



Domain Controller S.O.P.

By: LCpl Hundley

LCpl Hepton, Cpl Jimenez

3rd PLT DCO-IDM

LU: 20231024

This document will serve as the guide to Domain Controller installation and usage for operations.

Domain Controller Overview.....	1
Domain Controller Intent.....	2
Domain Controller Installation.....	3
Domain Controller Set-Up: DC1.....	5
Domain Controller Setup: DC2.....	15
Adding a Workstation to the Domain.....	18

Domain Controller Overview

This guide will go over how to properly set up multiple domain controllers on a CyberPac running ESXI. A domain controller is a server or servers on a network responsible for managing the network and identity security requests. In our network, we set up a minimum of two domain controllers for redundancy purposes.



Domain Controller Intent

The primary intent of having a Domain Controller in a Windows-based network environment is to centrally manage, authenticate, and authorize users, computers, and resources within a domain. Here are some key purposes and benefits:

Single Sign-On (SSO): Users can access multiple resources within the domain without needing to enter their credentials repeatedly. Once authenticated by the Domain Controller, users can access various resources seamlessly.

Domain Name system (DNS): Hold server names and IP addresses for their domains and will share them within the network when requested.

Dynamic Host Configuration Protocol (DHCP): Automatically assigns and allocates IP addresses to hosts on the domain.

Centralized Management and Centralized Authentication: Domain Controllers authenticate and validate the identity of users and computers trying to access network resources. Domain Controllers also allow administrators to centrally manage user accounts, permissions, policies, and configurations across the network. This simplifies administration tasks and ensures consistency in settings and access control.

Group Policy Management: Domain Controllers facilitate the use of Group Policy Objects (GPOs), enabling administrators to apply and enforce policies, settings, and restrictions across multiple machines or users within the domain.

Resource Access Control: Domain Controllers help control access to network resources by defining and enforcing access permissions based on user roles, groups, or organizational units.

Redundancy and Fault Tolerance: In our environment we use two Domain Controllers which will provide fault tolerance and redundancy. This ensures that if one Domain Controller fails, the other can continue to provide its services.

In summary, Domain Controllers play a crucial role in managing user authentication, resource access, and network policies within a Windows domain-based network, providing security, centralized management, and efficient administration capabilities.



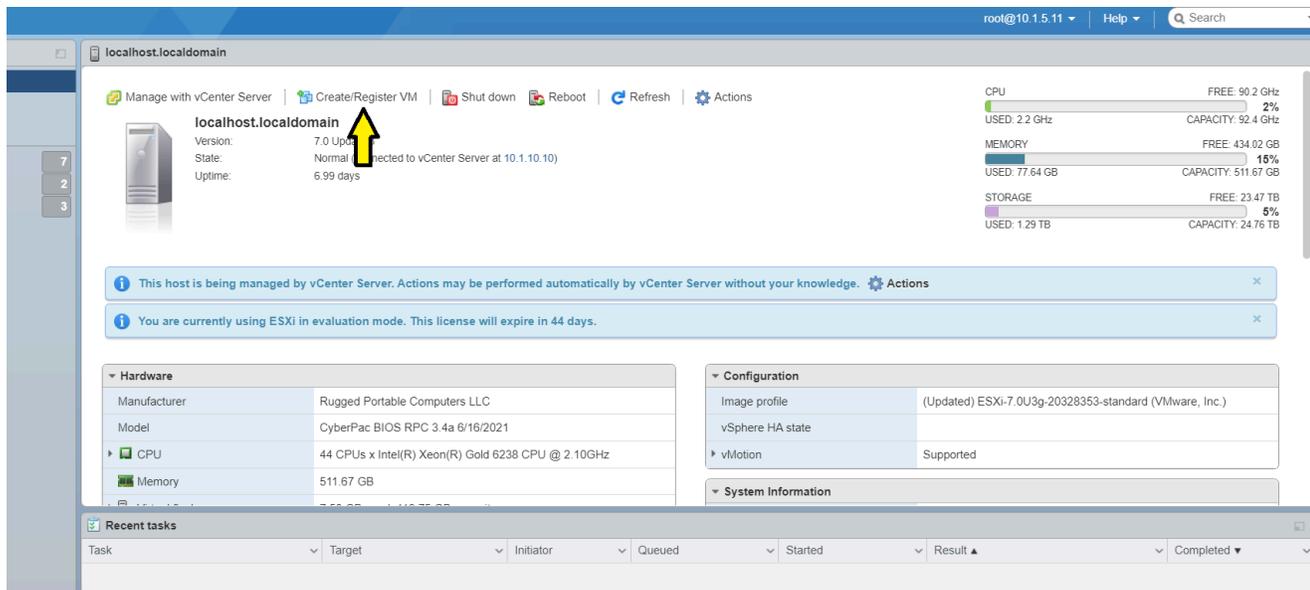
Domain Controller Installation

- ❖ Log in to ESXI VM
- ❖ Plug in bitlocker
- ❖ Enter password on the bitlocker
- ❖ Press connect
- ❖ Use the server2019 iso
- ❖ Within ESXI go to storage
- ❖ Upload the iso (Server2019-20210513) to data storage 2 (the storage that has the most space available)
- ❖ Note: the upload will take a minute

*****DC1 Installation and DC2 Installation*****

Step 1:

Create a new Virtual Machine





Step 2:

- ❖ Name: (name of Domain Controller Either DC1 or DC2)
- ❖ -Compatibility - ESXI 7.0 U2*
- ❖ -Guest OS family - Windows
- ❖ -Guest OS version - Microsoft Windows Server 2019 (64-bit)

New virtual machine - DC3 (ESXi 7.0 U2 virtual machine)

1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete

Select a name and guest OS

Specify a unique name and OS

Name
DC3

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility: ESXi 7.0 U2 virtual machine

Guest OS family: Windows

Guest OS version: Microsoft Windows Server 2019 (64-bit)

Enable Windows Virtualization Based Security

Back Next Finish Cancel

Step 3:

- ❖ Make sure the VM has the following hardware options set:
- ❖ *8G RAM
- ❖ *100G Hard Disk Space
- ❖ *Thin Provisioning
- ❖ *1 NIC (network adapter 1 should already be assigned)



New virtual machine - DC3 (ESXi 7.0 U2 virtual machine)

- 1 Select creation type
- 2 Select a name and guest OS
- 3 Select storage
- 4 Customize settings**
- 5 Ready to complete

Customize settings

Configure the virtual machine hardware and virtual machine additional options

Virtual Hardware | VM Options

Add hard disk | Add network adapter | Add other device

CPU	8	
Memory	8	GB
Hard disk 1	100	GB
Maximum Size	23.18 TB	
Location	[CyberPac Datastore 1] DC3/	Browse...
Disk Provisioning	<input checked="" type="radio"/> Thin provisioned <input type="radio"/> Thick provisioned, lazily zeroed <input type="radio"/> Thick provisioned, eagerly zeroed	
Shares	Normal	1000
Limit - IOPs	Unlimited	

Back Next Finish Cancel

Step 4:

- ❖ CD Drive -> select uploaded ISO file -> select ISO's Folder -> select "server2019"

New virtual machine - DC3 (ESXi 7.0 U2 virtual machine)

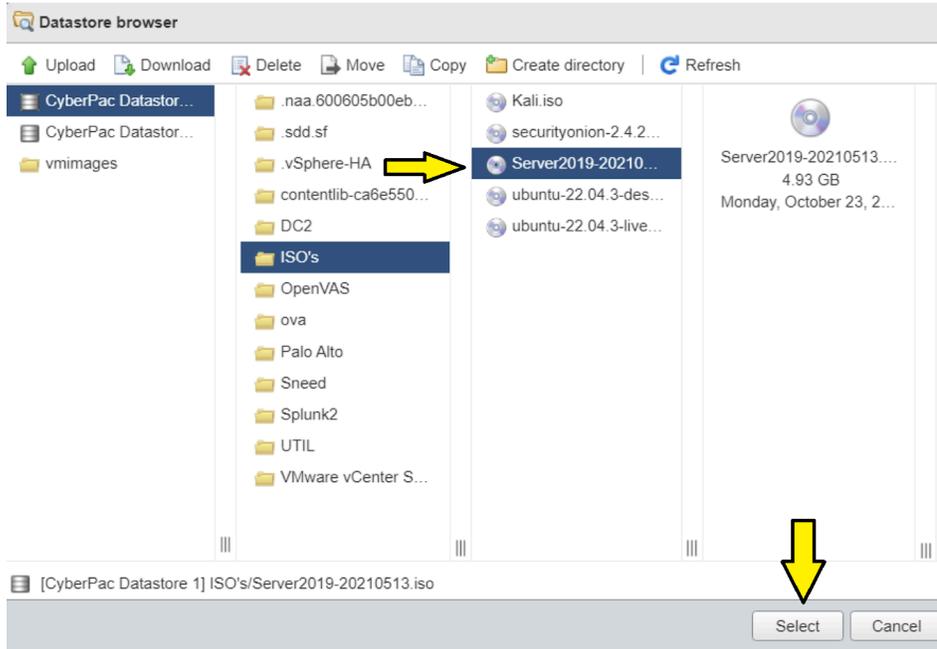
- 1 Select creation type
- 2 Select a name and guest OS
- 3 Select storage
- 4 Customize settings**
- 5 Ready to complete

Customize settings

Configure the virtual machine hardware and virtual machine additional options

Controller location	SCSI controller 0	SCSI (0:0)
Disk mode	Dependent	
Sharing	None	
SCSI Controller 0	LSI Logic SAS	
SATA Controller 0		
USB controller 1	USB 3.1	
Network Adapter 1	Domain Services	<input checked="" type="checkbox"/> Connect
CD/DVD Drive 1	Datastore ISO file	<input checked="" type="checkbox"/> Connect
Status	<input checked="" type="checkbox"/> Connect at power on	

