Lab 4: Team Organizational Unit (OU) and Network Management Tools

The objective of the lab is to familiarize you with the Windows Server 2019 management environment and introduce you to the creation and management basic Active Directory (AD) objects, as well as the creation of Active Directory users and groups.

This is a team assignment, but you must submit it as individuals, with all submitted work being your own.

Actions

Action 1: From your fellow classmates, form teams of no more than four members. . Each team has been assigned a Windows Server 2019 instance.

Note: there are twelve (12) Windows Server 2019 instances available for this exercise: one for each four-member team.

For Deliverable #1, write your name, the number of your team, the name of your partners, and the date.

Connect to the CCI Virtual Environment

Action 2: You will find instructions for connecting to the CCI virtual environment in Actions 1 – 3 of Lab 1: *Access Virtual Lab Environment*.

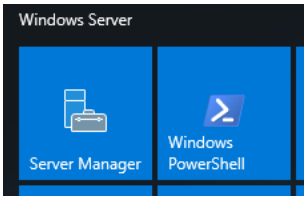
Rather than connecting to your individual Microsoft Windows 10 instances, however, one member of your team will connect to your team's Microsoft Windows Server 2019 instance, as you did in *Lab 3: Server Local User, Group, NTFS Permission, & Share Exercise*, using the TightVNC client on your Windows 10 virtual instance.

Install Active Directory Management Tools

When a Microsoft Windows Server 2019 computer is a Domain Controller, the installation process for Active Directory Services also installs the Active Directory management tools on that server. However, your team's Windows Server 2019 computer – the server to which you are presently connected - is still only a member server, and will not have installed the tools you will need to complete this assignment.

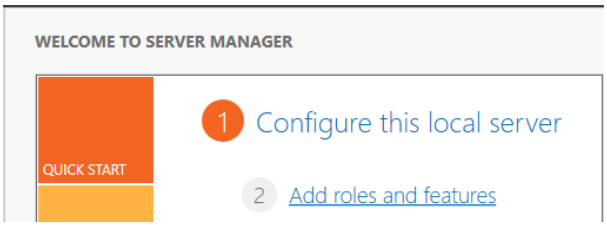
You will now install these tools.

Action 4: From the Start button, select *Server Manager*:

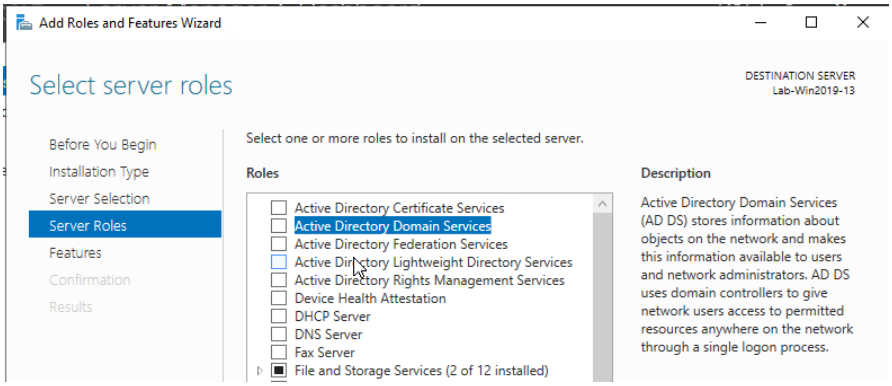


Install Active Directory Management Tools (continued)

In *Server Manager*, select *Add roles and features*:

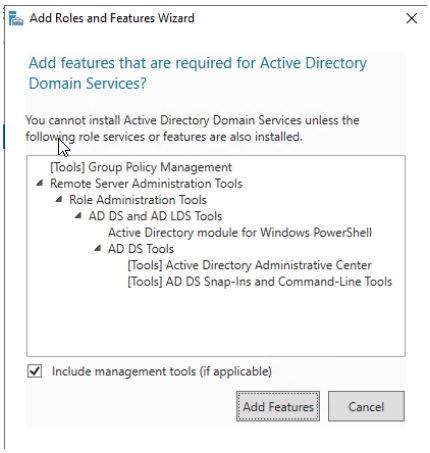


Select Next > until you get to *Select server roles*:



You're going to install *Active Directory Domain Services* – or more specifically, the *tools* for ADDS and the *capability* for this server to become a Domain Controller. You won't be promoting this server to a Domain Controller – certainly not in this lab – but you will need the tools.

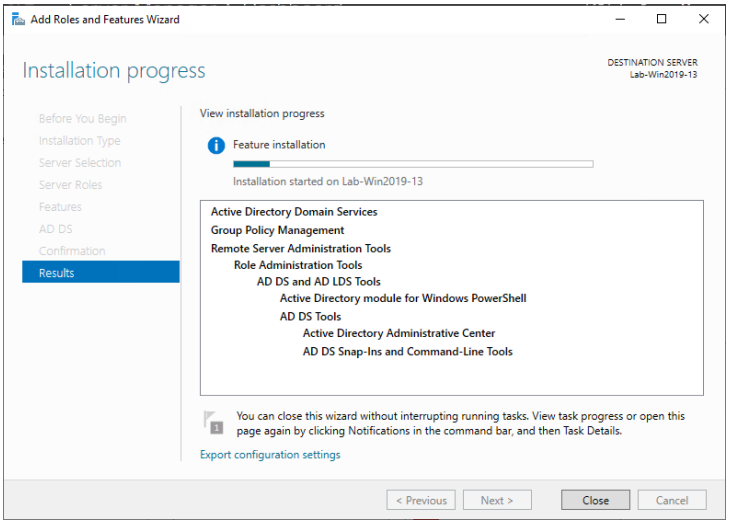
Check *Active Directory Domain Services* to install the capabilities and the tools:



Click *Add Features*. Click Next > until you get to *Confirm Installation Selections*, and then click Install.

