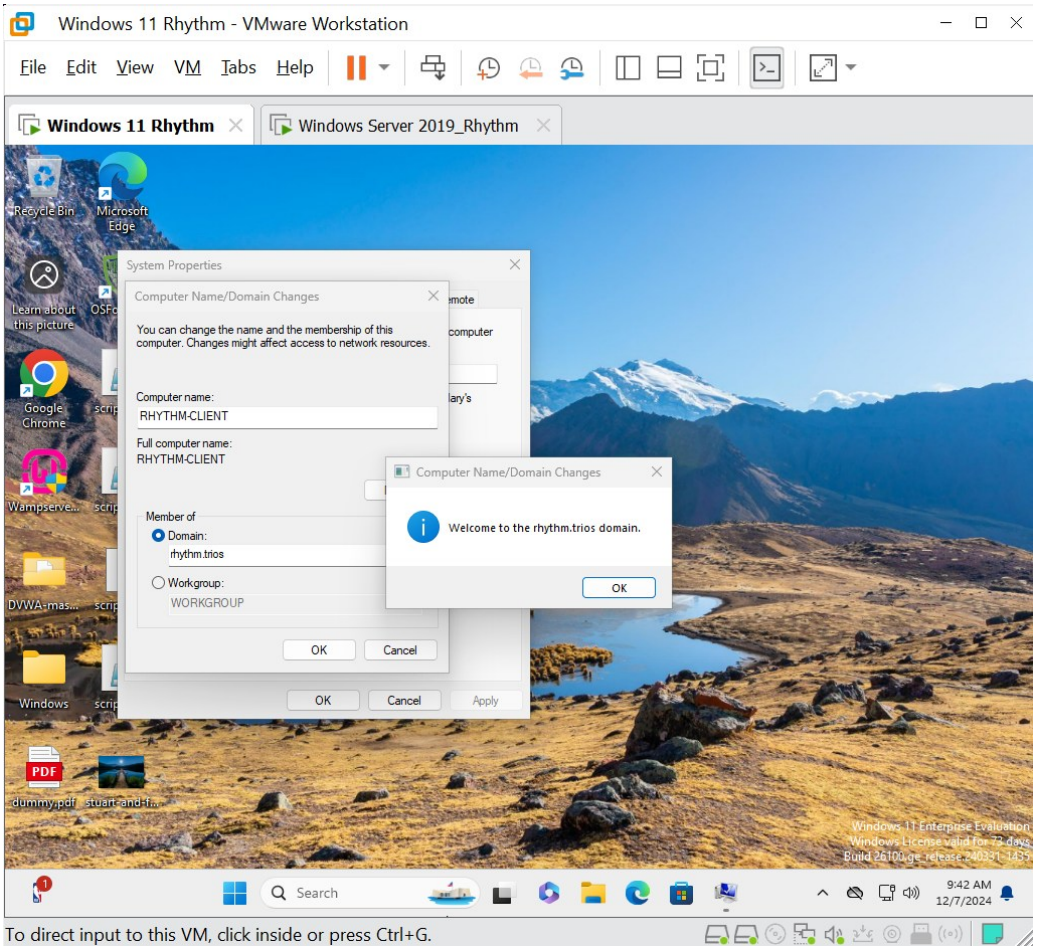
c) In the System Properties window, click the **Change…** button.

d) In the Member Of section, select the radio button next to Domain, enter the name of the domain you configured earlier (mine is mhs.net), and click the **OK** button.

e) At the Computer Name/Domain Changes popup, enter the username Administrator and the password you configured earlier for the Administrator account on the Windows Server 2019 VM. This is the name and password of an account with permission to join the domain, as

indicated in the popup. Click the **OK** button.

f) You should see a popup welcoming you to the domain. **Take the screenshot.** Click the **OK** button.

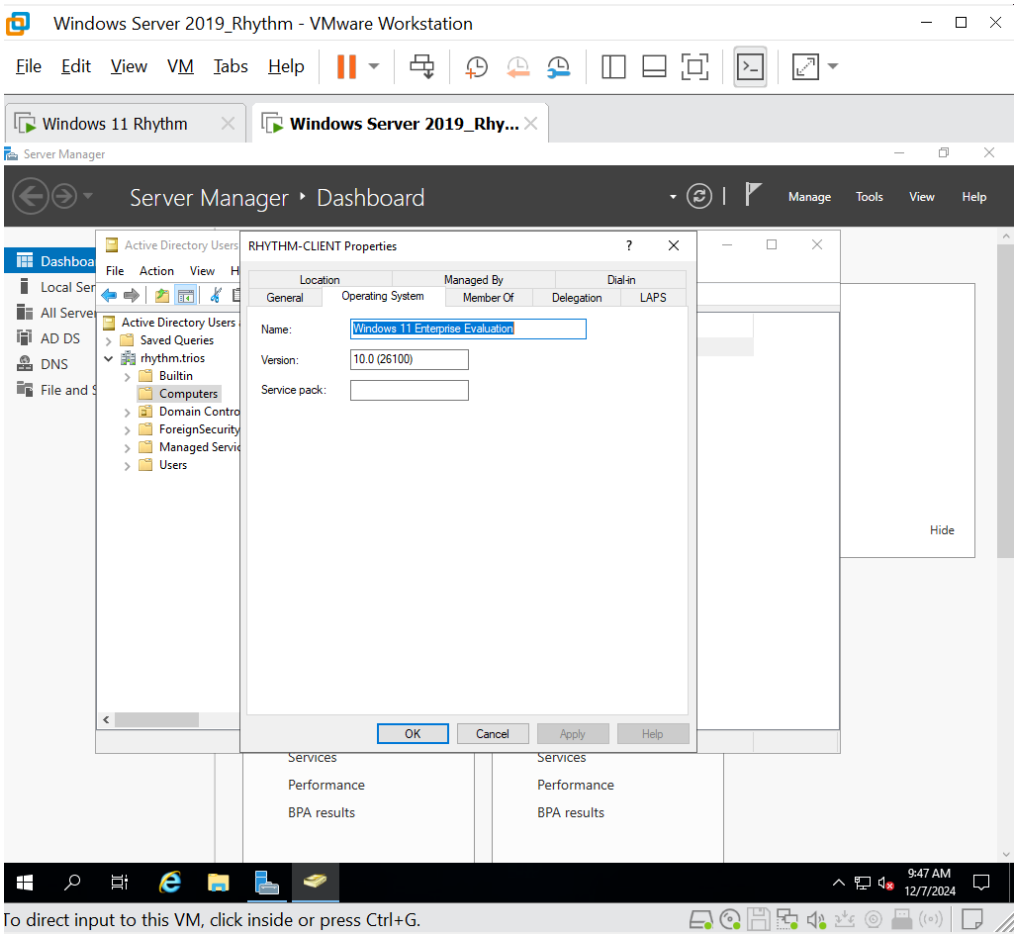


g) In the popup that states "You must restart your computer to apply these changes," click the **OK** button. In the System Properties window, click the **Close** button. In the next popup, click the **Restart Now** button to reboot.

h) On the Windows Server 2019 VM, open Server Manager, click **Tools**, and click **Active Directory Users and Computers**. Expand your domain by clicking the arrow. Select the Computers container, in the left pane, and notice the client machine that was just added to Active Directory, in the right pane. **Take the screenshot.**

i) Double-click the computer in the right pan

j) e. In the window that pops up, notice in the Operating System tab that the correct OS has been identified. **Take the screenshot.**



Activity 2: Organizational Units and Groups

An organizational unit (OU) organizes AD objects, like a folder organizes files on a hard drive. However, unlike folders, which are part of the path of a file, and domains, which are part of the DNS namespace, OUs are not part of the DNS namespace. OUs offer multiple ways to achieve great flexibility, more than just domain administration, in managing resources of business units, departments, and divisions.

Many different objects can be placed inside an OU, including users, groups, computers, and shared folders. OUs can even be placed inside of other OUs. The nesting of OUs allows for the hierarchical grouping of objects and resources in many different ways, and it can flex at any point in one of many different directions, due to business needs or reorganization. When moved, OUs will inherit the permissions of a new parent by default. Permissions set on a parent OU are automatically inherited by all the objects in a child OU, but this behaviour can be overridden.

Microsoft recommends to not have more than 10 levels of OUs. Horizontal OUs are more efficient than vertical OUs. More processing will be needed for vertically nested OUs for multiple layers of policies and settings.

Group Policy objects (GPOs) can be applied to all objects in an OU, with inheritance for nested OUs. This will allow you to push out common policies dealing with security and configuration to the objects in an OU. For example, a GPO can restrict users from installing new programs, accessing the Control Panel, and making certain selections for display, networking, desktop, and other settings.

You can even use OUs to delegate administrative control over users and groups to appropriate users and groups. It is not realistic for a single person, like an IT director, to do all the work. Assigning tasks and responsibilities to others for certain OUs makes much more sense. One systems administrator could be in charge of the Marketing OU, and another one can administer the Human Resources OU. Responsibilities for managing printers and print queue objects can be given to one systems administrator, while another can manage security permissions for users and groups. This delegation occurs at the OU level, not at the object level. Delegation also prevents systems administrators from having huge authority over large numbers of objects. Delegation from a parent OU can be inherited by multiple child OUs, inside of the parent OU, at the same time. Implementing the principle of least privilege, each systems administrator will have just enough control to perform their tasks and not a single drop more.