Back Next Finish Cancel

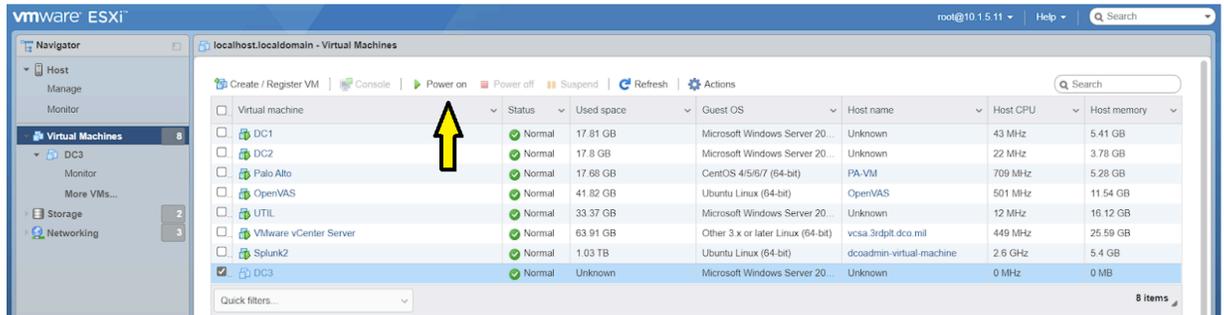


Domain Controller Set-Up: DC1

Step 1:

Power on the created VM

- ❖ press any button to get to the blue setup screen and boot normally
- ❖ continue through prompts

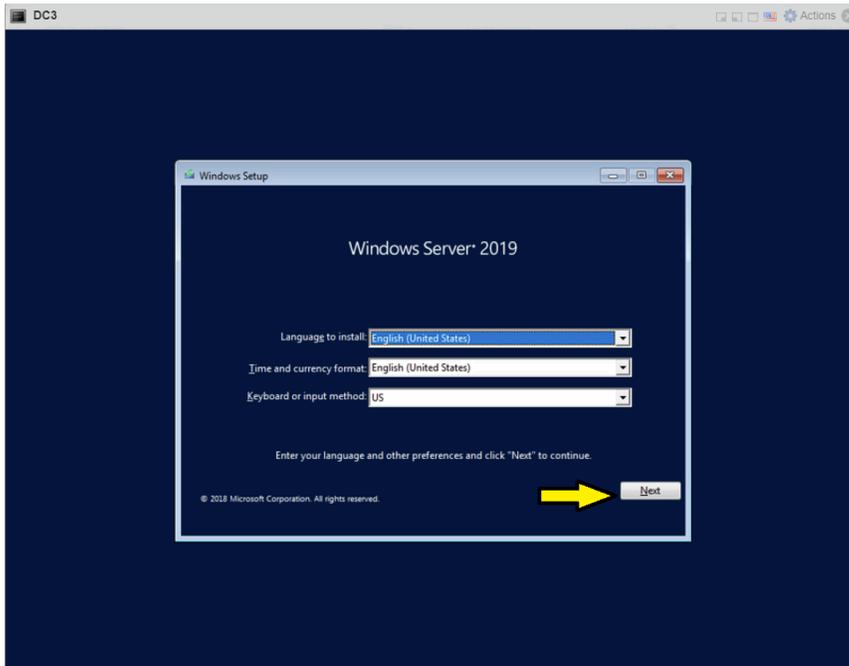


NOTE: When powering on the machine you will click the small screen to access the terminal, you will have to be quick to click in the window and press any key in the terminal otherwise it will timeout.



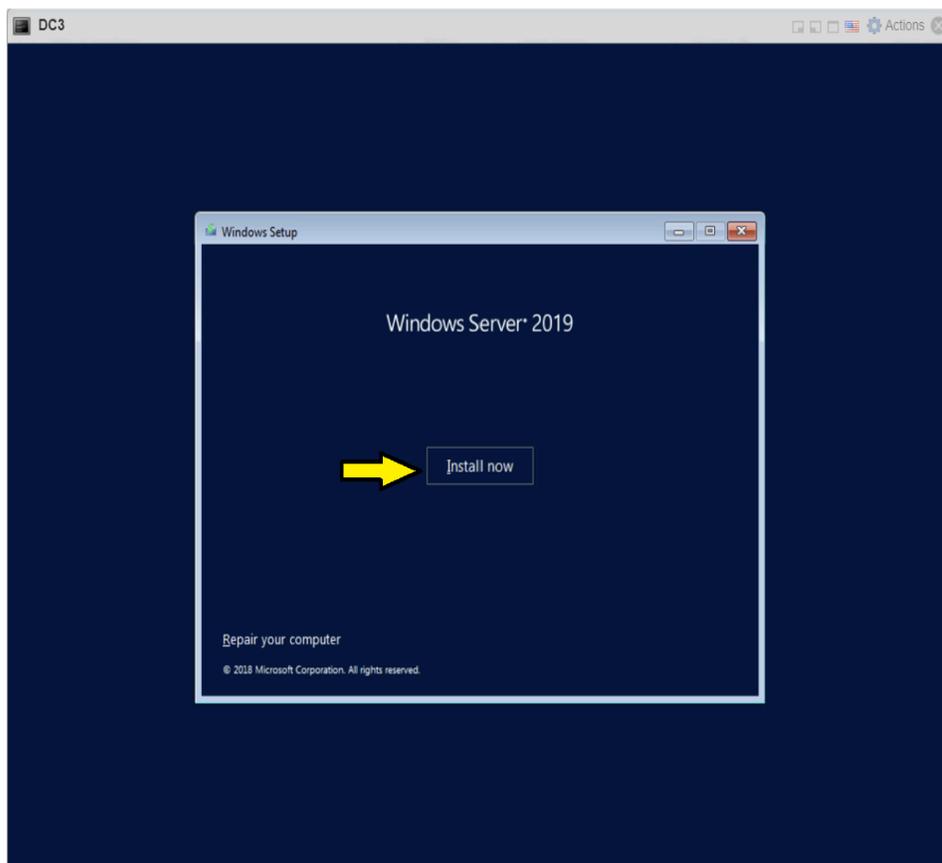
Step 2:

- ❖ Select Next



Step 3:

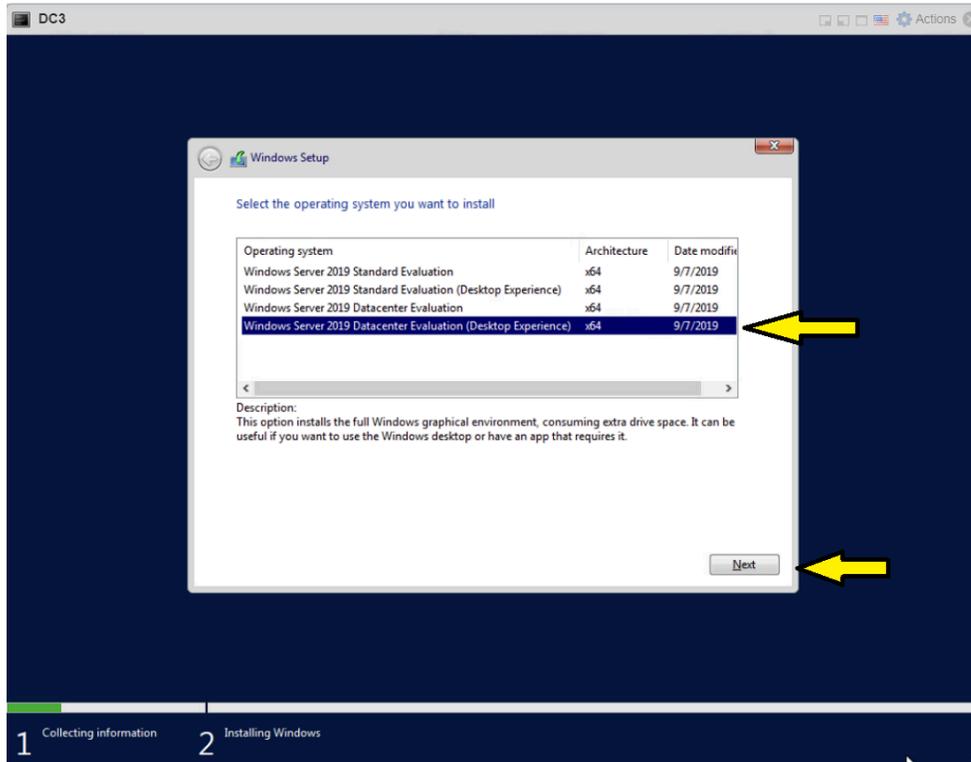
- ❖ Select Install





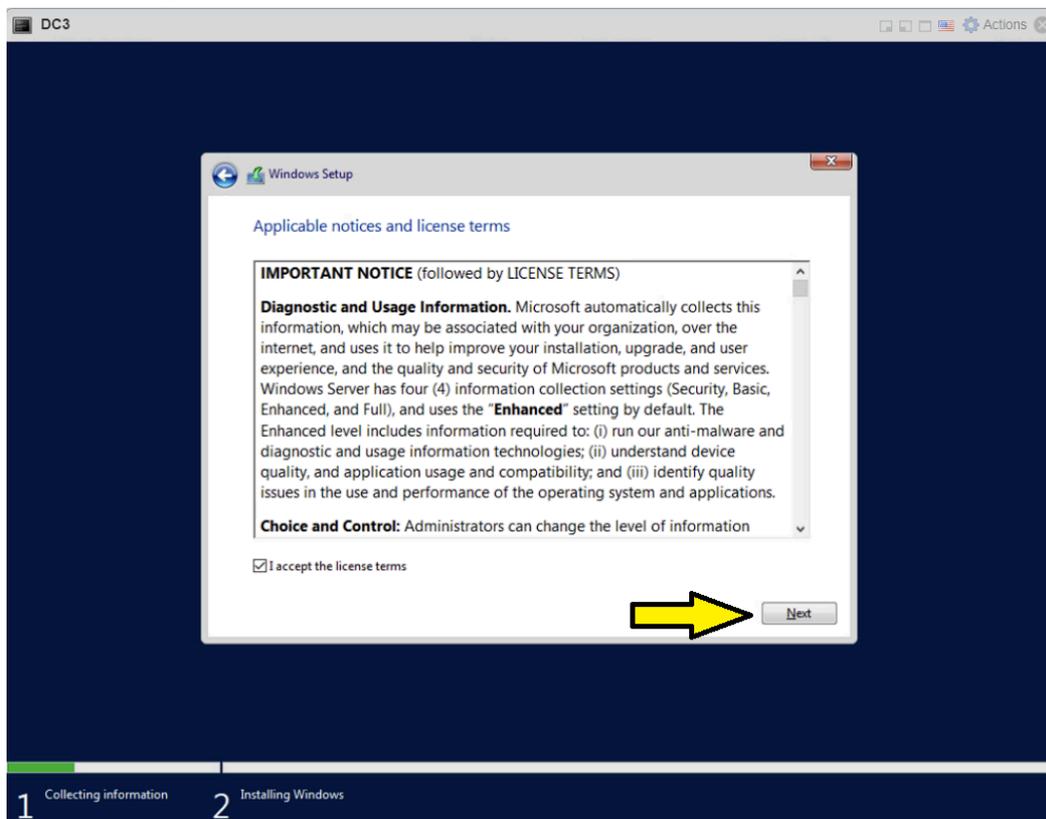
Step 4:

- ❖ -select datacenter evaluation (desktop experience)



Step 5:

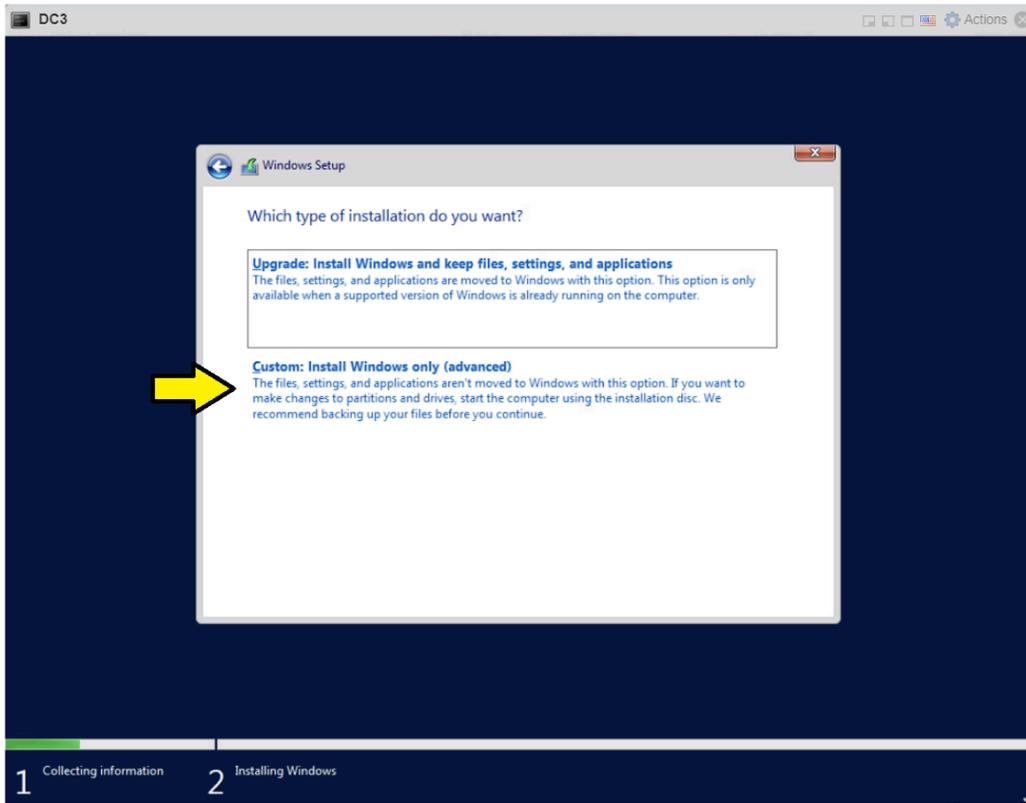
- ❖ Accept Eula





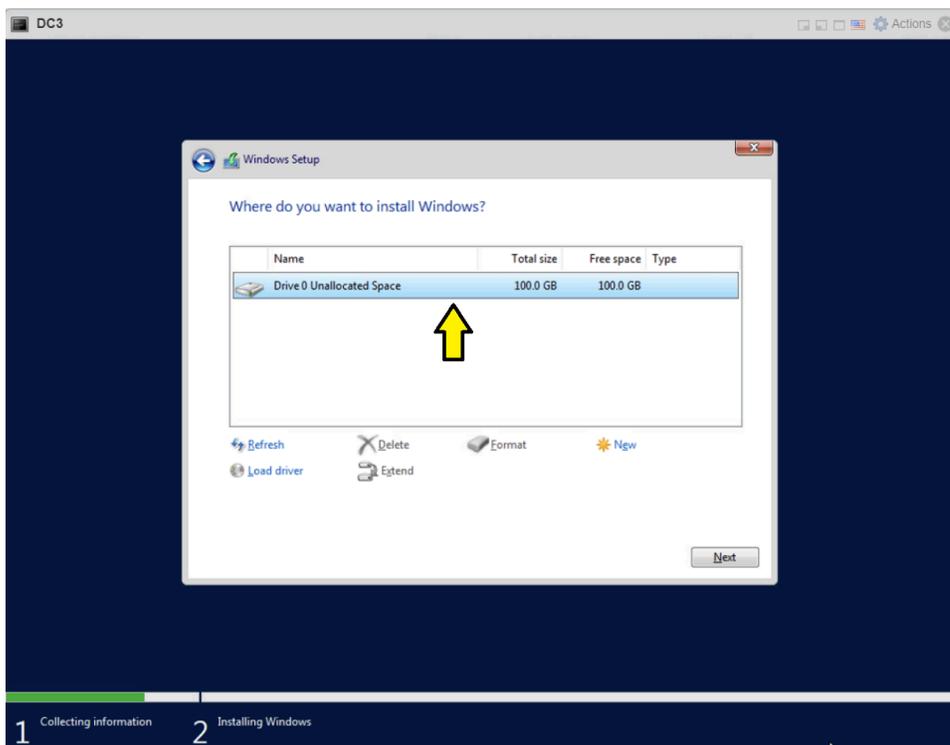
Step 6:

- ❖ Select Custom Install



Step 7:

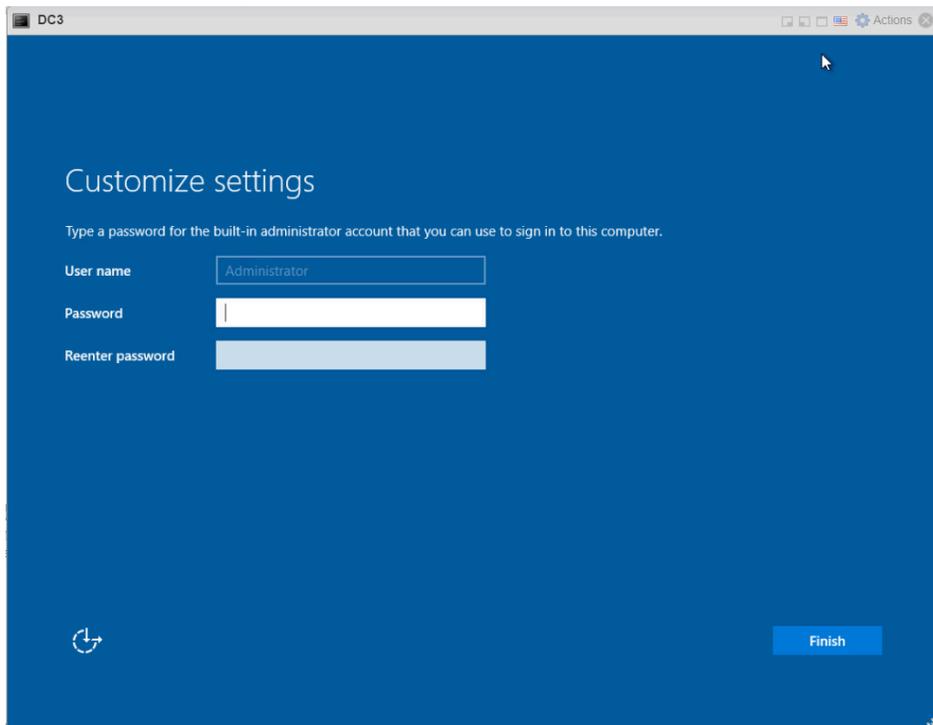
- ❖ Use Drive 0 (should be only one)





Step 8:

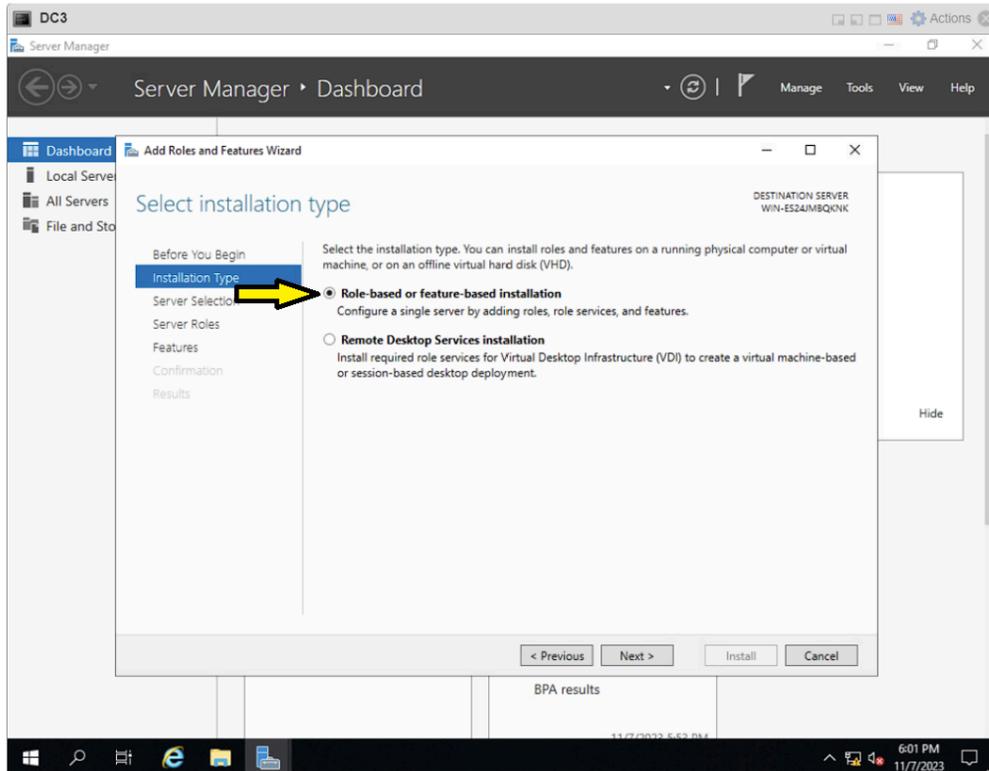
- ❖ Create admin password
- ❖ -Login

A screenshot of a Windows installation window titled 'DC3'. The window has a blue background and contains the text 'Customize settings'. Below this, it says 'Type a password for the built-in administrator account that you can use to sign in to this computer.' There are three input fields: 'User name' with 'Administrator' entered, 'Password', and 'Reenter password'. A 'Finish' button is located at the bottom right. The window title bar shows 'DC3' and 'Actions'.