Make a mental note of the messages that appear while moving forward to the final installation page.

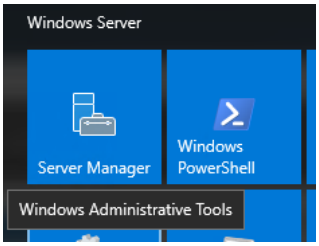
Install Active Directory Management Tools (continued)



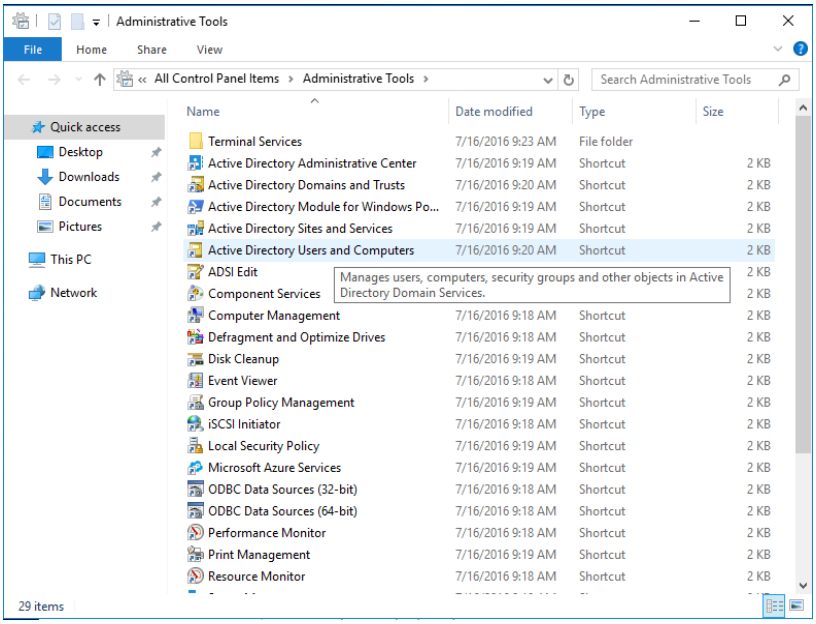
When the installation process completes, close the wizard.

DO **NOT** PROMOTE THIS SERVER TO A DOMAIN CONTROLLER AT THIS TIME.

You may access these newly installed tools via *Start* button → *Windows Administrative Tools*.

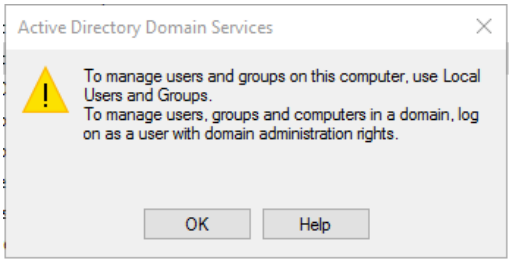


Click Windows *Administrative Tools*. You will see a wide variety of tools not present when this server was in standalone mode. You will be using *Active Directory Users and Computers* quite a bit in this course. Select and open it.

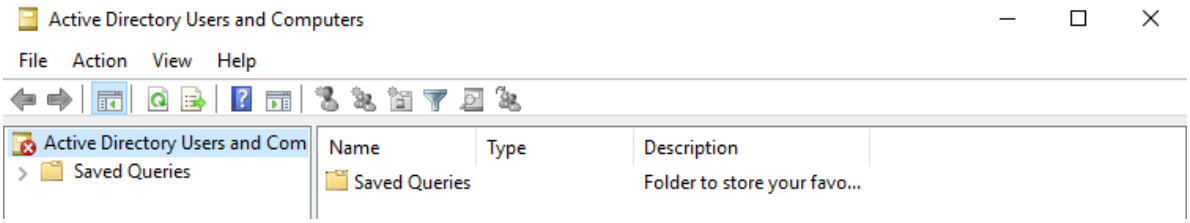


Install Active Directory Management Tools (continued)

Remember that this server is only a standalone server: it has only local users and groups, so there are no Active Directory users or groups for the tool to manage, and the tool warns you of this:

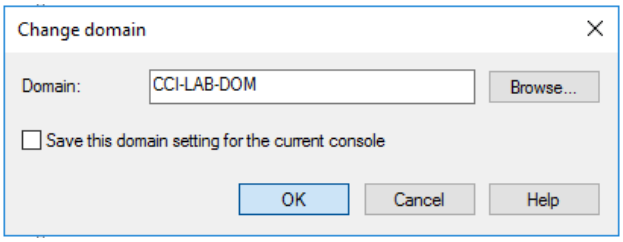


Click *OK*.



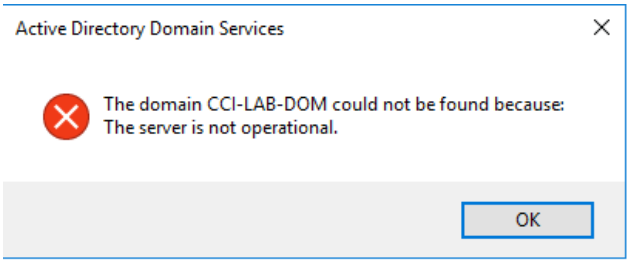
You will see a red X indicating that this tool is not yet usable.

You could Change Domain so that you could attach the tool to a Domain in which Active Directory users and Active Directory groups actually exist (see below)…



… except that there's nowhere to enter credentials. Click *Cancel*.

Had you not clicked *Cancel*, you would have eventually received the message below:



This Domain has no knowledge of your standalone Windows Server 2019 computer, and vice-versa.

For Deliverable #2, why isn't your *Active Directory Users and Computers* tool working?