Security permissions to resources should be assigned to group account objects, not user account objects. Think of the groups as roles that users fill. If security permissions to resources were assigned to user objects, it would be an administrative nightmare. If a user was being moved out of a department in the organization that has access to 100 resources and into a different department that has access to 100 other resources, you would have to make 200 changes if permissions were assigned to user account objects. If groups are implemented, and permissions to resources are tied to group account objects, all you would have to do is remove the user's membership from the original group and add the user as a member to the new group. That would be two changes instead of 200. Furthermore, as is the practice today, users can serve in multiple roles, and as such, they need to have the cumulative permissions of multiple groups. Giving permissions to groups and assigning users to groups is the way to go.

It is important to understand the differences between groups and OUs. Think of a group as a collection of users or even computers. A group can also be a member of another group. The usage of groups is for security purposes (for example, granting permissions to a resource such as a shared folder, file, server, printer, or application). These permissions cannot be assigned to OUs. Groups have a security identifier (SID) that uniquely identifies them, but OUs do not.

An OU is more like a logical boundary for organizing your infrastructure and applying GPOs to it (GPOs can also be linked to a site and domain) that implement security policies to common objects. GPOs cannot be linked to groups. Whereas an OU can contain group objects, user objects, computer objects, and other OUs, an object can only be inside of a single OU. Conversely, a user object and group objects can be a member of multiple groups.

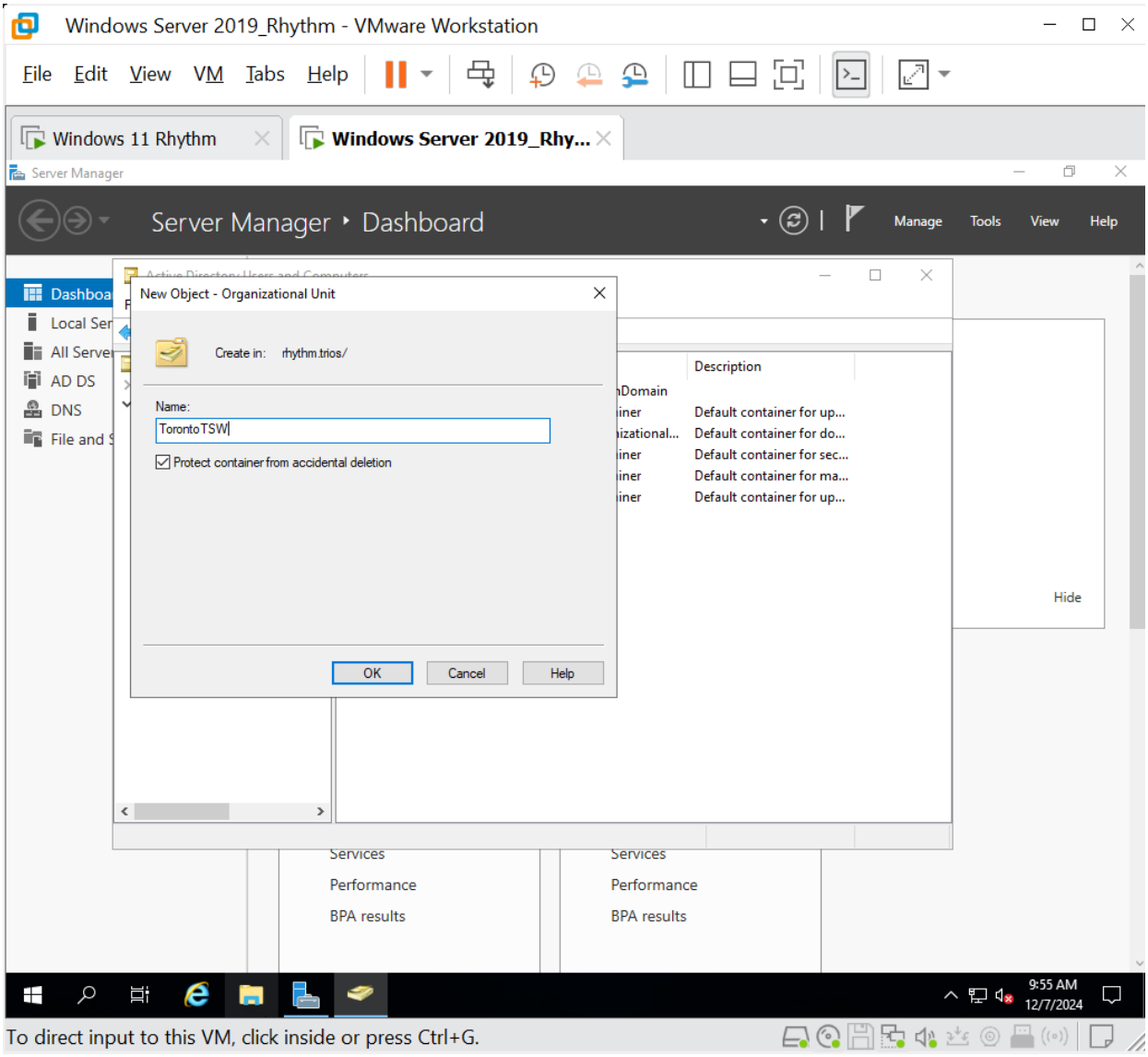
In this lab exercise, you will create logical containers for AD objects.

Step 1: Before configuring OUs, you need to decide on a hierarchy and structure that meets your business and technical needs. Names and descriptions of OUs should be short and to the point. Names of objects can be duplicated in multiple OUs, but not in the same OU.

a) On the Windows Server 2019 VM, open **Server Manager**, click **Tools**, and click **Active Directory Users and Computers**. You will notice multiple default containers. Clicking each container reveals the contents in the pane on the right. Built-in contains default group objects. Computers contains the computer object representing your Windows 10 VM that was just joined to the domain. Double-click the computer object to see more information about it. Domain controllers contains a computer object for the Windows Server 2019 VM you are on now. Double-click the computer object to see more information about it. ForeignSecurityPrincipals and Managed Service Accounts will be empty. Users contains default user objects and group objects.

b) Right-click the domain name (mine is mhs.net), mouse over New, and select **Organizational Unit**.

c) In the Name: textbox, type **TorontoTSW**, uncheck the box marked Protect Container from Accidental Deletion, and click the **OK** button.



If this box was checked, and you wanted to remove the OU, you would have to click View from the menu at the top and then select Advanced Features (this is a toggle selection, so clicking View and then Advanced Features again returns the view to the way it was). With Advanced Features selected, more items appear in the hierarchy, under the domain name, and more tabs appear for each object's properties listing. Right-click the OU you want to delete, select **Properties**, and in the Object tab (which, like other tabs, is not visible without Advanced Features selected), remove the check in the box next to Protect Object from Accidental Deletion. Now, the OU will be able to be deleted. How that is done will be coming up later. If you did turn on Advanced Features, turn it off at this point.

d) In the same fashion, and also directly underneath the domain name, create these OUs: Brampton, Mississauga, and Waterloo. The order in which the OUs are created does not matter. They will be automatically alphabetized the next time you open Active Directory Users and Computers.

e) Directly inside the TorontoTSW OU (this time, right-click the TorontoTSW OU, mouse over New, and select **Organizational Unit**), create the following second-level OUs: Administrative, Clients, Servers, Users, and Groups.

s

f) Directly inside the Clients OU, create the following third-level OUs: Faculty, Staff, and Students.