*****STOP HERE FOR [Domain Controller Setup: DC2](#)*****

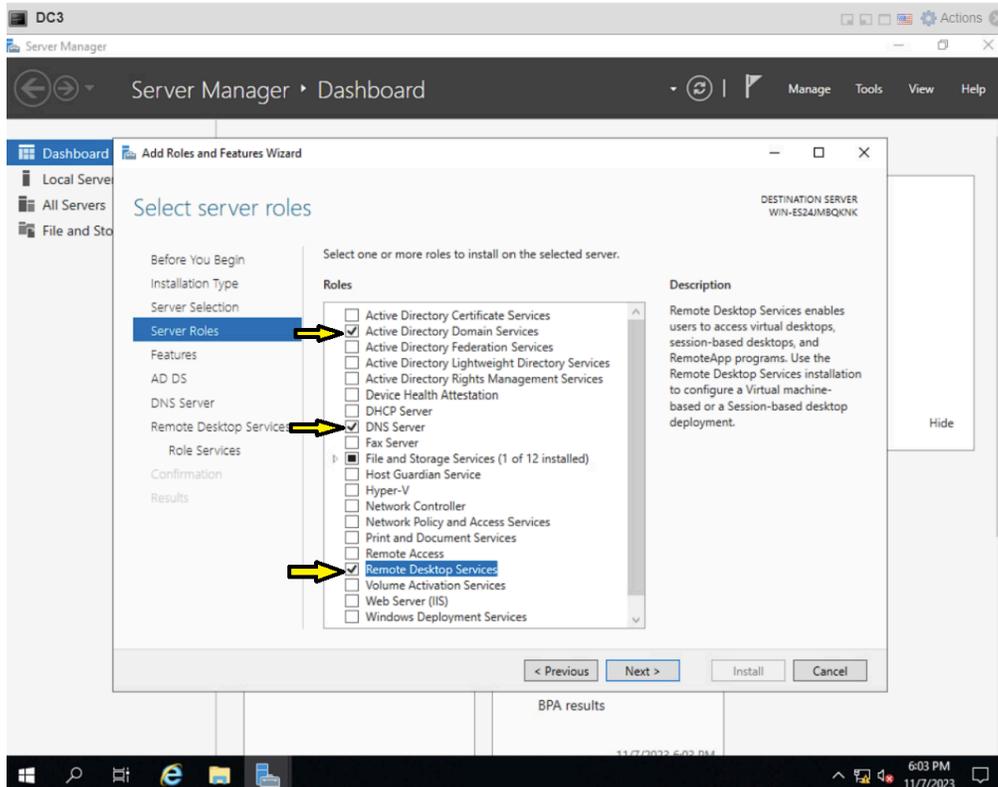
Step 9:

- ❖ On the server manager screen (which automatically opens upon login)
Click Add roles and features
 - Select 'Next'
- ❖ -Select role based install



Step 10:

- ❖ -Select active directory domain services, dns server, remote desktop services



Step 11:

- ❖ -role services
 - Scroll to the bottom and click next until you see several more checkboxes with more RDP options
- ❖ -Select RDP web access



DC3 Server Manager Dashboard

Add Roles and Features Wizard

Select role services

Before You Begin

- Installation Type
- Server Selection
- Server Roles
- Features
- AD DS
- DNS Server
- Remote Desktop Services
- Confirmation
- Results

Role services

- Remote Desktop Connection Broker
- Remote Desktop Gateway
- Remote Desktop Licensing
- Remote Desktop Session Host
- Remote Desktop Virtualization Host
- Remote Desktop Web Access

Description

Remote Desktop Web Access (RD Web Access) enables users to access RemoteApp and Desktop Connection through the Start menu or through a web browser. RemoteApp and Desktop Connection provides users with a customized view of RemoteApp programs, session-based desktops, and virtual desktops.

< Previous Next > Install Cancel

❖ **Step 12:**

❖ Set the restart checkbox, then select "Install"

DC3 Server Manager Dashboard

Add Roles and Features Wizard

Confirm installation selections

Before You Begin

- Installation Type
- Server Selection
- Server Roles
- Features
- AD DS
- DNS Server
- Remote Desktop Services
- Role Services
- Web Server Role (IIS)
- Role Services
- Confirmation
- Results

To install the following roles, role services, or features on selected server, click Install.

- Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Add Roles and Features Wizard

If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

Yes No

Remote Desktop Web Access

Remote Server Administration Tools

- Role Administration Tools
- AD DS and AD LDS Tools

Export configuration settings

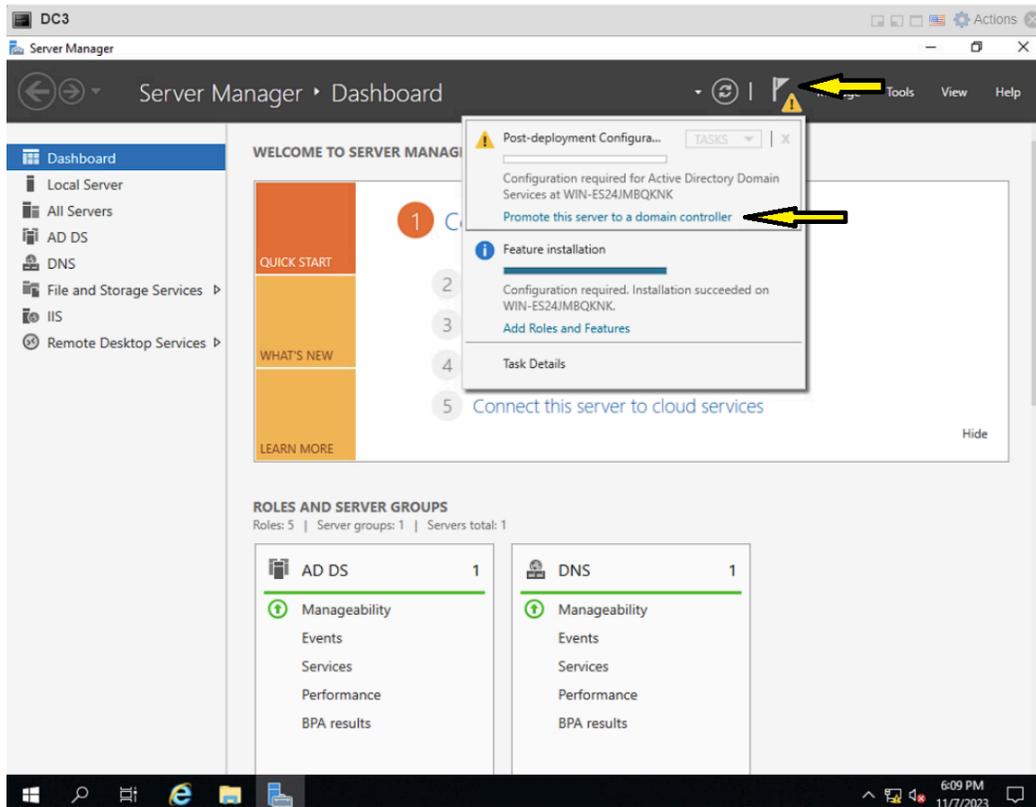
Specify an alternate source path

< Previous Next > Install Cancel



Step 13:

- ❖ Click yellow caution triangle in server manager (ESXI)\
- ❖ -Promote to domain controller



Step 14:

- ❖ For DC1, select 'add new forest'
- ❖ -3rdplt. I



The screenshot shows the 'Deployment Configuration' step of the Active Directory Domain Services Configuration Wizard. The 'Add a new forest' radio button is selected. The 'Root domain name' field contains '3rdpltdco.mil'. The 'Next >' button is highlighted.

Deployment Configuration

TARGET SERVER
WIN-ES24JMBQKNK

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Root domain name: 3rdpltdco.mil

< Previous Next > Install Cancel

Step 15:

❖ Create password

The screenshot shows the 'Domain Controller Options' step of the Active Directory Domain Services Configuration Wizard. The 'Forest functional level' and 'Domain functional level' are both set to 'Windows Server 2016'. The 'Domain Name System (DNS) server' and 'Global Catalog (GC)' checkboxes are checked. The 'Password' and 'Confirm password' fields are filled with dots. The 'Next >' button is highlighted.

Domain Controller Options

TARGET SERVER
WIN-ES24JMBQKNK

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

- Domain Name System (DNS) server
- Global Catalog (GC)
- Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: [dots]

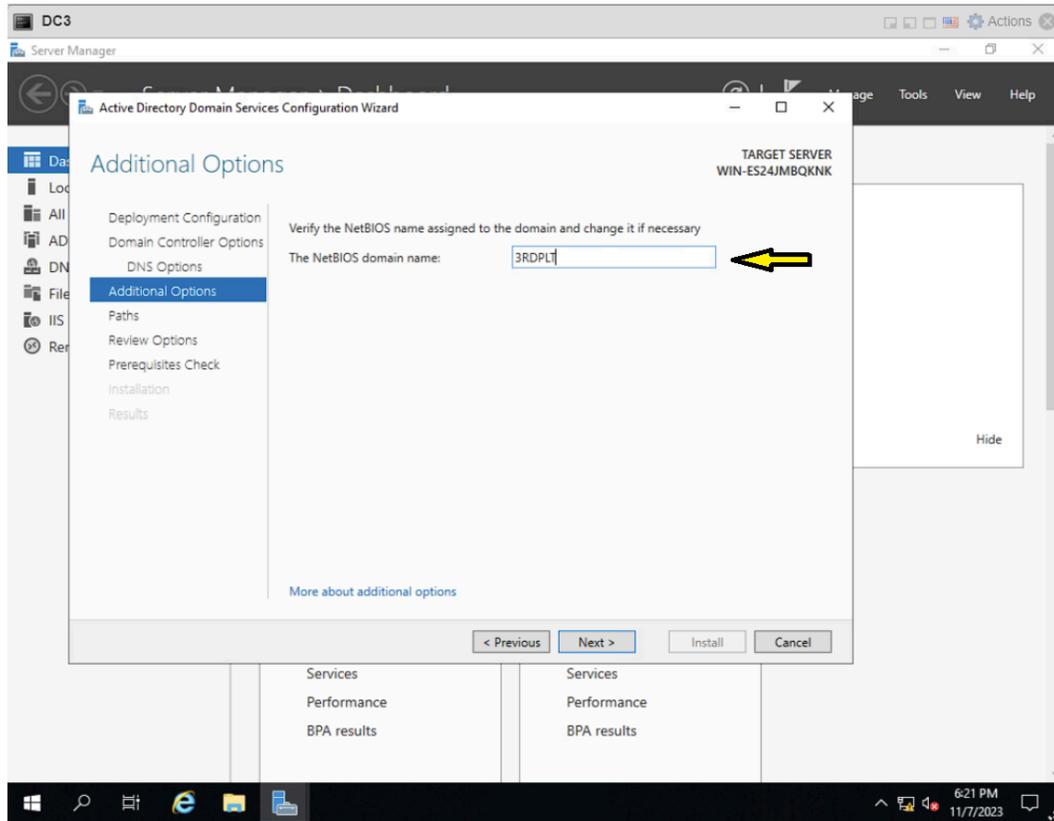
Confirm password: [dots]