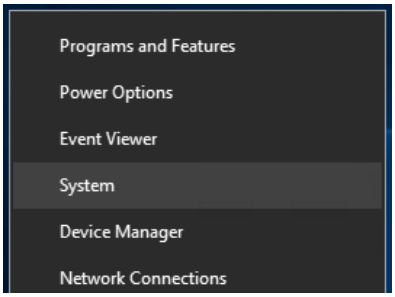
You'll have to remedy this:

Join Your Windows Server 2019 Server to the Root Domain

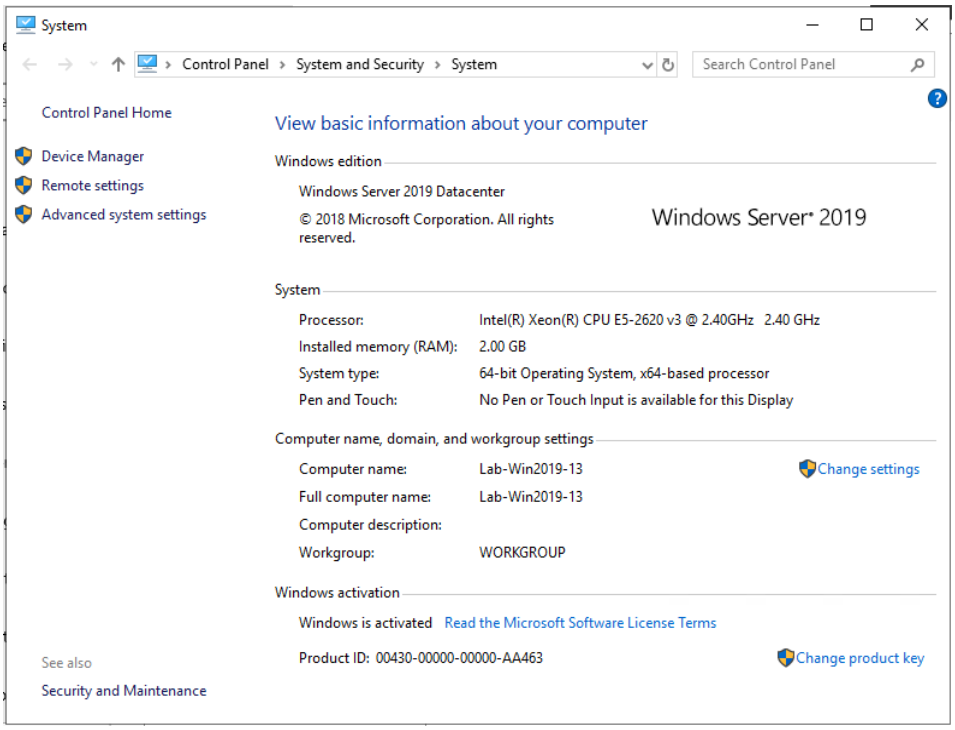
Action 5: Close *Active Directory Users and Computers*, if it is still open.

To participate in the full benefits of a Domain, a computer must be a member of it.

Right-click the *Star*t button, and then click *System*, and then *System Info*:

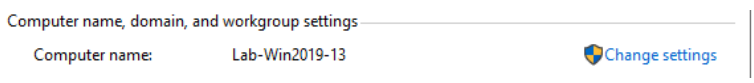


Pay attention to these steps, as this is very much how you will be joining your Windows 10 computers to the Microsoft Domain in the next lab.



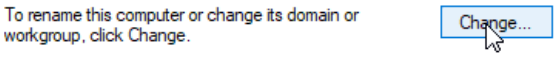
Note: remember the warning in the last lab to be mindful of where you are, i.e. that you're using your personal device to RDP to your Windows 10 virtual lab workstation, and in turn using TightVNC to connect to you team Windows Server 2019 instance. If the screen above is not Windows Server 2019, then you're in the wrong window.

Click *Change Settings*.



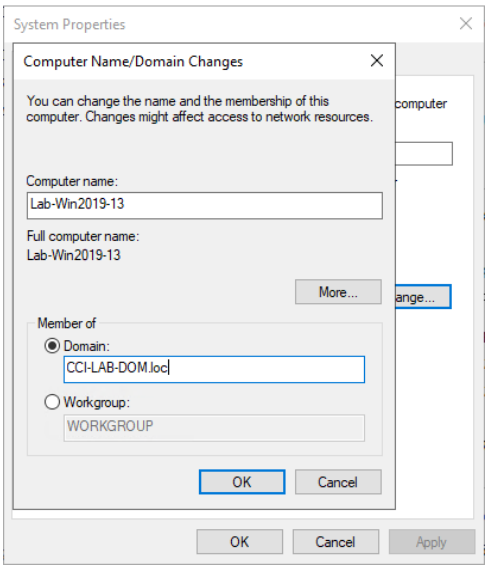
Join Your Windows Server 2019 Server to the Root Domain (continued)

You're going to change this computer's Domain, so click *Change*.

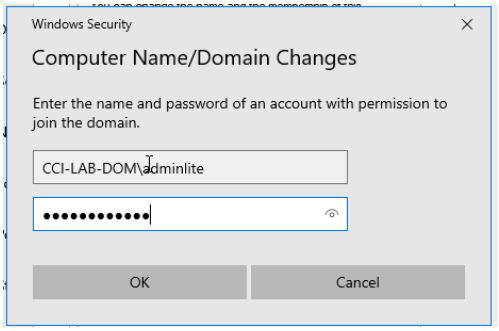


Click the bubble for *Domain*, and then enter the name of the course root Domain: CCI-LAB-DOM

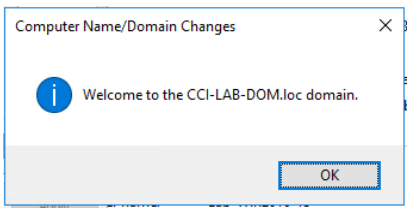
Click *OK*.