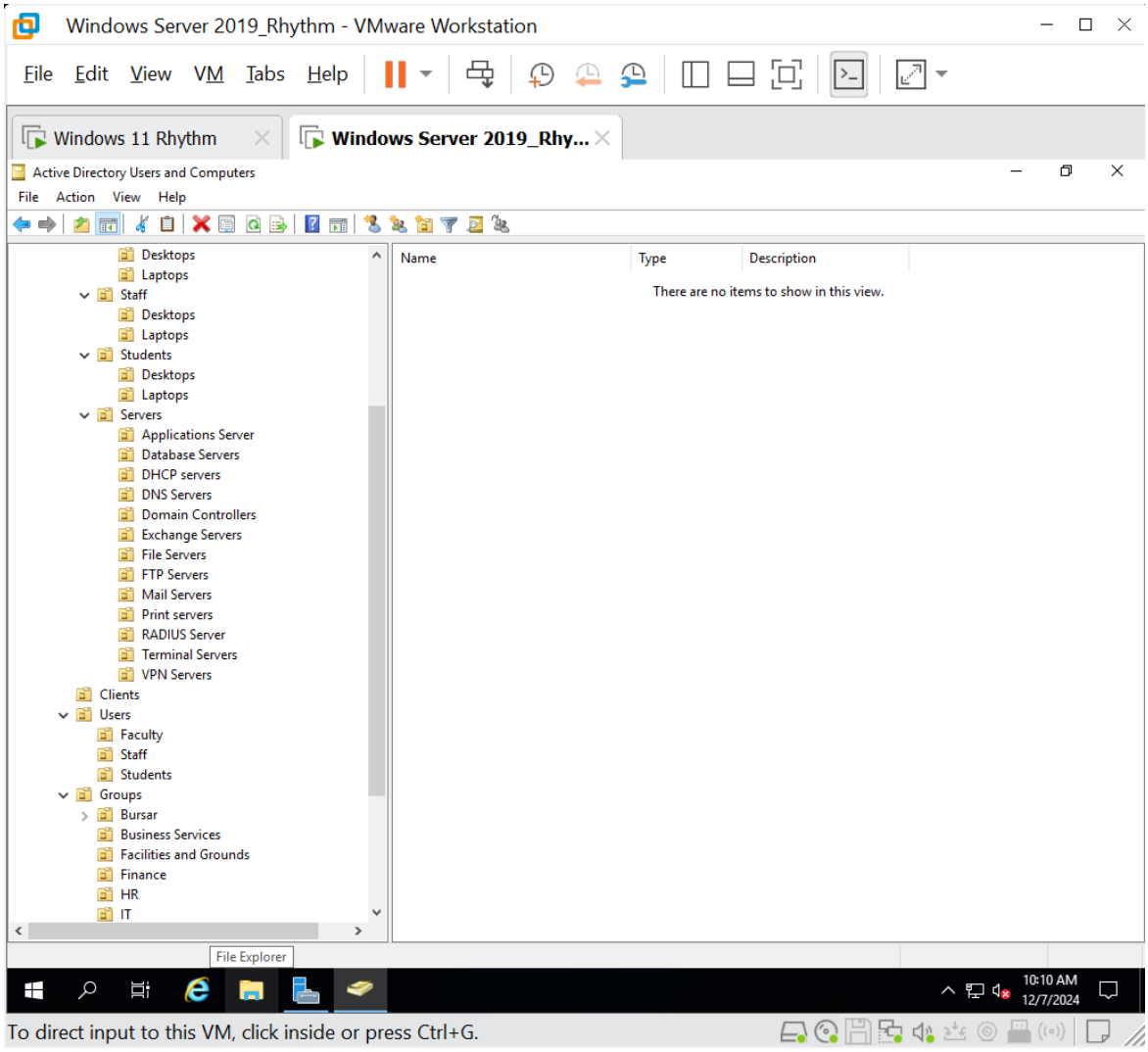
g) Directly inside the Faculty OU, the Students OU, and the Staff OU, create the following fourth-level OUs: Desktops and Laptops.

h) Directly inside the Servers OU, create the following third-level OUs: Application Servers, Database Servers, DHCP Servers, DNS Servers, Domain Controllers, Exchange Servers, File Servers, FTP Servers, Mail Servers, Print Servers, RADIUS Servers, Terminal Servers, and VPN Servers.

i) Directly inside the Users OU, create the following third-level OUs: Faculty, Staff, and Students.

j) Directly inside the Groups OU, create the following third-level OUs: Bursar, Business Services, Facilities and Grounds, Faculty, Finance, Human Resources, Information Technology, Marketing, Registrar, Research and Development, Staff, and Students. The OUs created here will be containers for various groups in each category. For example, Staff Level 1 will not have all the permissions as Staff Level 2.

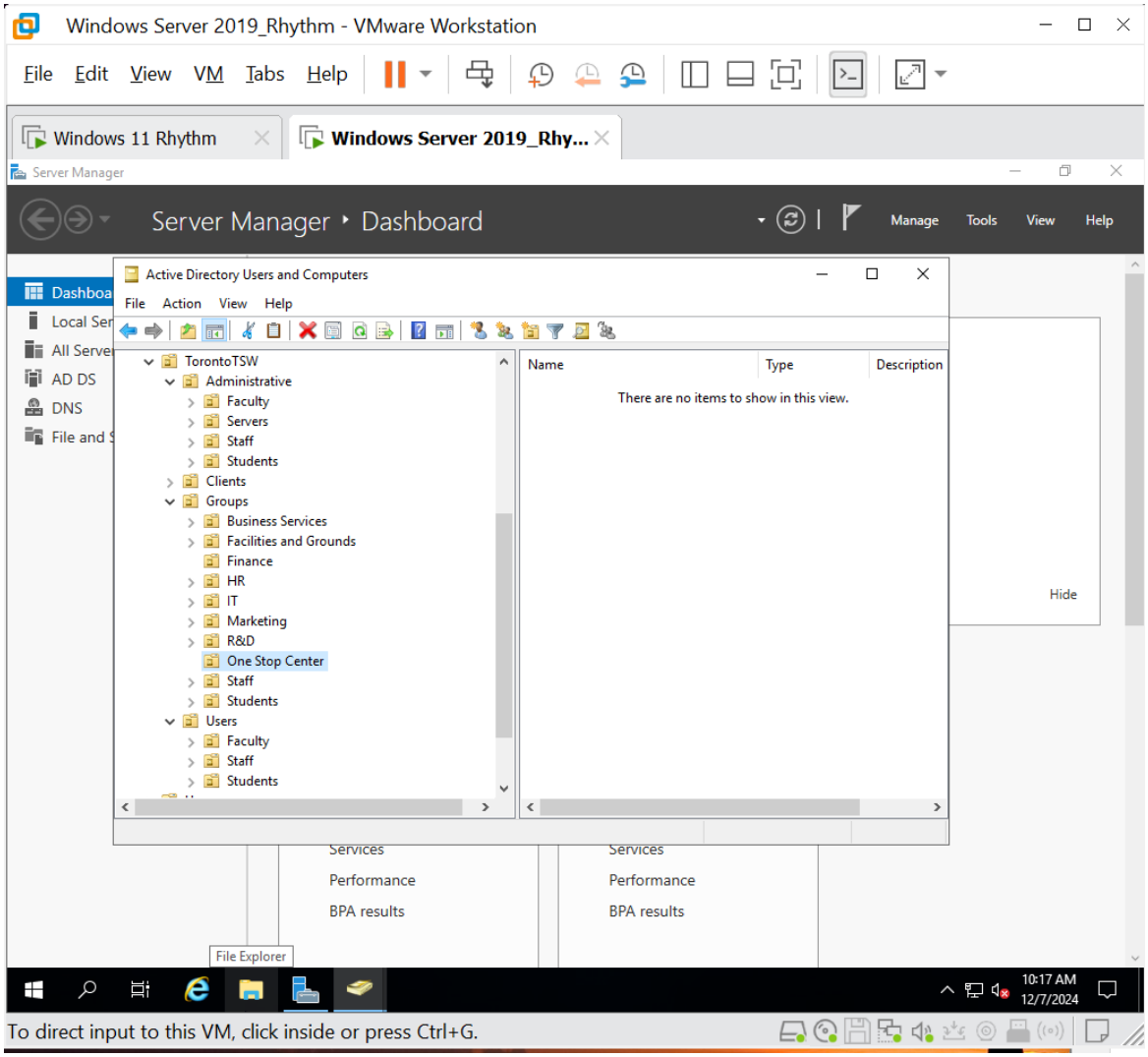
k) Expand all OUs and verify as per the details mentioned in above steps (a to j).