< Previous Next > Install Cancel



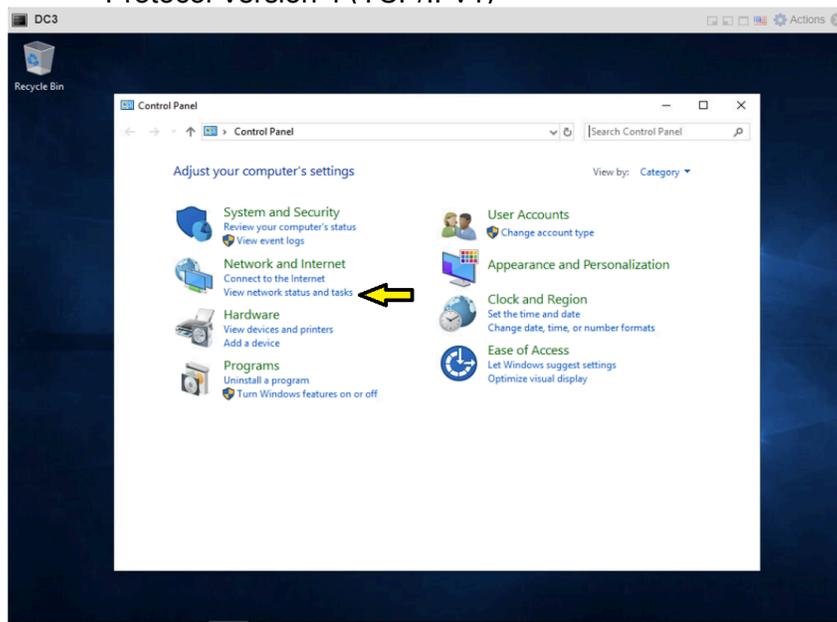
Step 16:

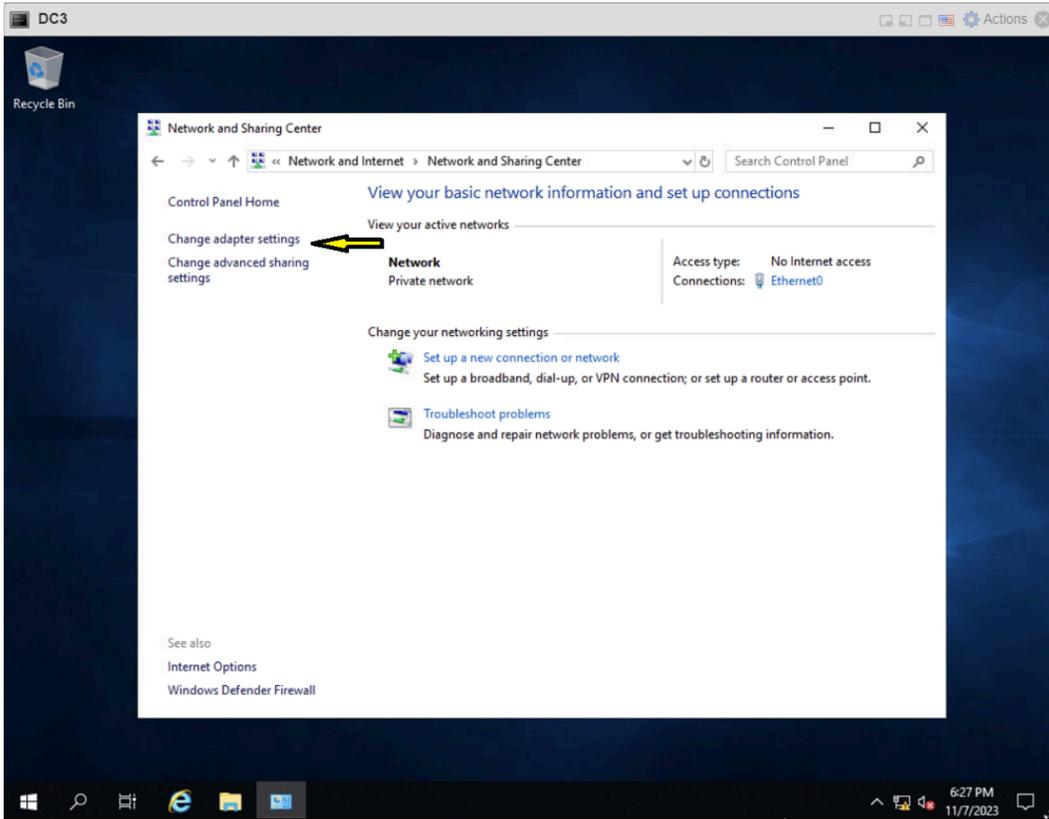
- ❖ Additional options
- ❖ -Verify that the netbios name is 3RDPLT (this should automatically populate)



Note if the VM does not restart automatically manually restart the VM

- ❖ **Step 17:**
- ❖ For DC1 Only- search control panel -> view network status and tasks -> change adapter settings -> click on ethernet -> properties -> double click on 'Internet Protocol Version 4 (TCP/IPv4)'





DC3

Recycle Bin

Network and Sharing Center

View your basic network information and set up connections

Control Panel Home

View your active networks

Change adapter settings **←**

Change advanced sharing settings

Network
Private network

Access type: No Internet access
Connections: Ethernet0

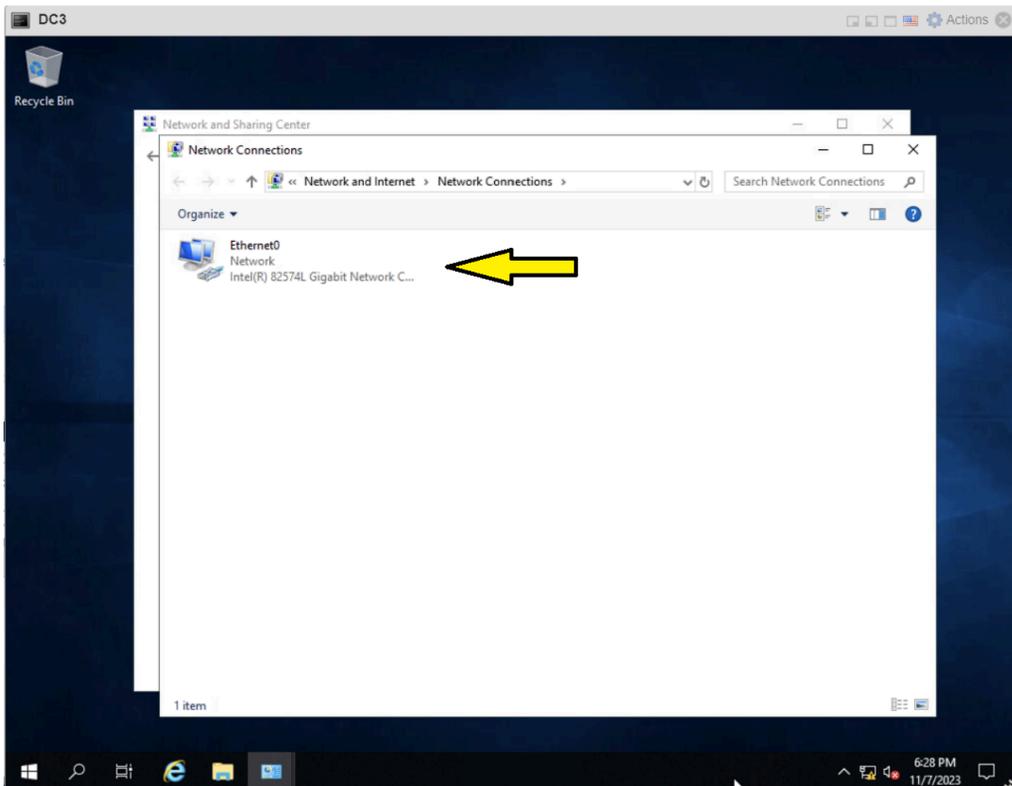
Change your networking settings

- Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
- Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

See also

- Internet Options
- Windows Defender Firewall

6:27 PM 11/7/2023



DC3

Recycle Bin

Network Connections

Organize

- Ethernet0**
Network
Intel(R) 82574L Gigabit Network C... **←**

1 item

6:28 PM 11/7/2023



Network Connections

Network and Internet > Network Connections

Ethernet0 Status

General

Connection

IPv4 Connectivity:	No Internet access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	02:04:39
Speed:	1.0 Gbps

Details...

Activity

Sent	Received
Bytes: 42,520	13,100

Properties Disable Diagnose Close

Network Connections

Network and Internet > Network Connections

Ethernet0 Properties

Networking

Connect using:

Intel(R) 82574L Gigabit Network Connection

Configure...