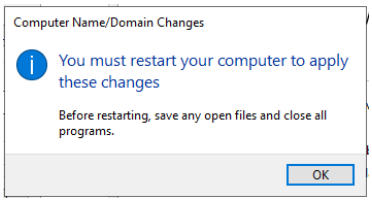


Enter the *full* username of an account with permission to join computers to the root Domain for course, and its password, and click *OK*. For this course, that username is CCI-LAB-DOM\AdminLite. The password will be given to you in class.



Upon successful joining to the Domain, click *Restart Now* to restart your instance. You may have to reconnect.



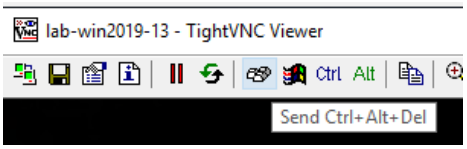


Note: you will have to reconnect your workstations' TightVNC client back to your team Windows Server 2019 after it reboots, as it will drop the TightVNC connection.

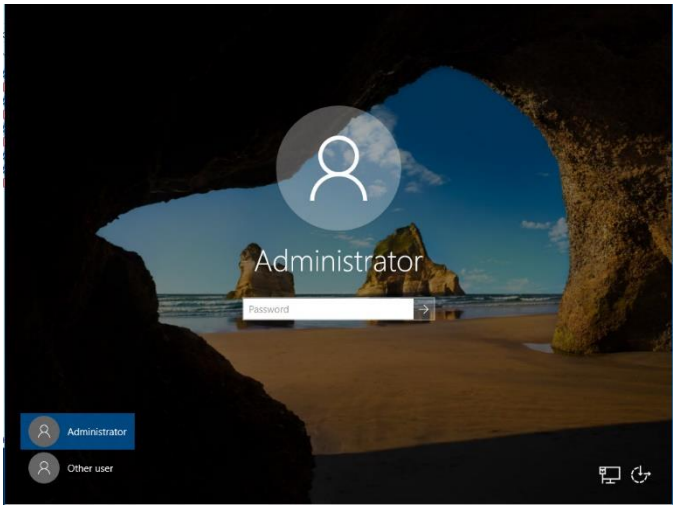
Confirm the Joining of Your Windows Server 2019 Server to the Root Domain

Action 7: Once your Windows Server 2019 computer instance is rebooted, log into it. Review the directions of Action 3 if you require assistance.

For the one team member you have log back into Windows Server 2019: don't forget to send a ctrl-alt-del:



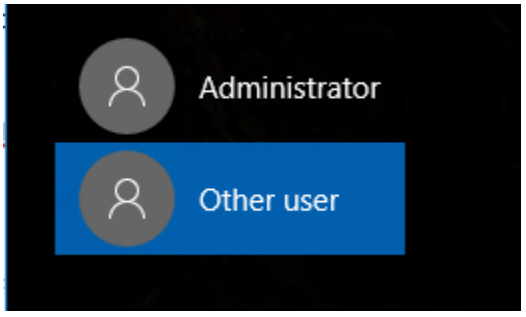
By default, the login screen will default to have you log in under the local account you had used prior to joining this machine to the Domain:



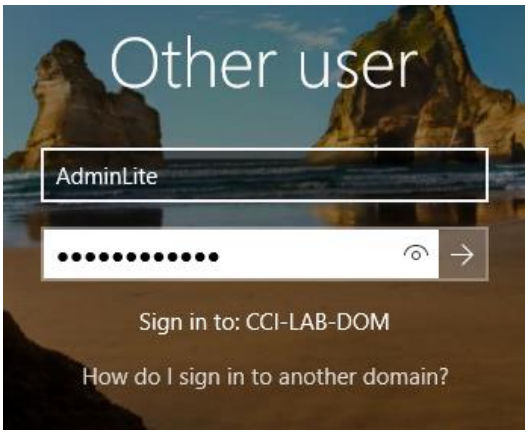
This is incorrect: to complete this exercise – and use the Domain management tool you installed previously - you need to log in as a Domain user, and using a Domain user account with the permissions necessary to create the things you need to create in the next few actions.

An account named AdminLite has been created to perform basic Active Directory management tasks. Log into your server using this account.

Sign on with *Other user*



using the AdminLite credentials:

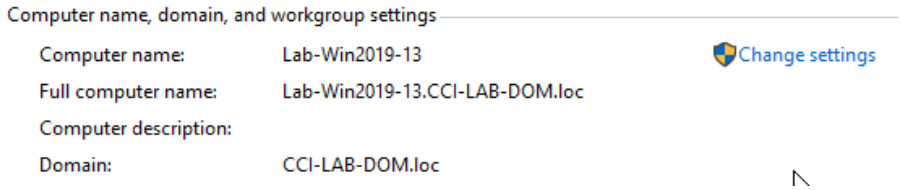


The simple act of being able to log in using a Domain account should confirm that you have successfully joined this server to a Domain, and that it is now a Domain member. However, you may confirm this with

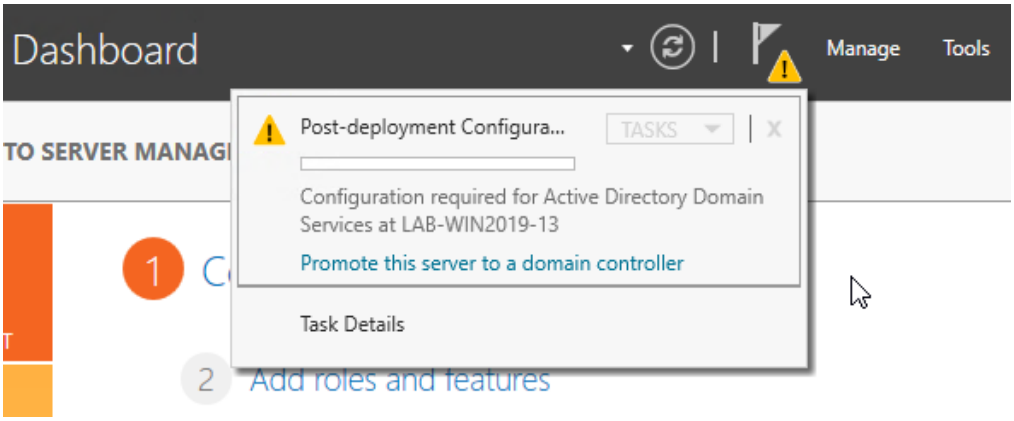
Confirm the Joining of Your Windows Server 2019 Server to the Root Domain (continued)

Right-click *Start* button → *System* → *System Info*.