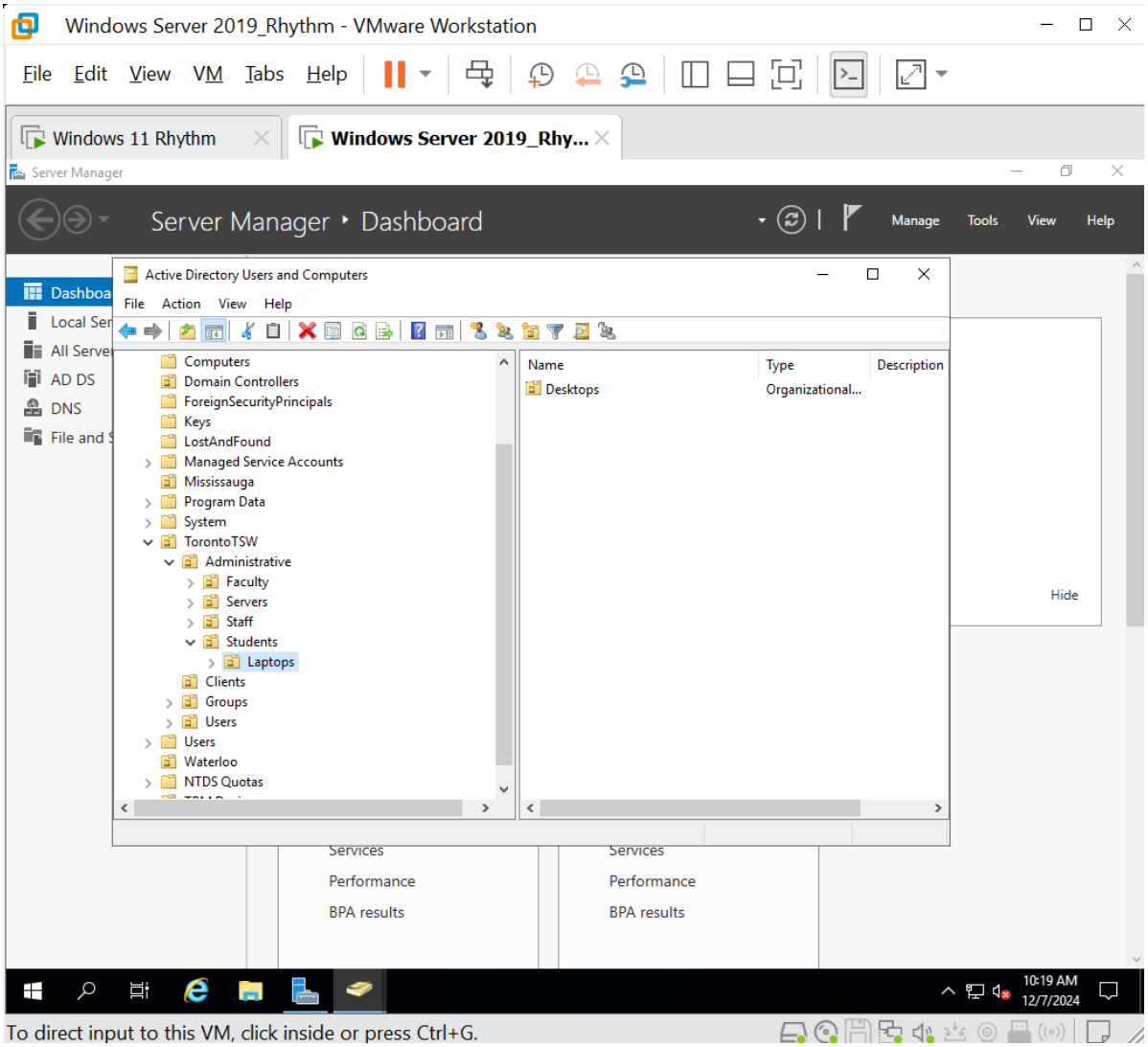
Step 2: Departments, employee roles, resources, and more change over time. The management of networks is challenging enough, but with dynamic changes, it is even more so. The structure of Active Directory, however, allows for structural changes with simple steps. You are about to move, delete, and rename OUs.

a) The Bursar and Registrar departments into the One Stop Center (they actually have). Right-click the **Bursar OU**, select **Delete**, and click the **Yes** button when prompted to confirm you want to delete the OU. Anything inside this OU would have been deleted, as well.

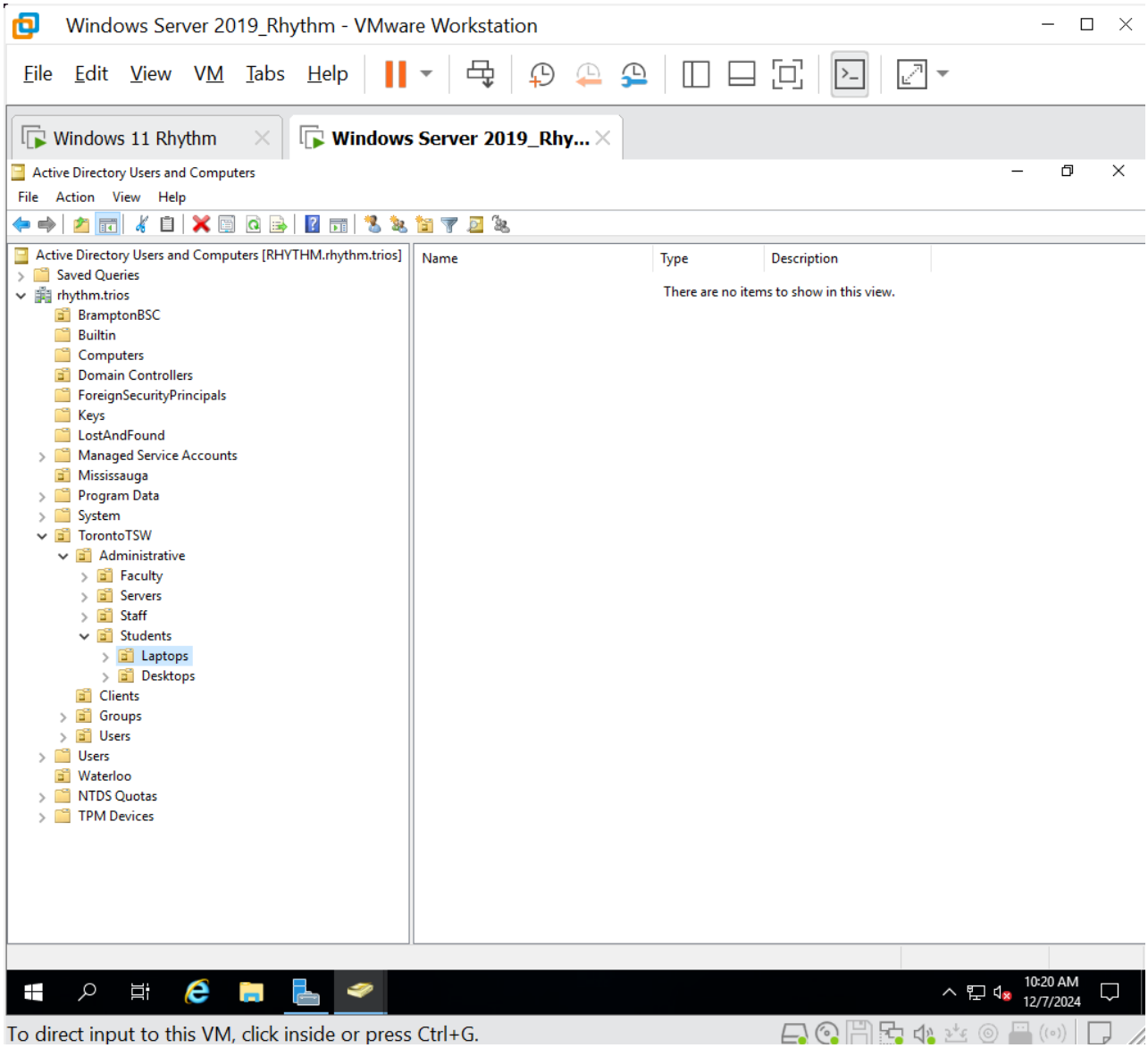
b) Right-click the **Registrar OU**, select **Rename**, type **One Stop Center**, and press **ENTER**.



c) Right-click the computer object for your client machine in the default Computers container, select **Move**..., expand **TorontoTSW**, expand **Clients**, expand **Students**, select **Desktops**, and click the **OK** button.



d) Navigate to the Desktops OU and click the computer object in the right pane. Drag and drop that object into the Laptops OU inside of Students in the left pane. Click the **Yes** button on the popup that warns you about what might happen when you move objects.



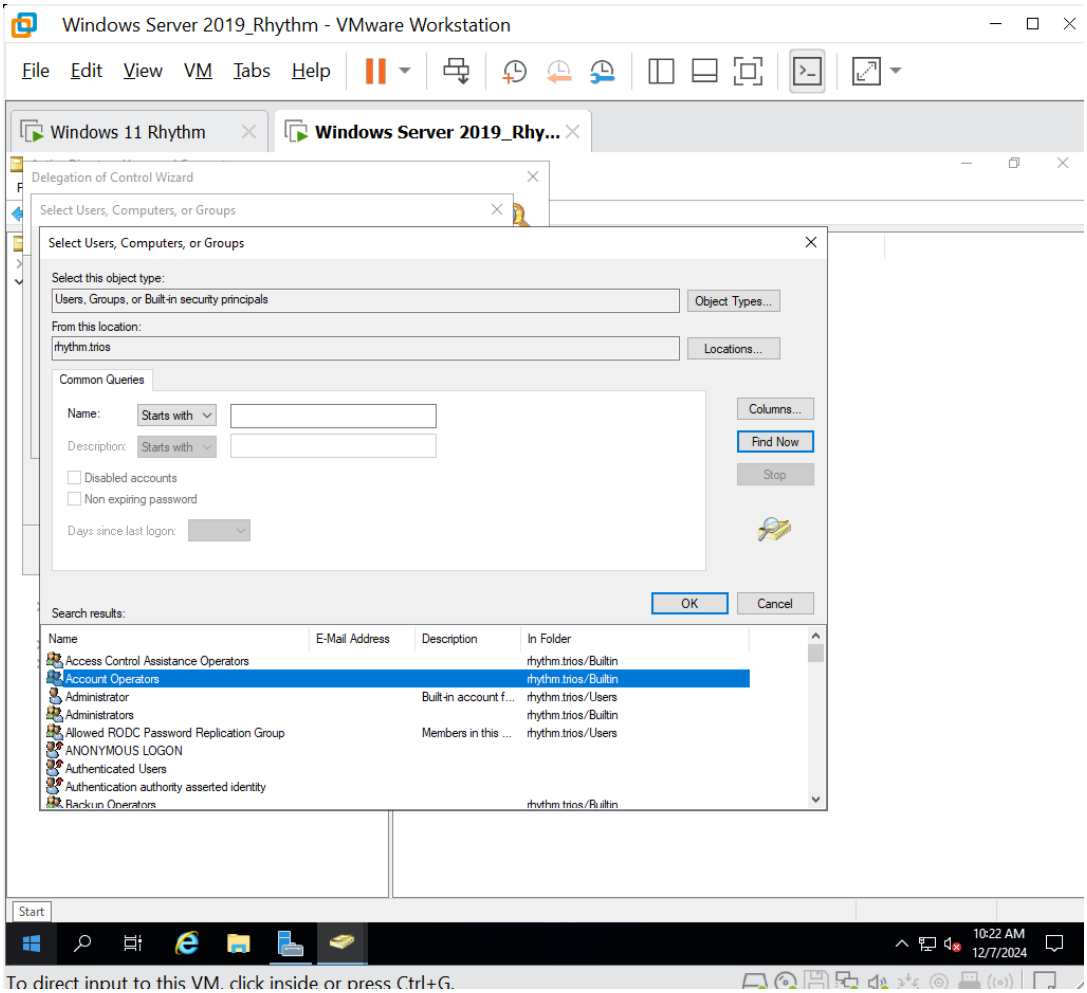
e) Navigate to the Laptops OU and click the computer object in the right pane. Either press **CTRL+X** or right-click the computer object and select Cut. Either click the Desktops OU and press **CTRL+V** or right click and select Paste. Click the **Yes** button on the popup that warns you about what might happen when you move objects. The pasting could have even been done in the right pane, with the proper OU selected. There are many ways to move objects. OUs can be moved in the same way you just moved the computer object.