This connection uses the following items:

- Client for Microsoft Networks
- File and Printer Sharing for Microsoft Networks
- QoS Packet Scheduler
- Internet Protocol Version 4 (TCP/IPv4)
- Microsoft Network Adapter Multiplexor Protocol
- Microsoft LLDP Protocol Driver
- Internet Protocol Version 6 (TCP/IPv6)

Install... Uninstall Properties

Description

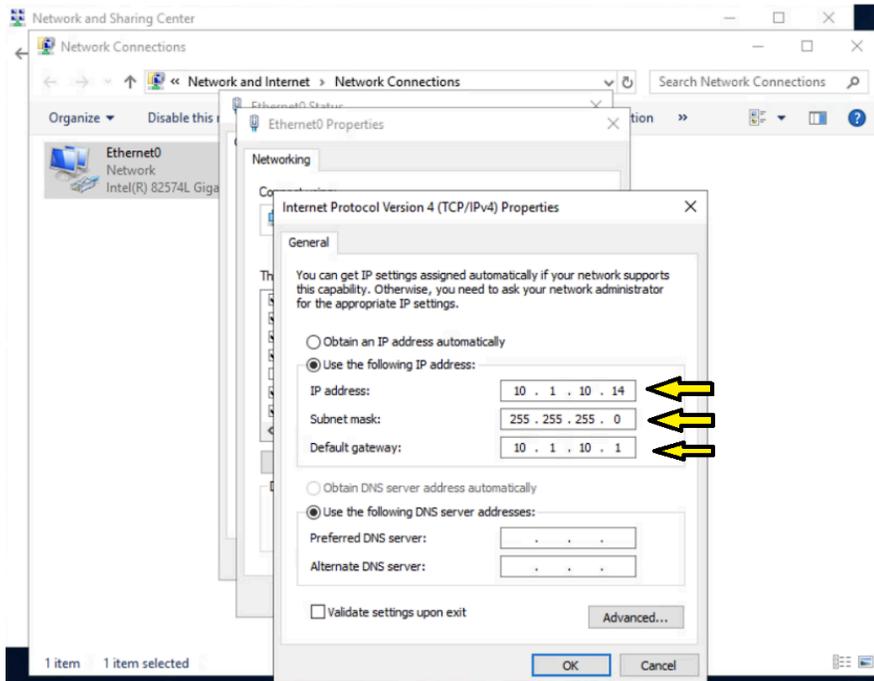
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Step 18:

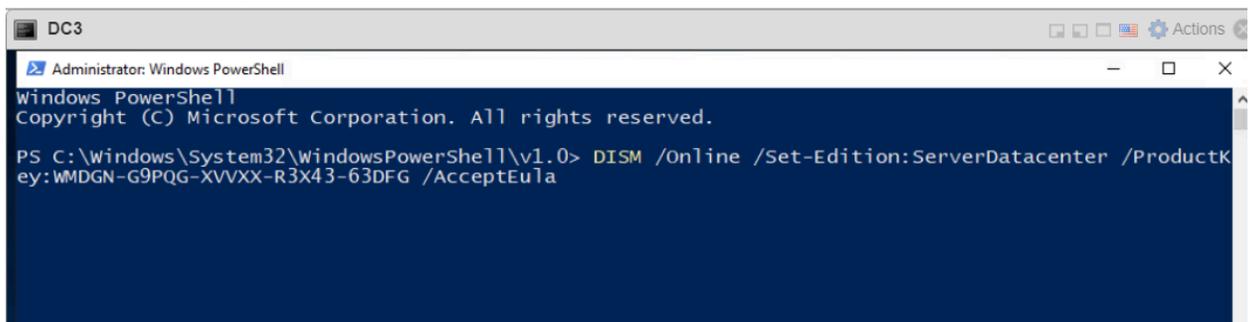


- ❖ Change the ip address and subnet mask settings (10.1.10.14, Subnet mask 255.255.255.0, Default gateway 10.1.10.1)



Step 19:

- ❖ run powershell as administrator
- ❖ Next take the DC out of evaluation mode by entering the following command:
 - ❖ DISM /Online /Set-Edition:ServerDatacenter /ProductKey:WMDGN-G9PQG-XVXX-R3X43-63DFG /AcceptEula



Wait for prompt to ask to restart. Restart Server

Note: DC1 is configured fully at this point

Domain Controller Set-up: DC2

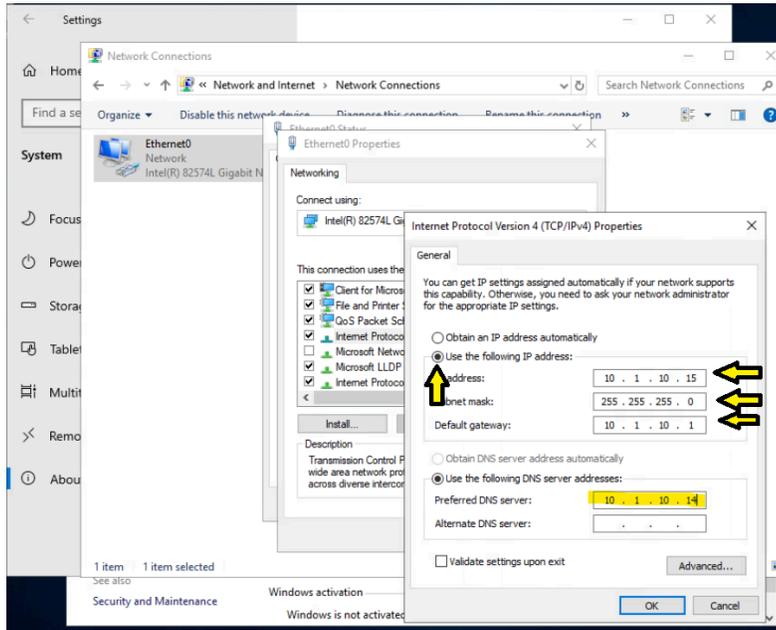
Step 1-9:

- ❖ Follow [steps 1-4](#) DC installation and [steps 1-12](#) DC Setup from DC1 setup



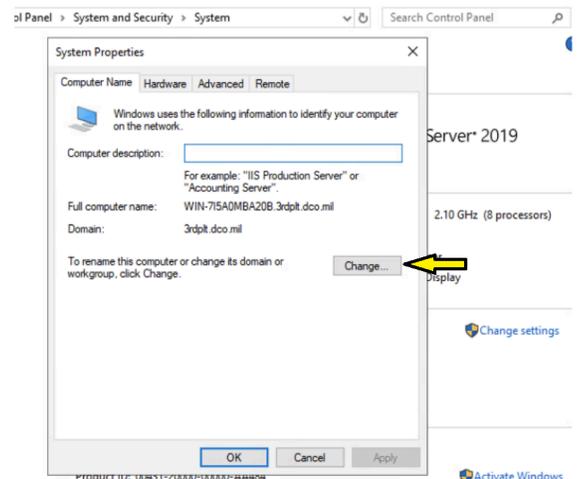
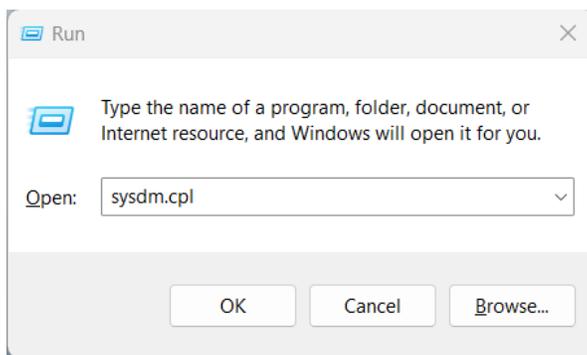
Step 9:

- ❖ Go to control panel -> Network and Internet -> Network Connections -> Ethernet 0 ->
- ❖ -Ensure that DC2 has an IP address (10.1.10.15) so that it can reach the domain and that DC1 has the correct subnet mask
- ❖ Assign DC1 IP as DC2's preferred DNS Server (10.1.10.14)



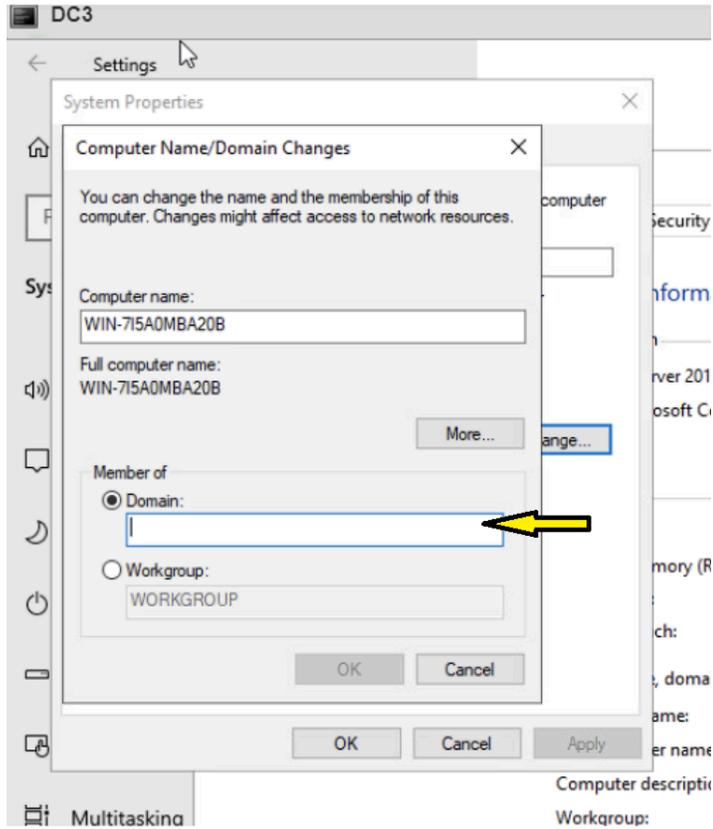
Step 10:

- ❖ Once you are on the Desktop type Windows key+R this will bring up the Run dialog box. Type 'sysdm.cpl'. Near the bottom of the screen, select 'Change'. This will bring up another dialog box which will let you change the domain and the system name.
 - Note: if the Shortcut doesn't work to get to "sysdm.cpl" go to Settings -> System -> About -> System info -> Computer Name/Domain Changes -> Change Settings