Note that you would see a similar screen for the root Domain Controller:



In other words, all you can really tell from this screen is that this computer participates as part of a Domain. Whether it's an actual Domain Controller or just a Domain member really can't be proven from this screen. The Server Manager, however, reveals that Active Directory Domain Services (AS DS) isn't active on this server:



Clicking the flag will produce the screen above.

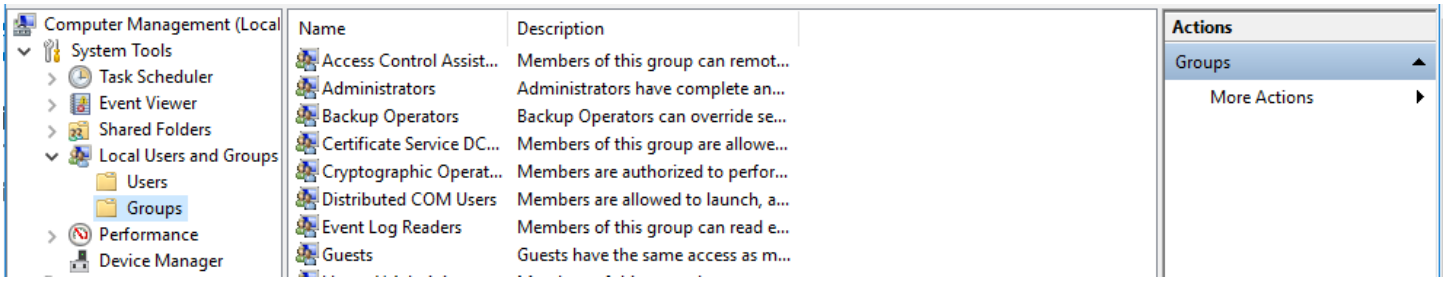
DO NOT PROMOTE THIS SERVER TO A DOMAIN CONTROLLER.

For Deliverable #4, in which mode is your team server presently operating: stand-alone, member, or Domain controller?

Let's see what else changed when you joined your team server to a Domain.

Right-click *Start* button → *Computer Management* tool.

You'll remember this as the tool in which you created *local* users and groups in the previous lab. Using this tool, checks the membership of the *local* Administrators group:



For Deliverable #5, what new members have appeared in the local Administrators group? What does this mean?

Close the *Computer Management* tool.

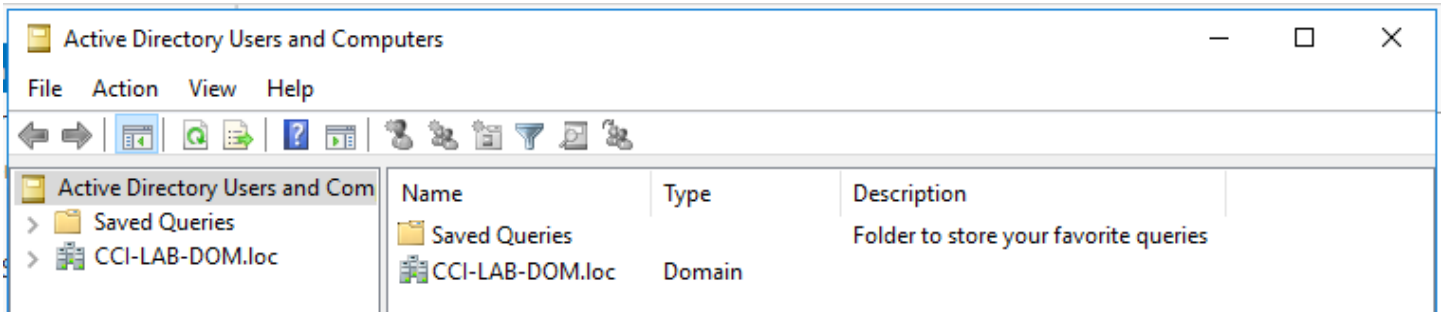
Create a Team Organizational Unit in the Root Domain

Your team will now create for itself an Organizational Unit (OU) that will serve as the context for the next several labs. You will need to use the *Active Directory Users and Computers* tool for this.