f) Expand all OUs and select the Desktops OU to display the computer object.

Step 3: Delegating control of OUs could allow large organizations to divide roles and responsibilities between multiple systems administrators. For example, a systems administrator can manage objects in a few domains, all user and group objects, or all file and print services. You will now delegate control.

a) Right-click the Users OU inside the TorontoTSW OU and select **Delegate Control**..., which will start the Delegation of Control Wizard. Click the **Next** button.

b) In the Users or Groups window, click the **Add** button. In the Select Users, Computers, or Groups window, click the **Advancesd** button and then click the **Find Now** button. You will see a list of all users and groups. Double-click the border between the Name and Email Address columns to expand the Name column. Scroll down to see all entries; then scroll up and double-click the second item, **Account Operators**. Click the **OK** button. Click the **Next** button.



c) In the Tasks to Delegate window, with the radio button for Delegate the Following Common Tasks selected, put a check in the box next to the second item, Reset User Passwords and Force Password Change at Next Logon.

d) Click the **Next** button.

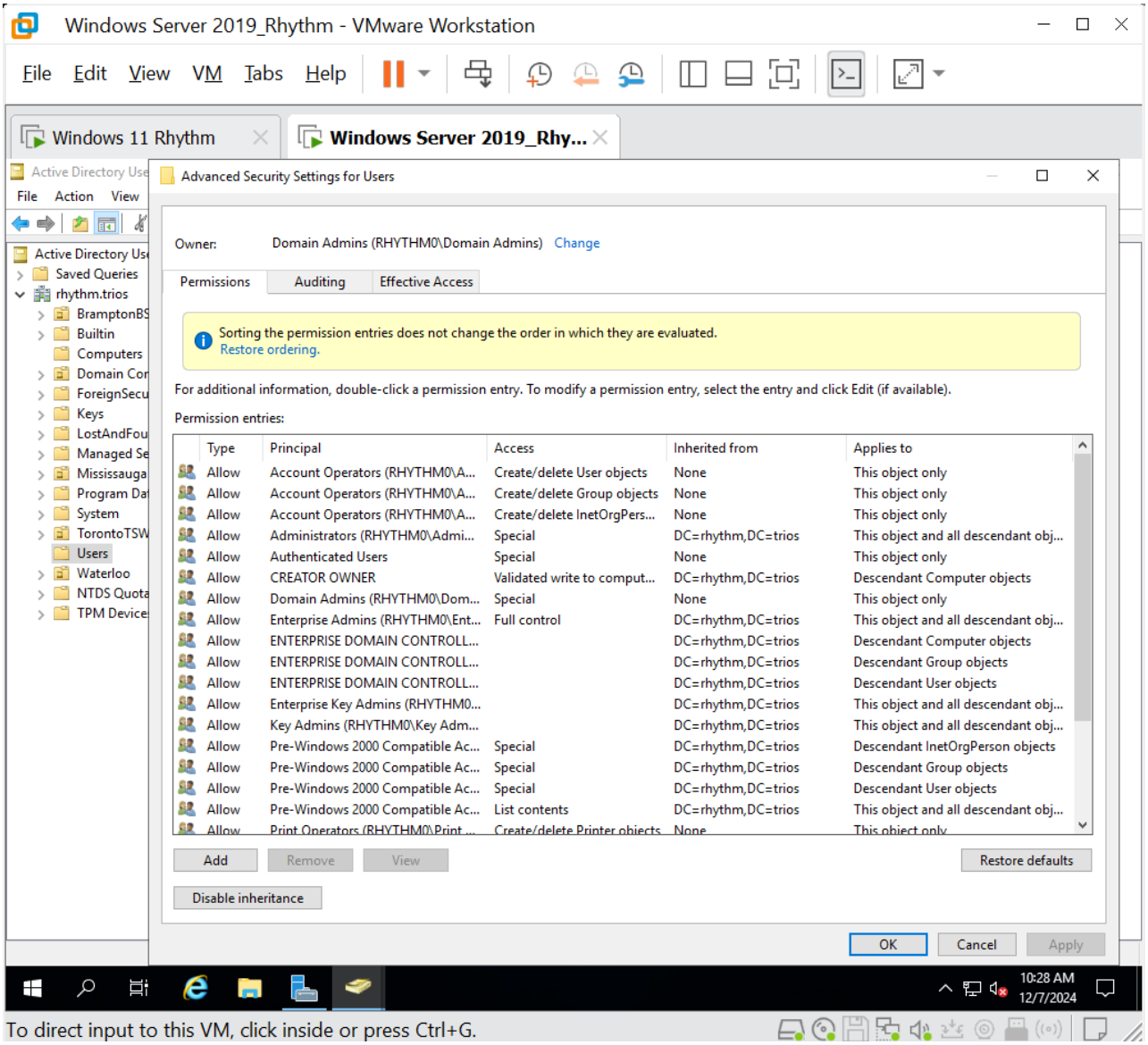
e) Click the **Finish** button.

f) Select the built-in container and double-click **Account Operators**. Notice the description of this group: Members can administer domain user and group accounts. Close the window with either the X button in the top right, the **OK** button, or the Cancel button.

g) Click **View** on the menu bar and select Advanced Features (a toggle selection, as discussed in the previous lab exercise). If you click **View** again, you will see a check next to Advanced Features, which means it is enabled. Do not select Advanced Features again, as that will toggle it off. There are more items in the Active Directory Users and Computers window now.

h) Right-click the **Users OU** inside the TorontoTSW OU, select **Properties**, select the **Security** tab (which would not be visible if Advanced Features was not toggled on), and click the **Advanced** button.

i) The columns are sortable if you click the column header. Click the **Principal** column. Click it again to sort by reverse alphabetical order. Click it once more to order the items in alphabetical order. **Take the screenshot.**



j) Notice that the first six entries have Account Operators as the Principal. Even though in

Step 3c you did not select Create/Delete InetOrgPerson Objects, Create/Delete Computer Objects, Create/Delete Group Objects, or Create/Delete User Objects in the Delegation of Control Wizard, members of the Account Operators group have these permissions by default. However, members of the Account Operators group were not able to change passwords, until you delegated that to them.

