Citrix VDI Guide for Intel® Data Center GPU Flex Series

Setup Reference Guide

March 2024

Revision 1.0

Document Number: 819221

Intel technologies may require enabled hardware, software or service activation.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Performance varies by use, configuration, and other factors. Learn more on the Performance Index site.

Your costs and results may vary.

"Conflict-free" refers to products, suppliers, supply chains, smelters, and refiners that, based on our due diligence, do not contain or source tantalum, tin, tungsten or gold (referred to as "conflict minerals" by the U.S. Securities and Exchange Commission) that directly or indirectly finance or benefit armed groups in the Democratic Republic of the Congo or adjoining countries.

All product plans and roadmaps are subject to change without notice.

Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visiting the Intel Resource and Document Center.

Contents

Figures

Tables

Revision History

Revision Number	Description	Date
1.0	• Initial release of the document.	March 2024

1 Introduction

The purpose of this document is to provide Citrix* VDI (Virtual Desktop Infrastructure) setup for Intel® Data Center GPU Flex Series on Intel® Xeon® platforms, BIOS, OS, drivers which are required to enable VDI.

1.1 Terminology

The following acronyms and terms are used in this document.

Table 1-1. Terms and Their Definitions

Term	Description
ATSM	Arctic Sound-M graphics cards
BDF	Bus Device Function
BIOS	Basic input-output system
GPU	Graphics Processing Unit
Intel GVT	Intel Graphics Virtualization Technology
INTDCGPU	Intel Data Cetner GPU
IRC	Intel Resource Center
MMIO	Input-Output Memory Management Unit
PCIe	Peripheral Component Interconnect Express*
PECI	Platform Environment Control Interface
SRI0-V	Single Root I/O Virtualization

2 VMware ESXi* Setup

2.1 Host BIOS Configuration

Following are the recommended BIOS settings for the Intel Data Center GPU Flex Series card:

1. Memory Mapped I/O Size: Set to 1024G or 2048G** if supported.
2. MMIO High Base: Set to the maximum value supported (36T-56T depending on the system)
3. Memory Mapped I/O above 4 GB: Set to Enabled
4. Advanced → Processor Configuration → Intel® Virtualization Technology: Set to Enabled (if using GVT-D pass-thru or SRIOV virtualization)
5. Intel® Virtualization Technology for Directed IO: Set to Enabled (if using Intel® Graphics Virtualization Technology (Intel® GVT) pass-thru or SRIOV virtualization)
6. SRIOV Support: Set to Enabled (if using SRIOV virtualization) or disabled otherwise.
7. System cooling: Set to maximum/performance mode.

For the Intel M50 CYP Server, the settings may be found in the BIOS configuration under the following paths:

1. Advanced → PCI Configuration → Memory Mapped I/O Size: Set to 1024G.
2. Advanced → PCI Configuration → MMIO High Base: Set to 56T.
3. Advanced → PCI Configuration → Memory Mapped I/O above 4 GB: Set to Enabled
4. Advanced → Integrated IO Configuration → Intel® VT for Directed IO: Set to Enabled
5. Advanced → PCI Configuration → SRIOV Support: Set to Enabled
6. Advanced → System Acoustic and Performance Configuration → Performance
7. Advanced → Processor Configuration → Intel Virtualization Technology: Set to Enabled

Note that the BIOS configuration may vary depending on the host system. Refer to the host system vendor's BIOS configuration guide for specific instructions.