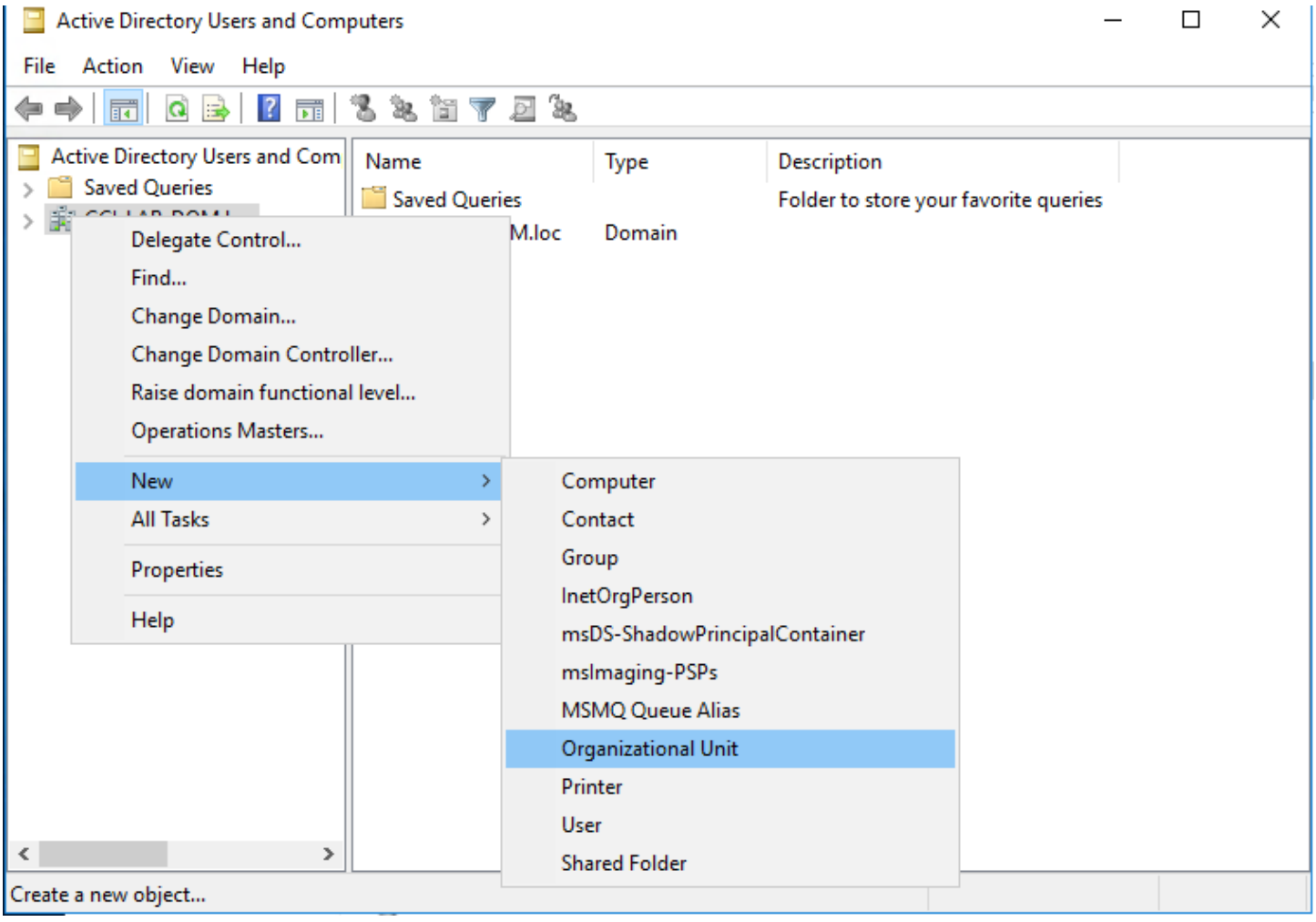
Action 8: From *Start* button → *Windows Administrative Tools*, open the *Active Directory Users and Computers* tool.

By the way, you may also open the *Active Directory Users and Computers* tool by *Start* button → right-click *Run* and then typing *dsa.msc*

Note that the red error X is no longer present: the computer you are using is now a full member of the Domain and can now use Active Directory services.

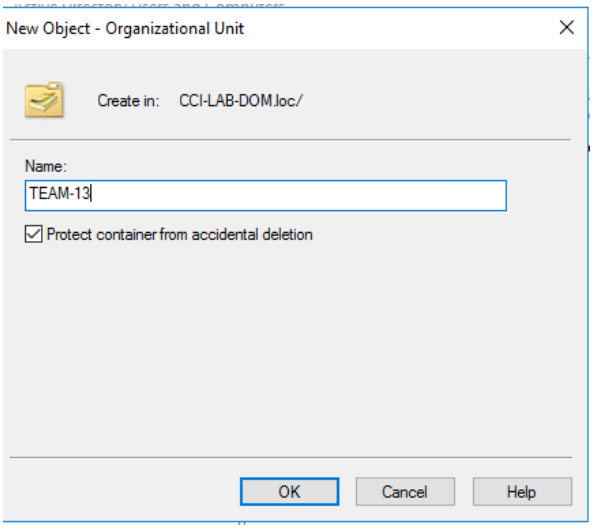


Right-click the Domain for this course it is CCI-LAB-DOM.loc, and then select *New* → *Organizational Unit*.



Create a Team Organizational Unit in the Root Domain (continued)

Have your team decide on an appropriate name and enter it into the box:



Click *OK* to create the Organizational Unit object.