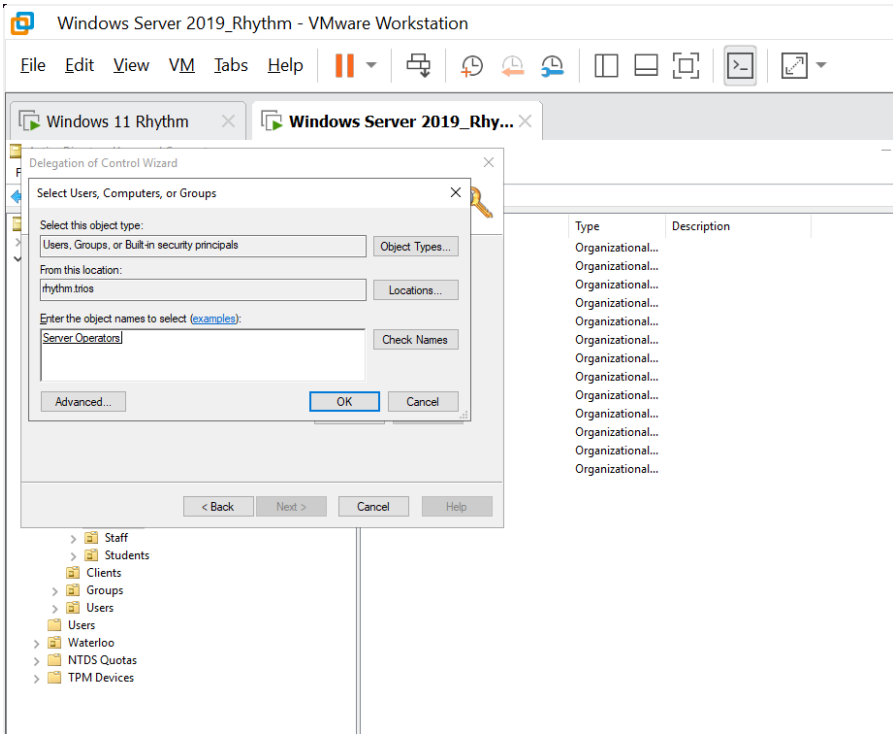
In addition to being able to modify accounts and groups in the domain, as shown previously, members of the Account Operators group can sign into Domain Controllers through a Default Domain Controllers Policy GPO. Members of this group cannot directly modify any AD administrative-related groups, but can join administrative groups through associated privileges.

Due to the default and over-delegated permissions inherent to the Account Operators group (as well as the other Built-in groups), it is a best practice to actually avoid using it. Creating a new group that has nothing by default, and then assigning permissions, following the principle of least privilege, is a better option. You could make a new group and just grant the permission of reset passwords and force password changes to members, without giving them anything more.

Step 4: Now you will perform a more granular type of delegation.

a) Right-click the **Servers OU** inside the TorontoTSW OU and select **Delegate Control**…, which will start the Delegation of Control Wizard. Click the **Next** button.

b) In the Users or Groups window, click the **Add** button. In the Select Users, Computers, or Groups window, type server in the textbox and click the **Check Names** button, which will autocomplete your entry to Server Operators.



Through a GPO linked to the Domain Controllers OU, Server Operators are given permissions to sign in locally to DCs, back up files and directories, force a shutdown of the DC from a remote system, restore files and directories, and shut down the system. As such, this is another example of avoiding the Built-in groups and adhering to the principle of least privilege with your own manually created and delegated groups. You will create your own groups shortly.

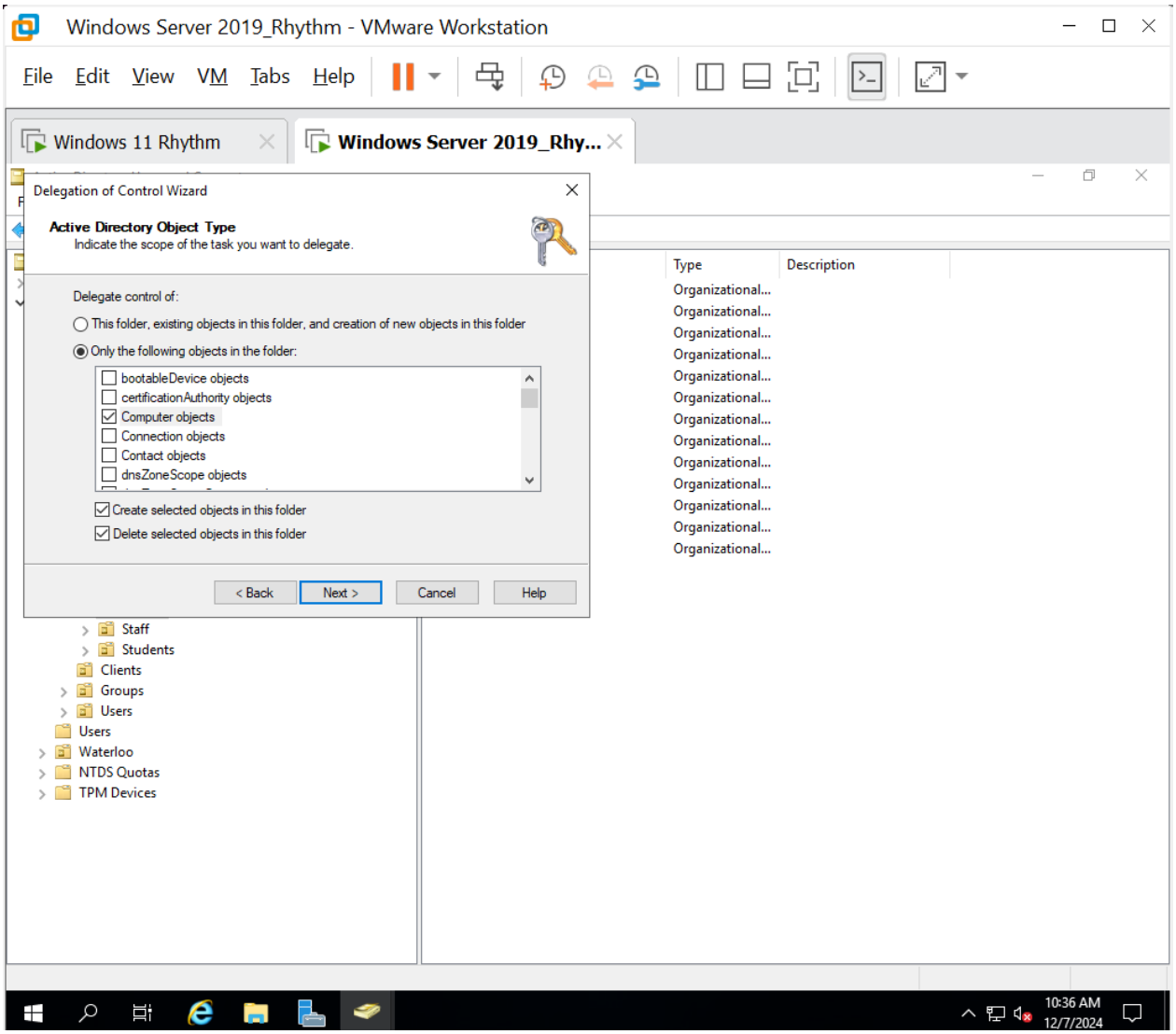
Click the **OK** button. Click the **Next** button.

a) In the Tasks to Delegate window, select the radio button next **to Create a Custom Task to Delegate** and then click the **Next** button.

b) Click the radio button next to Only the Following Objects in the Folder.

c) Put a check in the box next to Computer Objects.

d) Put checks in the boxes underneath the selection window marked Create Selected Objects in This Folder and Delete Selected Objects in This Folder.