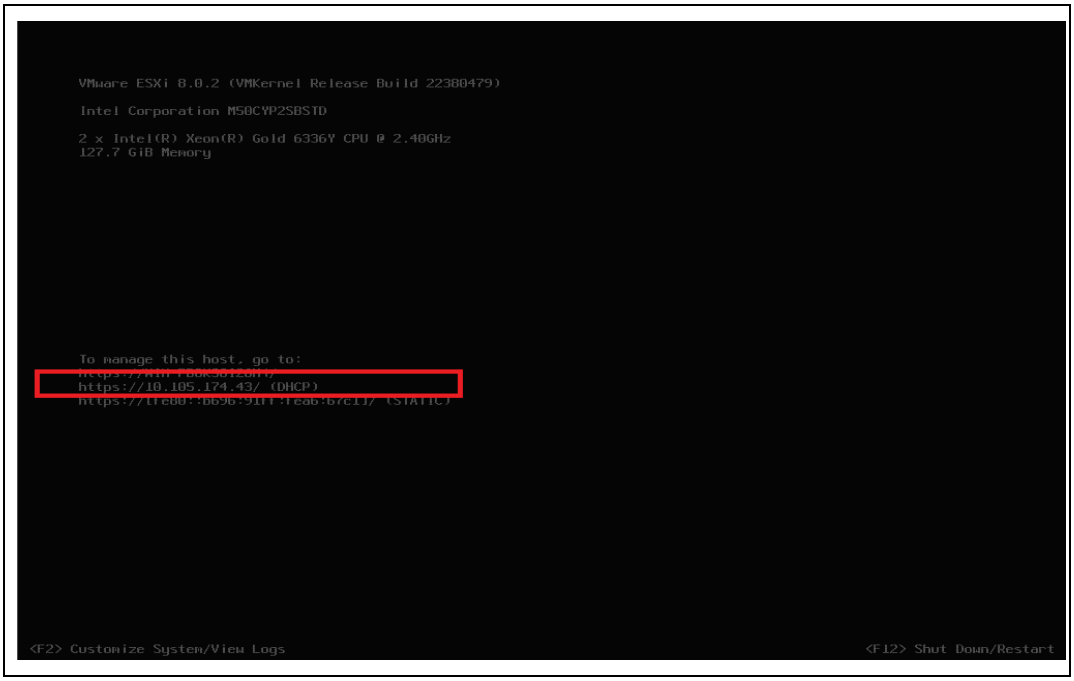
2.2 OS Setup

Download the latest ESXI OS(8.0.2) build which supports Intel® Data Center GPU Flex Series from VMware website.

For ESXi installation refer the set-up guide:
https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-esxi-801-installation-setup-guide.pdf

After ESXI is successfully installed, note down the IP address of the server.

Figure 2-1. Screenshot with IP Address



2.3 Enable SSH

2.3.1 Enable SSH through UEFI

Enable SSH on ESXi via DCUI (Direct Console User Interface)

1. Log in to the ESXi host console directly or through a remote console session.

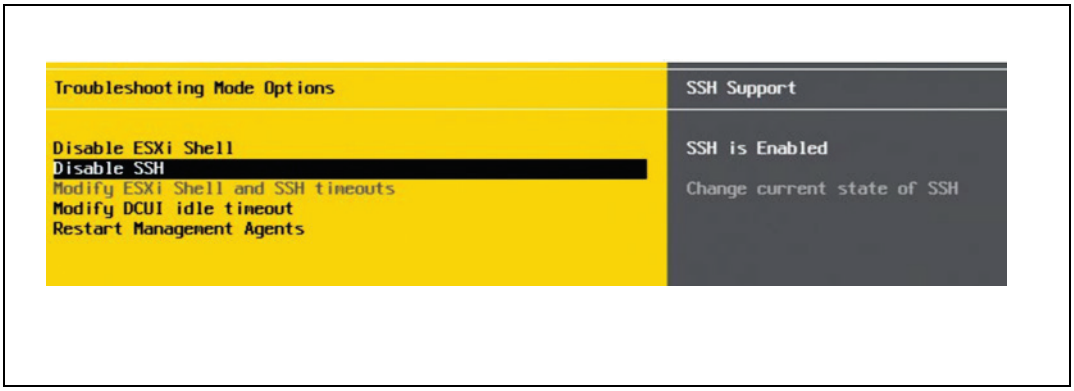
Figure 2-2. Screenshot with Authentication