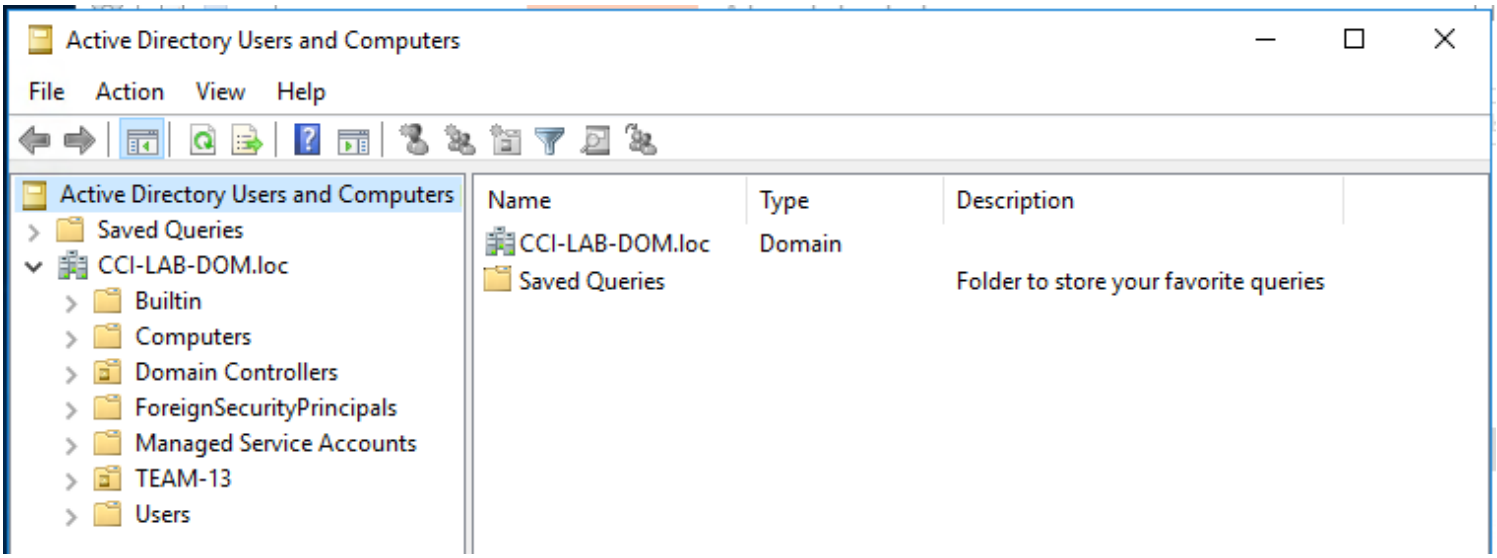
For Deliverable #6, what did your team name its Organizational Unit object?

For Deliverable #7, is this Organizational Unit object a container object or a leaf object?

Create User and Group Objects in Your Team Organizational Unit

Your team will now create for itself a team group in the Organizational Unit (OU) that you just created, and within that OU, also user accounts for your team members. You will continue to use the *Active Directory Users and Computers* tool for this.

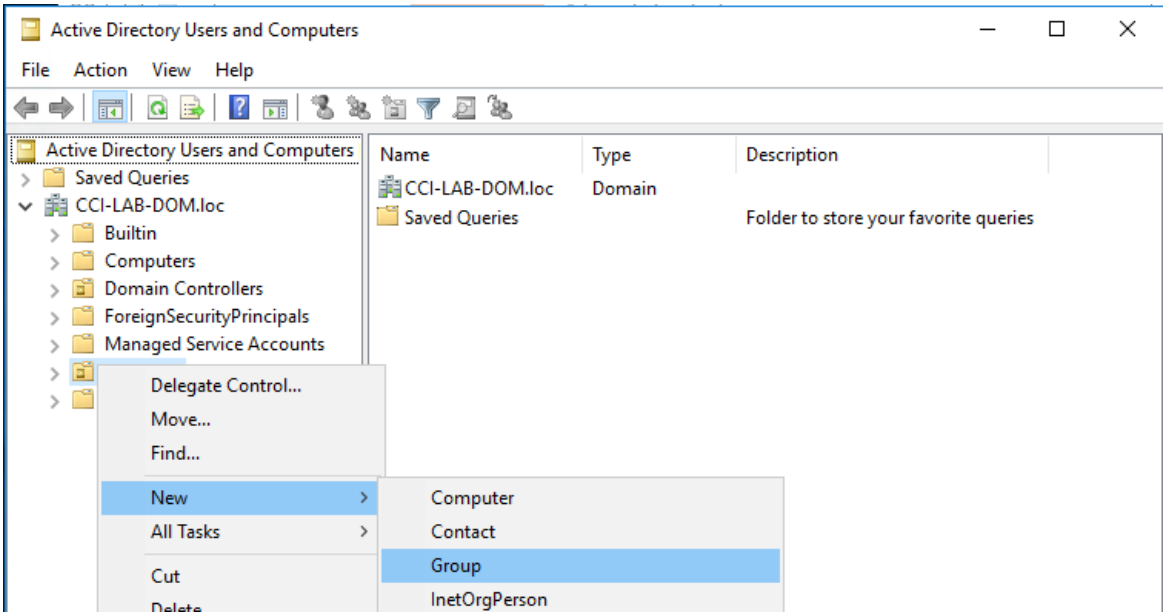
Action 9: Expand the Domain to view all of the containers and objects within it:



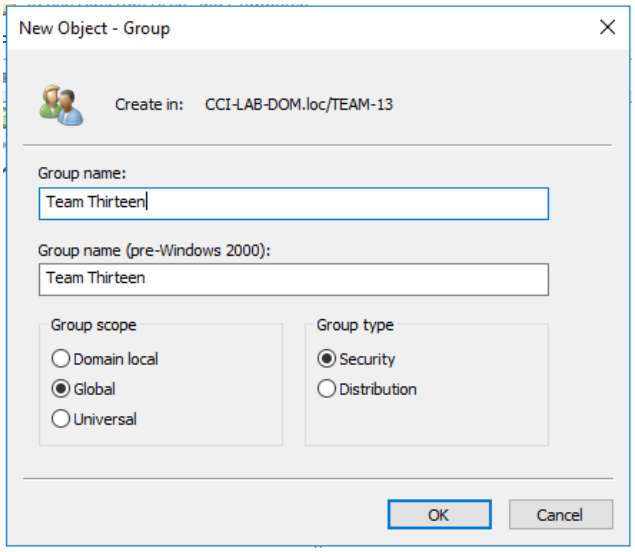
You'll be working in and with the Organizational Unit (OU) you've created, for the next few labs.

Create User and Group Objects in Your Team Organizational Unit (continued)

Right-click the container you just created and select *New Group*.