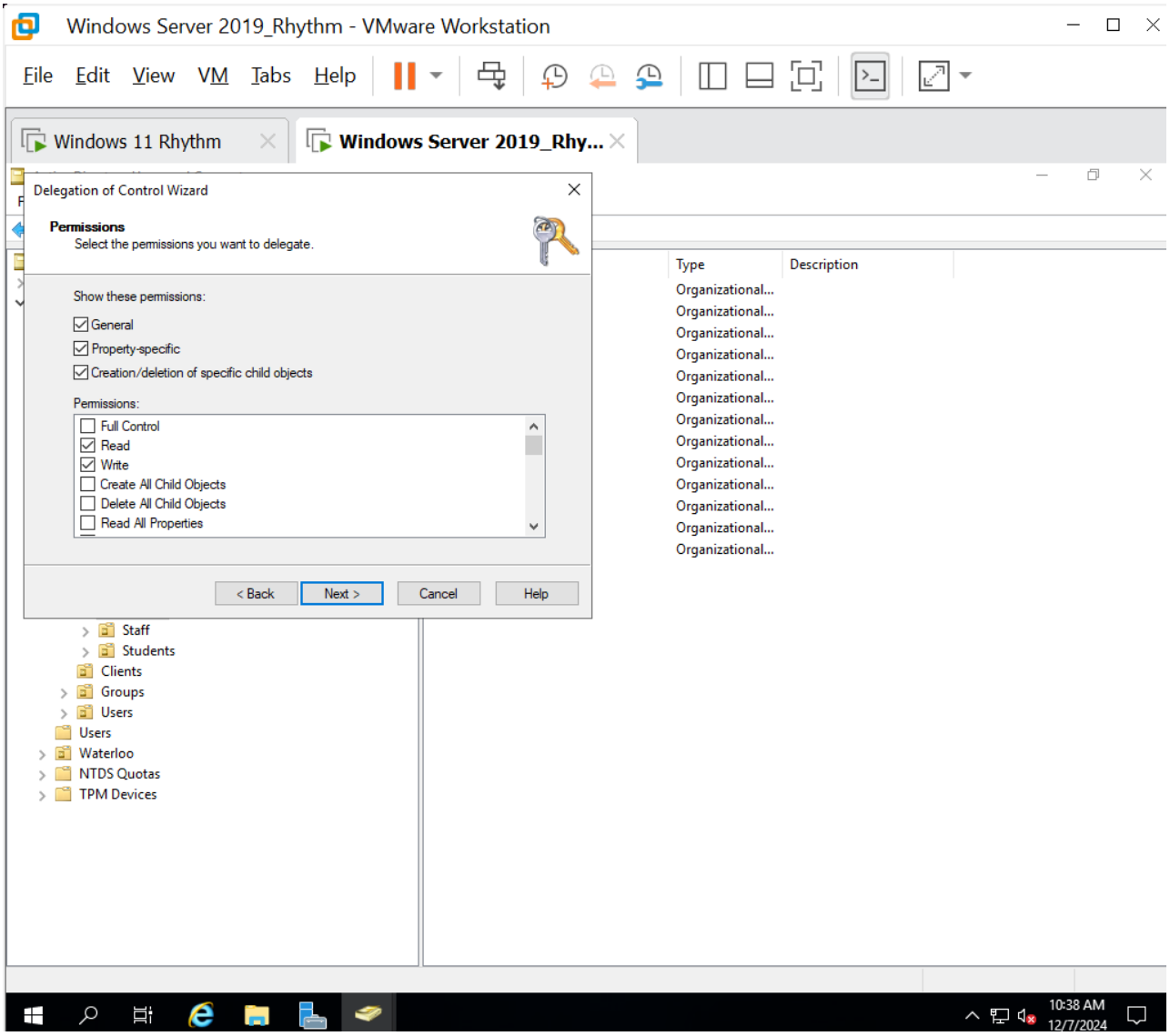


e) Click the **Next** button.

f) In the Permissions screen, with the box next to General checked, scroll through the

permissions in the window below. Do the same by checking just Property-Specific and then Creation/Deletion of Specific Child Objects.

g) Put a checkmark next to the General option, and make sure the other options are not checked. Put a check in the boxes next to Read and Write (which will trigger a check in the box next to Property-Specific). Scroll down to see all the additional checks that were added to specific permissions.



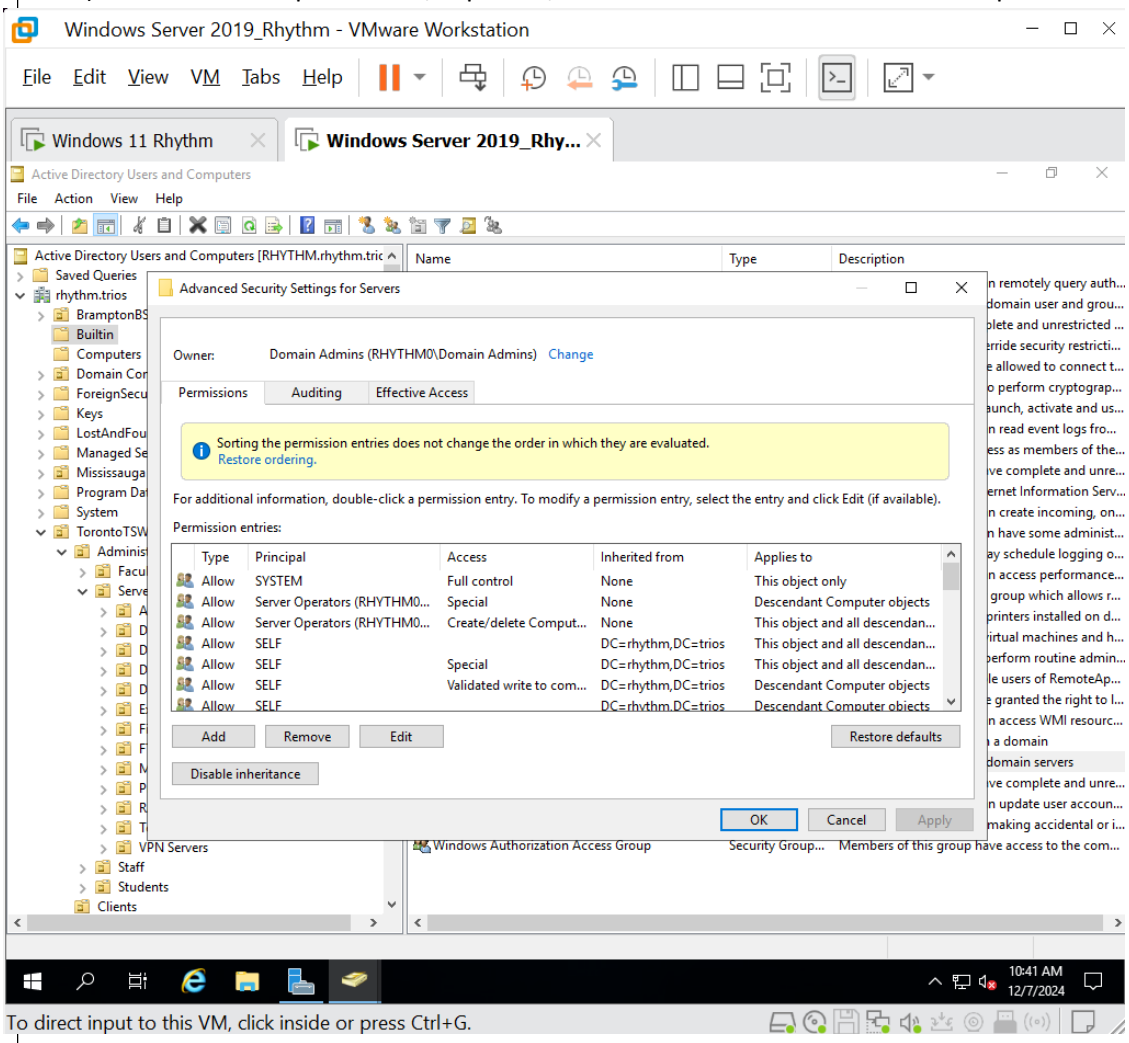
h) Click the **Next** button. Click the **Finish** button. This gives the members of the Server Operators group the ability to create new Computer objects within the Servers OU and the permissions to read and write all properties for Computer objects.

i) Select the **Built-in** container and double-click **Server Operators**. Notice the description of this group: Members can administer domain servers. Close the window with either the X button in the top right, the **OK** button, or the Cancel button. As mentioned in regard to Account Operators, it is probably best to not use the Server Operators group, with its over-delegated permissions.

j) Right-click the **Servers OU** inside the TorontoTSW OU, select **Properties**, select the **Security**

k) tab, and click the **Advanced** button.

l) Sort the Principal column, expand it, and examine the entries for Server Operators.



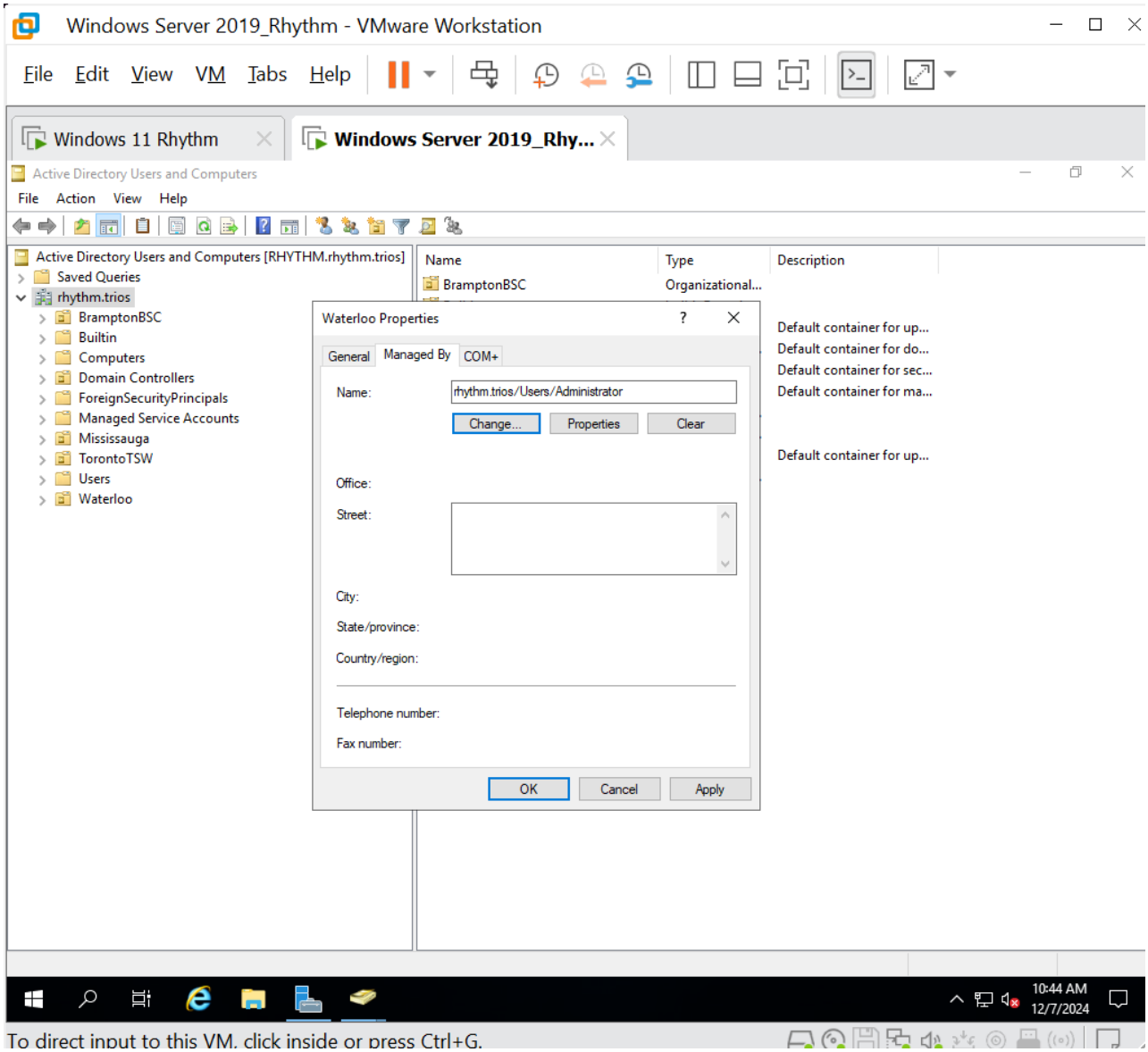
m) Toggle the Advanced Features off through the View menu bar item.