2. Navigate to the "Troubleshooting Options" menu.

Figure 2-3. Screenshot with Troubleshooting Options

3. Within the Troubleshooting Options menu, locate the option for SSH and select it.

Figure 2-4. Screenshot with SSH Options menu



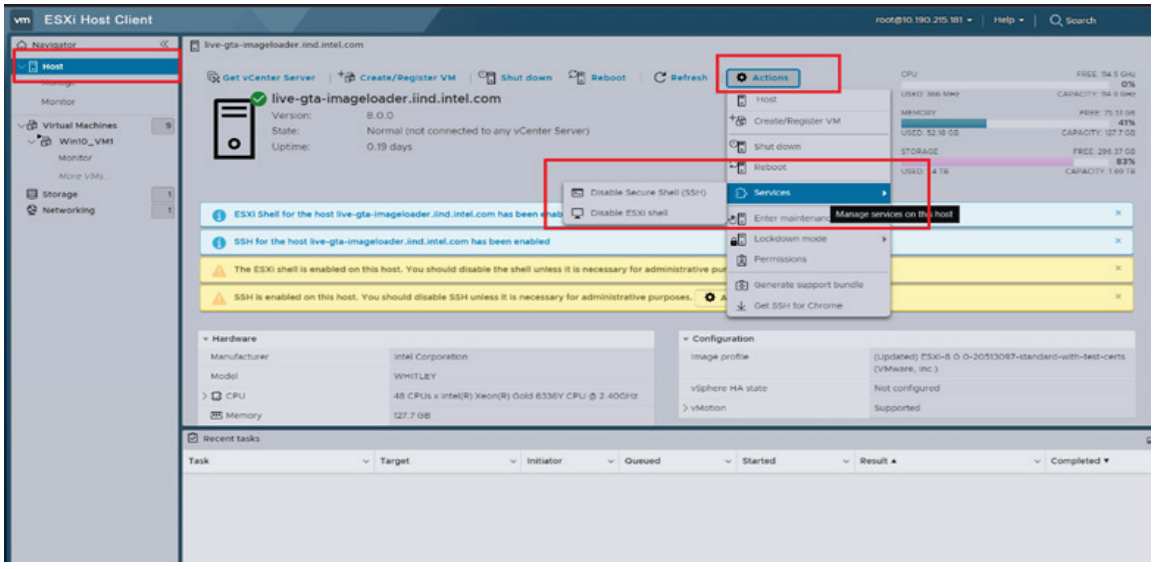
4. Check SSH status, if it is disabled, click enter to enable.
5. After enabling SSH, confirm your selection and save the changes.
6. Exit the DCUI interface.

2.3.2 Enable SSH through ESXi Host Web Client

To establish a connection to the ESXi host, SSH and ESXi Shell must be enabled. Follow these steps:

1. Open the ESXi Host WebClient.
2. Click on the 'Host' tab and then select the 'Actions' button.
3. Next, click on 'Services.' A dropdown menu will appear, allowing you to enable SSH and ESXi Shell.

Figure 2-5. Screenshot with Web Client



2.4 Installing Intel Data Center Graphics Driver for VMware ESXi Host

1. Download the ESXI PF driver and Idcgputools package from Intel public website.
   https://www.intel.com/content/www/us/en/download/786751/intel-data-center-graphics-driver-for-vmware-esxi.html

2. Open a secure shell (SSH) connection to the target ESXi host (SSH needs to be enabled to perform this operation).
3. Put the system in maintenance mode.

   esxcli system maintenance Mode set -e=1

1. Copy the driver component package to the ESXi server '/tmp' folder.

Here is an example of using the Linux* `scp` utility to copy the file from the downloaded location to the remote/target ESXi server located at 10.10.10.10:

   scp *-idcgpu-*.zip root@10.10.10.10:/tmp

2. Copy the esxcli plugin component to the ESXi server.

   scp *-idcgputools-*.zip root@10.10.10.10:/tmp

3. Install the idcgpu component.

   esxcli software component apply --no-sig-check -d /tmp/*-Intel-idcgpu-*.zip

   Note: This step can take some time (30+ seconds).

4. Install the idcgputools component.

   esxcli software component apply --no-sig-check -d /tmp/*-Intel-idcgputools-*.zip

5. Reboot the system to complete driver installation:

   reboot

6. If the Intel® Data Center Graphics Driver loaded without errors, the idcgpu module is present in the list of system modules:

   esxcfg-module -l | grep idcgpu
   idcgpu 0 4868

7. If the idcgputools component is installed correctly, then 'intdcgpu' namespace is present when `esxcli` is run.

8. Exit maintenance mode.

   esxcli system maintenanceMode set -e=0

2.5 Uninstalling Driver

1. Open an SSH connection to the target ESXi host.
2. Shut down all running VMs.
3. Uninstall the idcgputools component.

   esxcli software component remove -n Intel-idcgputools

4. Uninstall the idcgpu component.

   esxcli software component remove -n Intel-idcgpu

5. Reboot the system to complete the removal process.

   reboot

2.6 Profile Map

The following table defines the available profiles for Flex 140 and Flex 170 cards.

The following are the available profiles for Intel Data Center GPU Flex 140 and Flex 170.