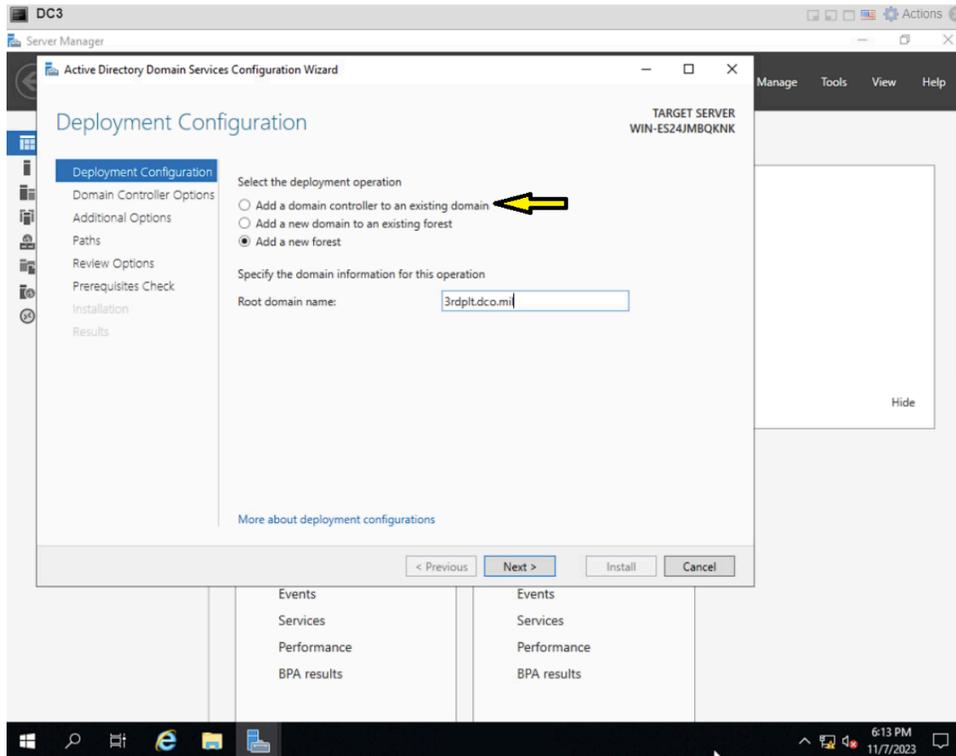


- ❖ **Step 11:**
- ❖ In the domain tab type 3rdpltdco.mil to join Domain controller 2 to Domain controller 1



Step 12:

- ❖ Go to the server manager
 - select add a domain controller to an existing domain
 - select change user and supply credentials

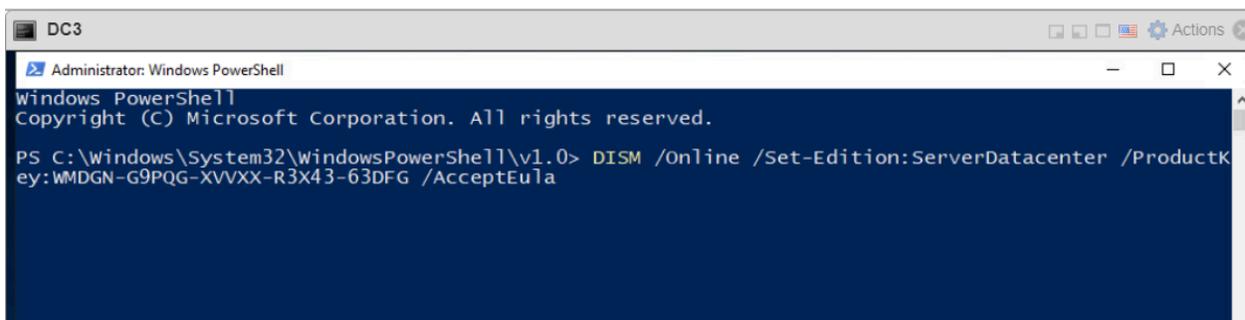


Step 14:

- ❖ After you have verified that all settings are correct, select install
- ❖ The VM should automatically restart after finishing install.

Step 15:

- ❖ run powershell as administrator
- ❖ Next take the DC out of evaluation mode (both of them) by entering the following command:
 - ❖ DISM /Online /Set-Edition:ServerDatacenter /ProductKey:WMDGN-G9PQG-XVXX-R3X43-63DFG /AcceptEula





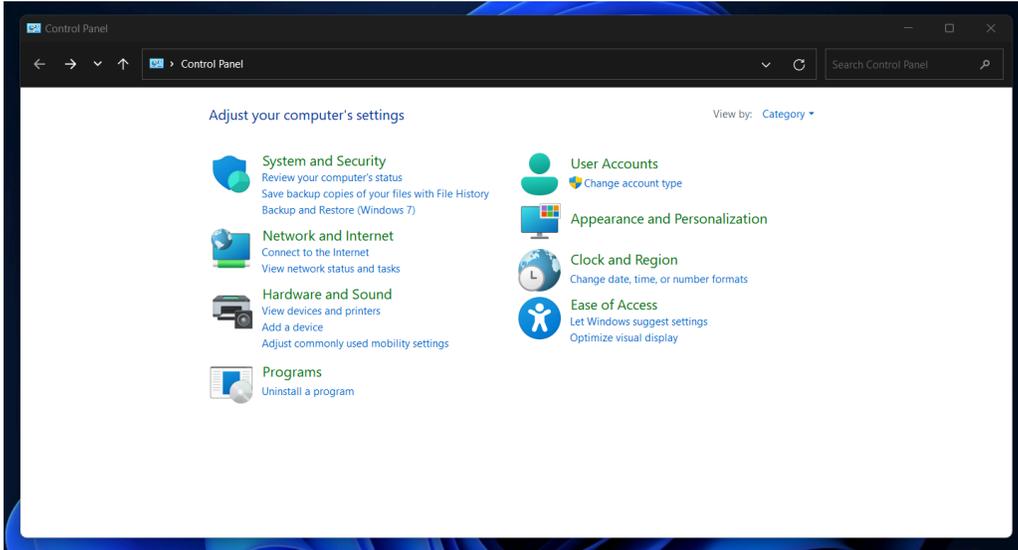
Adding a Workstation to the Domain

Step 1:

- ❖ Verify workstation has connectivity to the DC, by pinging the DC

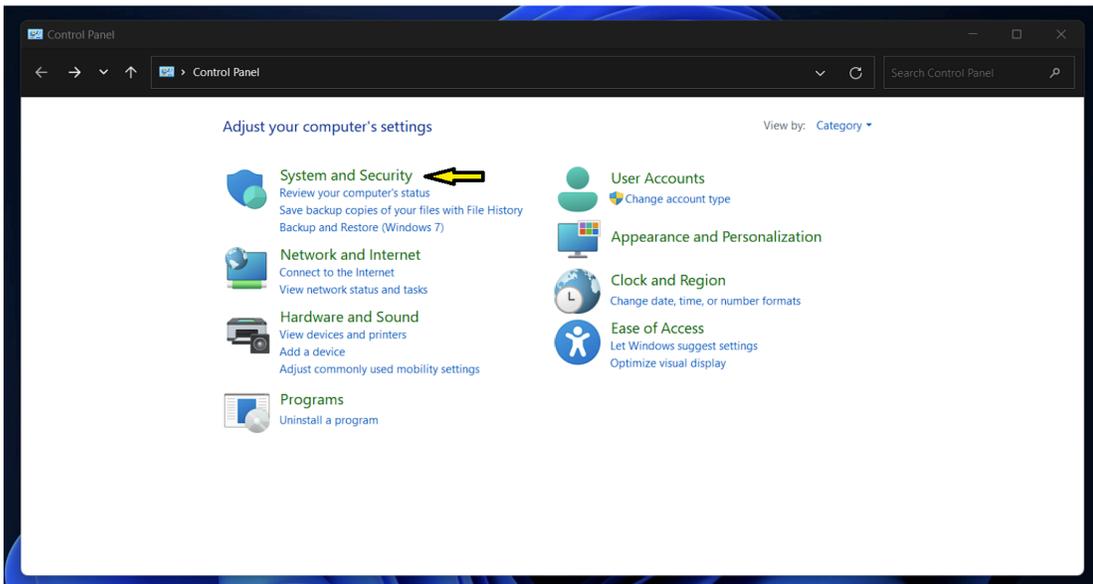
Step 2:

- ❖ Open Control Panel



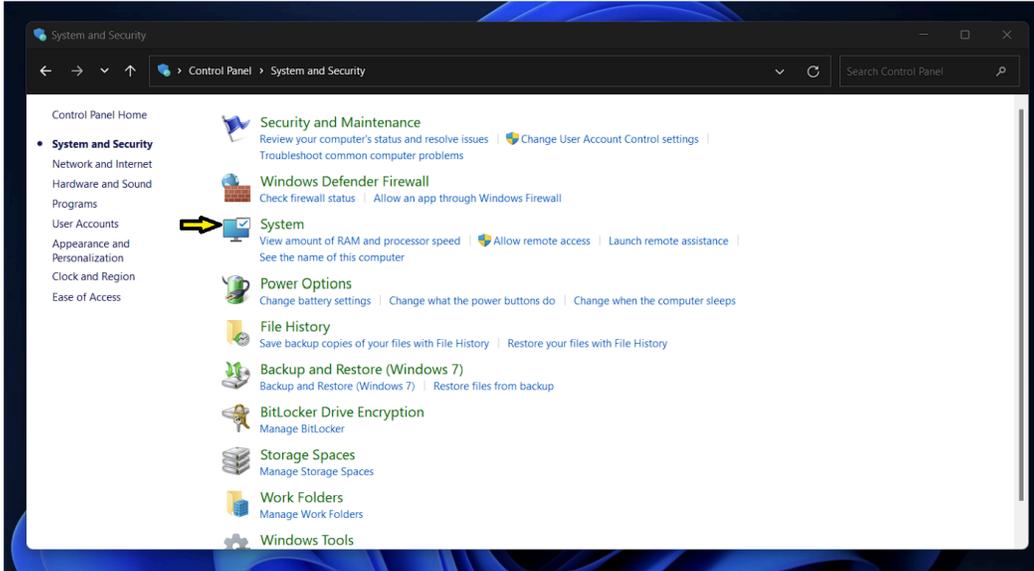
Step 3:

- ❖ Go to system and security



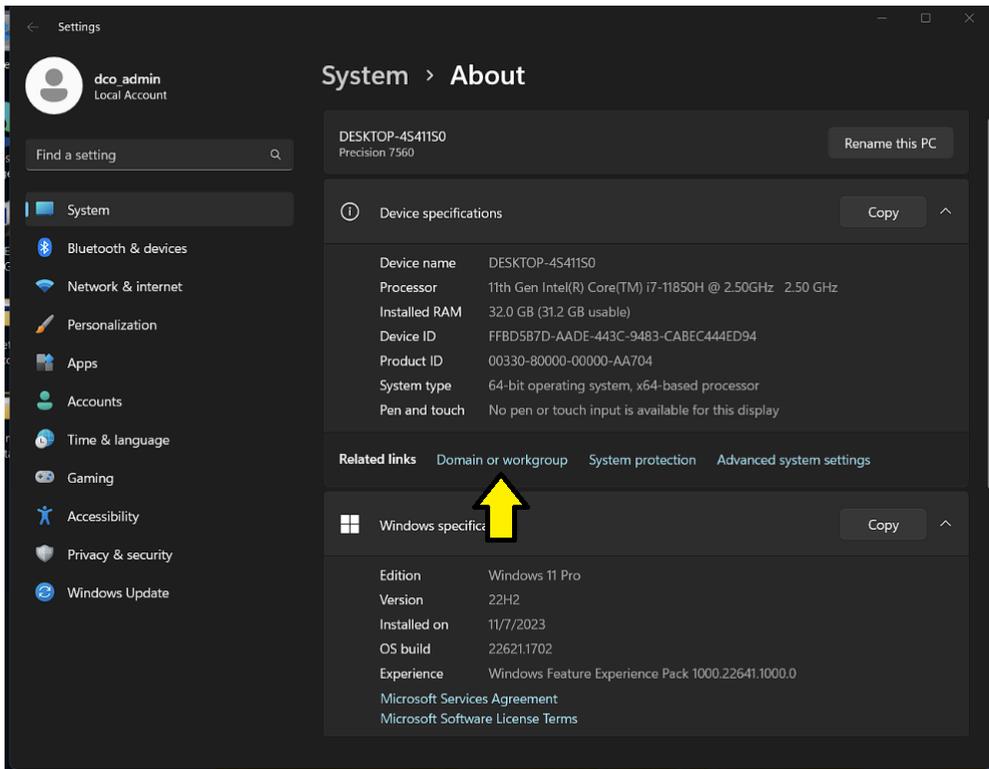
Step 4:

- ❖ Click system, a new window should open



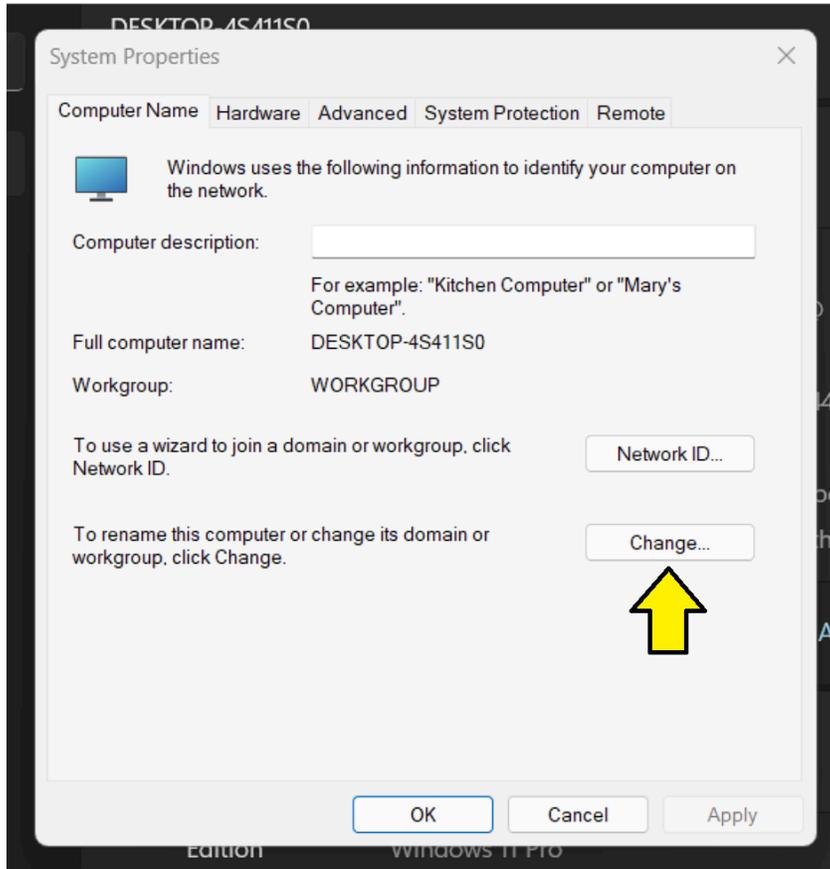
Step 5:

- ❖ Click domain or workgroup, a new window should open



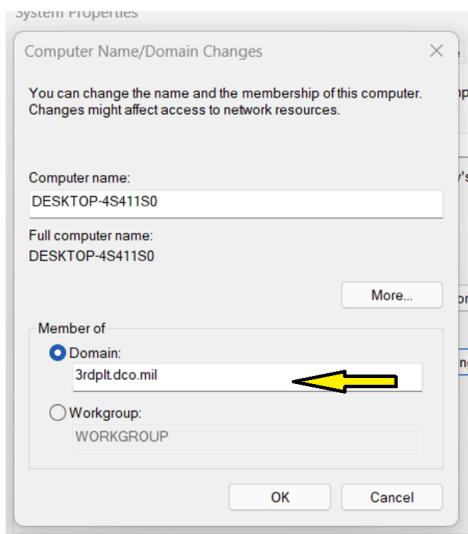
Step 6:

- ❖ Click change



Step 7:

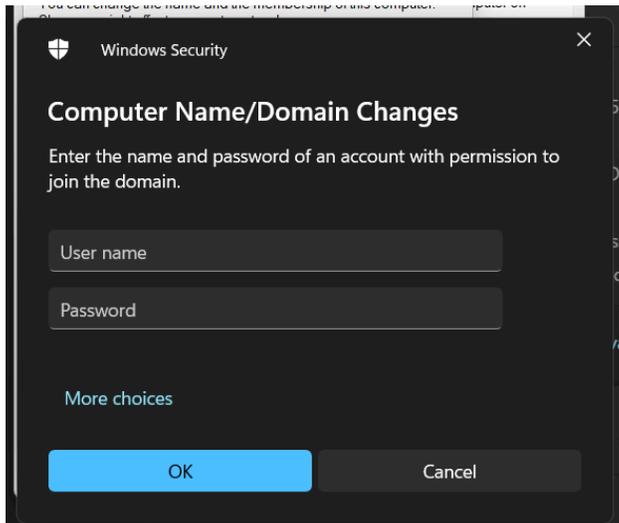
- ❖ Click the domain circle, type in the name of your domain





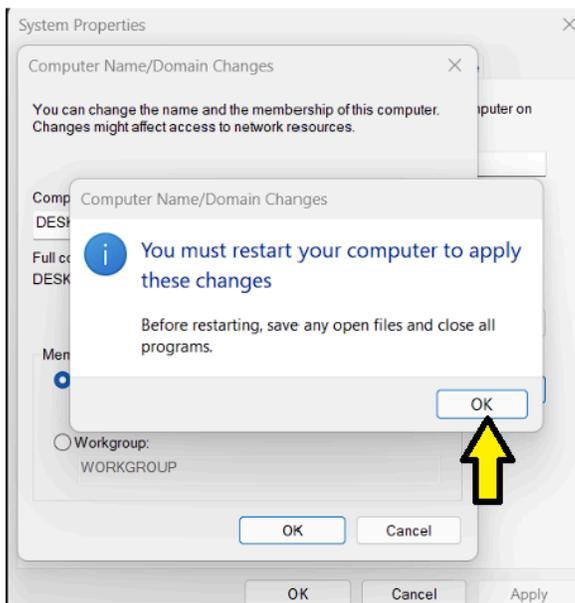
Step 8:

- ❖ Click OK, a new window should appear. Input the username and password of an administrator, a new window should open (this is authentication to the DC, **NOT** your local workstation)



Step 9:

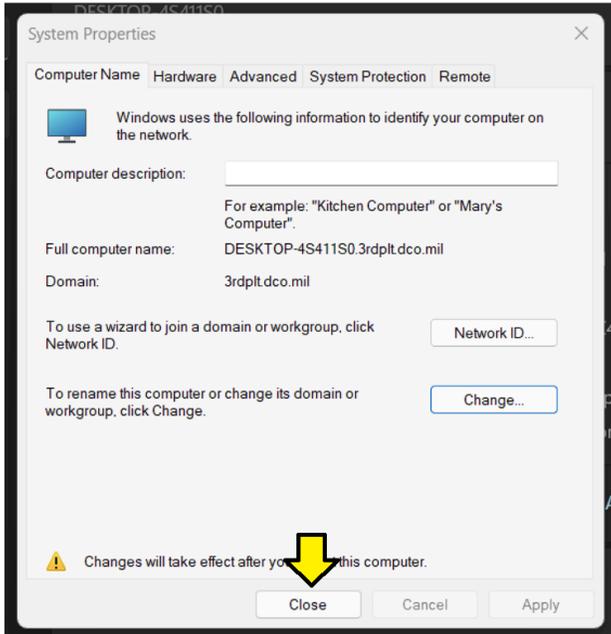
- ❖ Click OK, it should close that window





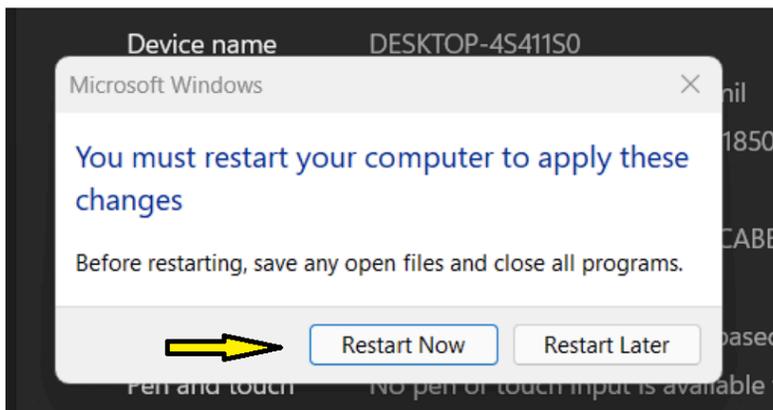
Step 10:

- ❖ Click Close, it should close that window



Step 11:

- ❖ Click "Restart Now", the computer should restart



Step 12:

- ❖ Repeat step 1-5 and next to domain it should show your domain name



System Properties

Computer Name Hardware Advanced System Protection Remote

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: DESKTOP-4S411S0.3rdpltdco.mil

Domain: 3rdpltdco.mil

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.