Step 5: Properties of OUs can be helpful in identifying items like the user responsible for managing an OU. Contact information is important for systems administrators in case they need to contact the person in charge of an OU. Configuring contact information does not grant permissions, like delegation does, and is merely cosmetic. Now, you will configure contact information.

a) Right-click the **Waterloo OU** (directly off the domain), select **Properties**, and click the **Managed By** tab.

b) Click the **Change…** button, click the **Advanced** button, click the **Find Now** button, and double-click the **Administrator** account. Click the **OK** button.

c) If there was additional information about the account, it would automatically populate in the respective sections (Office, Street, City, State/Province, Country/Region, Telephone Number, and Fax Number). **Take the screenshot.**



d) Click the **OK** button to close the Waterloo Properties dialog box.s

Step 6: There are two group types in Active Directory: security groups and distribution groups.

Security groups are granted (or denied) permissions to resources. For example, if you want to give a group of users access to an object, like a shared folder, but specify their level of control, create a security group, and then assign the permissions to the group. Then each user in the group gets those permissions. You can also send email to security groups. All users in a group would receive the email if a mail system that allows for mail-enabled groups, like Microsoft Exchange, is configured.

Distribution groups are strictly used for telephone lists and email lists if a mail system that allows for mail-enabled groups, like Microsoft Exchange, is configured. However, distribution groups never receive permissions for objects. They are just used for providing mass distribution of information in a quick fashion.

Security groups can be broken down further into three different types.

A local security group manages resources on a computer that is not part of a domain, and it is not considered one of the three types of domain security groups.

The first security group is known as a domain local group, which stays in the domain in which it was created. This group is used for granting permission to objects such as servers, folders, shared folders, and printers in a single domain. A domain local group cannot be used in any other domain and must be located in the domain in which it was created.

The second security group is known as a global group, which can contain other groups and accounts from the domain in which the group is created. This group can be given permissions in any domain in a forest. A domain local group is used to manage resources in a domain and to give global groups, from the same domain and different domains, access to resources. If you add user accounts that need access to resources, in the same domain as the global group or another domain to the global group, and then add that

global group to domain local groups, which would be a great administrative move.

Imagine a company's AD forest has a domain for the New York headquarters, a domain for a branch office in Texas, and a domain for a branch office in California. The company's board of trustees needs to be able to access the resources in all three of the domains. You can create a domain local group in each domain, which grants access to the resources needed by the board of trustees' members. Then you can create a global group in the New York headquarters domain that has the board of trustees' members as user account members. Then you can add the global group to each domain's domain local group. If a board of trustees' member leaves, you simply disable that account. If a new user joins the board of trustees, add that user's account to the global group. If new resources are added, add permissions for those to the domain local group.

The third security group is known as a universal group, which can contain other groups and accounts from any domain in the forest. A universal group can be given permissions in any domain in a forest. You can add user accounts that need access to resources in multiple (or all) domains to a global group and then add that global group to a single universal group, instead of a domain local group for each domain. This way, you can make one universal group that has access to resources in all three domains needed by the board of trustees' members—one global group that has the user accounts of the board of trustees' members—and make that global group a member of the universal group. Now you only have to manage two groups instead of four.

Universal groups can have members from any domain, and permissions can be set for any domain object. Universal groups are actually stored in the global catalog. When changes are made to a universal group, all changed properties need to be replicated to the other DCs that are global catalog servers. Since only property changes are replicated, instead of objects, there are no worries of a network bottleneck or latency.

The general guidelines are to use global groups to contain user accounts as members, use domain local groups to grant access to a specific domain's resources, and to use universal groups to provide forest-wide (multiple domains) widespread access to resources.

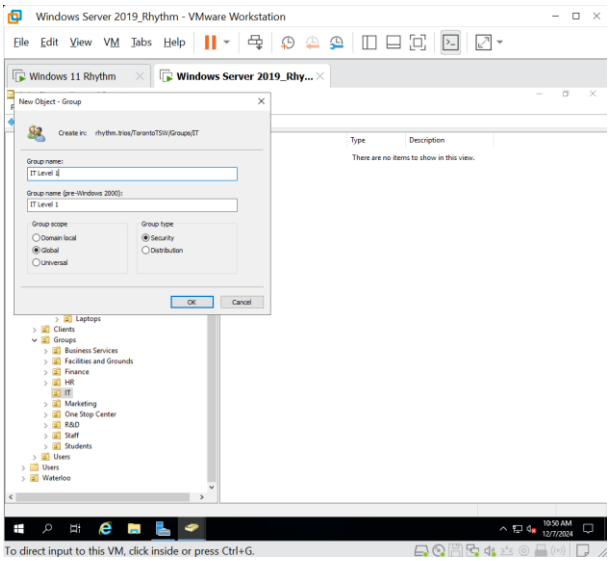
The Microsoft acronym AGDLP, for role-based access controls, is helpful for remembering how to set up groups. First, create user accounts (A). Next, put the user accounts into global groups (G). Then, put global groups into domain local groups (DL). Finally, assign permissions (P) for resources to the domain local groups.

Alternatively, the Microsoft acronym AGUDLP (also for role-based access controls) can be used. First, create user accounts (A). Next, put the user accounts into global groups (G). Then, put the global groups into universal groups (U). Then, put universal groups into domain local groups (DL). Finally, assign permissions (P) for resources to the domain local groups.

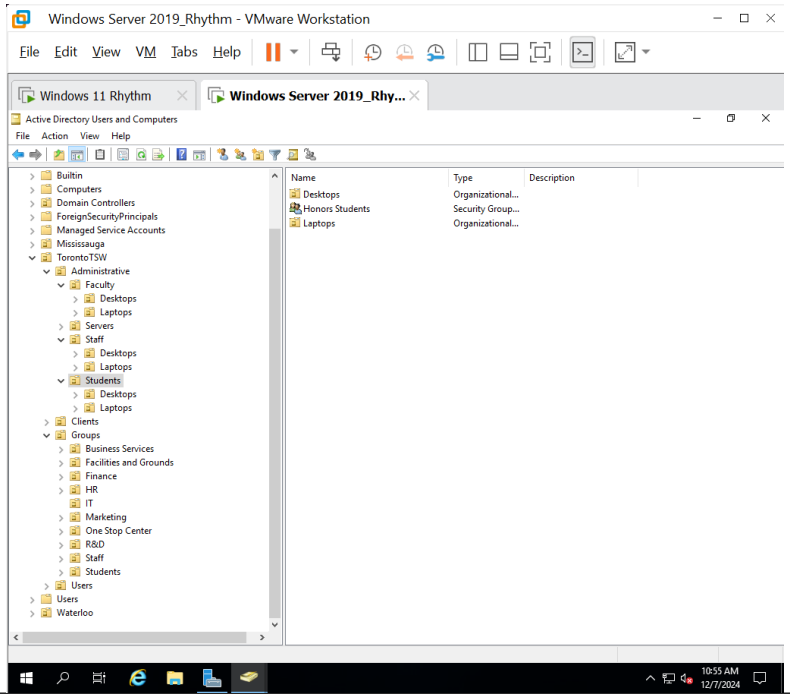
In our board of trustees' example, an alternative of assigning specific permissions to specific resources was done to the universal group instead of a domain local group.

Now, you will create groups:

a) Click the **Information Technology OU** in the Groups OU in the TorontoTSW OU. Right-click a blank area in the right pane, mouse over **New**, and select **Group**. In the Group Name: textbox, type IT Level 1. Keep the default radio button selection of Global for Group Scope.



b) Click the **Students OU** in the Groups OU in the TorontoTSW OU. In the same fashion, create a domain local group called Honors Students.



c) Click the **Human Resources OU** in the Groups OU in the TorontoTSW OU. In the same fashion, create a universal group called HR Managers. **Take the screenshot showing all the groups created.**