For more details refer to the Intel Datacenter GPU Series for VDI document solution: https://www.intel.com/content/www/us/en/products/docs/discrete-gpus/data-center-gpu/flex-series/vdi-solution-brief.html

Table 2-1. FLEX 140 Cards Supported Profiles

Profile Name	Profile ID	VFs /SOC		Memory per VF(MB)	
		Min	Max	ECC On	ECC off
ATSM75_V1	2	1	1	4198	5120
ATSM75_V3	3	1	3	1398	1706
ATSM75_V6	4	1	6	698	853

Illustration: with 1x Flex 140 card which has two SOCs, up to 12 VFs are supported using ATSM75-V6 Profile,

Table 2-2. FLEX 170 Cards Supported Profiles

Profile Name	Profile ID	VFs /SOC		Memory per VF (MBs)	
		Min	Max	ECC On	ECC Off
ATSM150_V1	2	1	1	12902	15360
ATSM150_V2	3	1	2	6450	7680
ATSM150_V4	4	1	4	3224	3840
ATSM150_V5	5	1	5	2580	3072
ATSM150_V8	6	1	3	1612	1920
ATSM150_V16	7	1	16	806	960

Illustration: with 1x Flex 170 card which has 1 SOCs, up to 16 VFs are supported using ATSM150_V16 Profile,

2.7 ECC configuration

ECC on provides additional data integrity protection by detecting and correcting errors in GPU memory, while ECC off may increase the GPU performance.

1. Enable maintenance mode for system updates:
   esxcli system maintenanceMode set -e=1

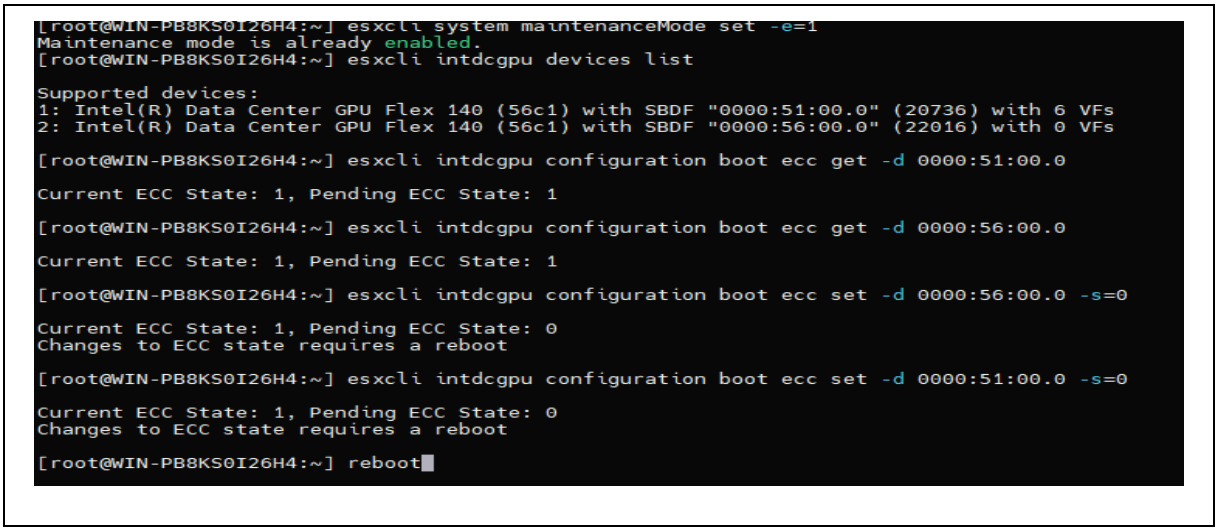
2. Display the list of Flex 140 devices:
   esxcli intdcgpu devices list

   For illustration purposes, let's assume the following Flex 140 devices:
   - Intel(R) Data Center GPU Flex 140 (56c1) with SBDF "0000:51:00.0" (20736) with 0 VFs
   - Intel(R) Data Center GPU Flex 140 (56c1) with SBDF "0000:56:00.0" (46848) with 0 VFs

3. Verify ECC status on each GPU:
   -d: The bus ID of the PCI device (e.g., 0000:51:00.0) (required)
   -s: The ECC state to be set on a device. Host needs a reboot for this setting to take effect (required)
   -s=0: Disable ECC on
   -s=1: Enable ECC on
   esxcli intdcgpu configuration boot ecc get -d 0000:51:00.0
   esxcli intdcgpu configuration boot ecc get -d 0000:56:00.0