Have your team come up with a name for the group in which you will place your users:



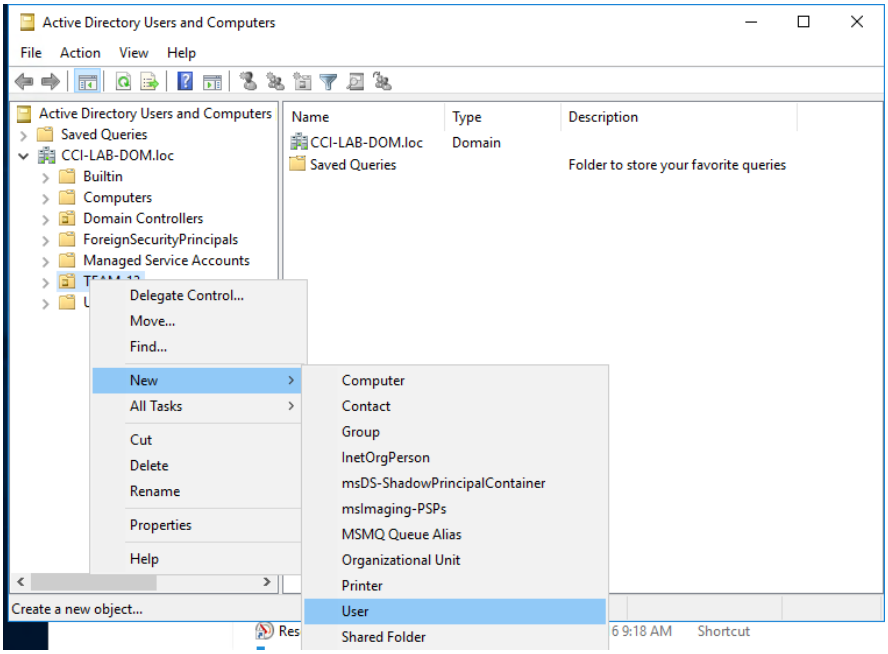
Create a Global group, with group type remaining Security.

Distribution groups are simply lists of users, typically used for e-mail notification.

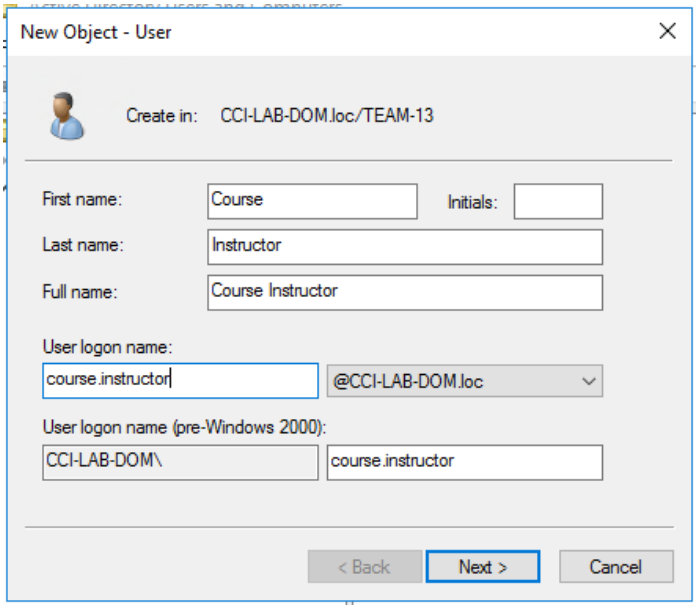
For Deliverable #8, what did your team name its Group?

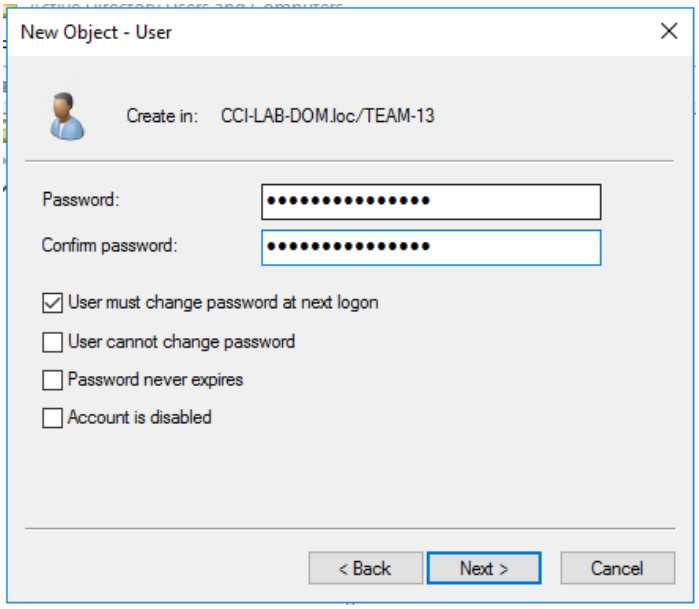
Create User and Group Objects in Your Team Organizational Unit (continued)

Right-click your team's container and select *New User*.



Have each member of your team create a user account for himself or herself.





AS ALWAYS, DO NOT USE THE SAME PASSWORD FOR ANY ACCOUNT YOU CREATE IN THIS CLASS AS YOU DO FOR ANY OTHER SYSTEM OR PURPOSE!

For Deliverable #9, what are the usernames of the accounts that your team created? Did your team do anything different that you did when you created local accounts in the previous lab?

Deliverables

Deliverable 1: From Action 1, write your name, the number of your team, the name of your partners, and the date.

Deliverable 2: From Action 4, why isn't your *Active Directory Users and Computers* tool working?

Deliverable 3: From Action 6, in which mode is your team server presently operating?

Deliverable 4: From Action 6, what new members have appeared in the local Administrators group? What does this mean?

Deliverable 5: From Action 7, what did your team name its Organizational Unit object?

Deliverable 6: From Action 7, is this Organizational Unit object a container object or a leaf object?

Deliverable 7: From Action 8, what did your team name its Group?

Deliverable 8: From Action 8, what are the usernames of the accounts that your team created? Did your team do anything different that you did when you created local accounts in the previous lab?