4. Disable ECC on each Flex GPU:
   esxcli intdcgpu configuration boot ecc set -d 0000:51:00.0 -s=0
   esxcli intdcgpu configuration boot ecc set -d 0000:56:00.0 -s=0
5. Enable ECC on each Flex GPU
   esxcli intdcgpu configuration boot ecc set -d 0000:51:00.0 -s=1
   esxcli intdcgpu configuration boot ecc set -d 0000:56:00.0 -s=1
6. ECC state changes require a system reboot. Perform a system reboot.
reboot

Figure 2-6. Screenshot with Authentication



2.8 Profile Configuration

Profile configuration for the Flex GPU can be accomplished through two methods.

2.8.1 Profile Configuration via Module Parameters

7. List Available Module Parameters:
   exclaim system module parameters list -m idcgpu
8. Clear Existing Module Parameters:
   esxcli system module parameters clear -m idcgpu
9. Set Parameters Using Command:
   esxcli system module parameters set -m idcgpu -a -p "<param_name>=<param_value(s)>"
10. List Devices:
    Each device is identified with an ID for parameter targeting.
    Example:

esxcli intdcgpu devices list
1: Intel Data Center GPU Flex 140 (56c1) with SBDF "0000:46:00.0" (17920) with 1 VFs
2: Intel Data Center GPU Flex 140 (56c1) with SBDF "0000:4a:00.0" (18944) with 0 VFs

To configure devices via module parameters:

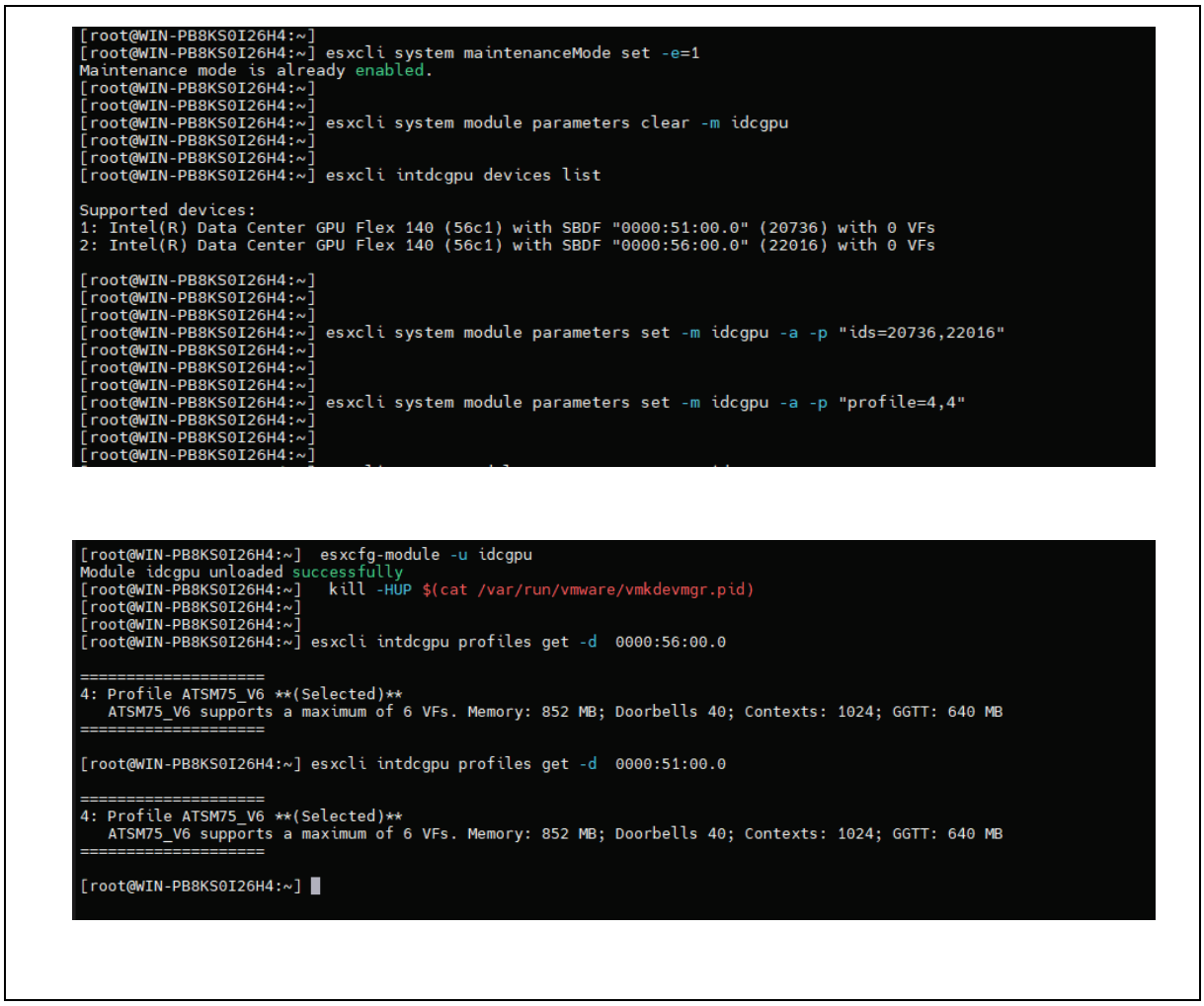
esxcli system module parameters set -m idcgpu -a -p "ids=17920,18944"

esxcli system module parameters set -m idcgpu -a -p "profile=1,1"

11. Reload Driver:
    Execute the following commands to apply changes immediately:

esxcfg-module -u idcgpu # unloads module if already running.
kill -HUP $(cat /var/run/vmware/vmkdevmgr.pid)

Figure 2-7. Screenshot with Module Parameter



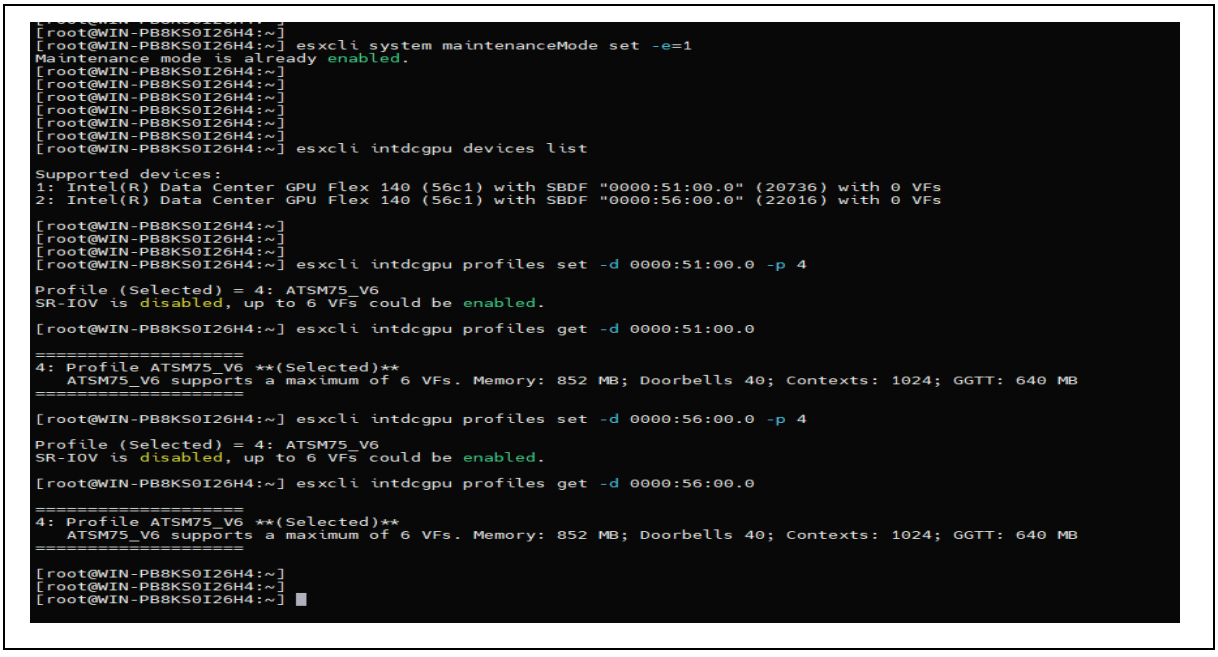
2.8.2 Profile Configuration Using `intdcgpu`

To configure profiles using the Intel `intdcgpu` tool, follow these steps. Please note that configurations made using this method are not persistent and will be removed upon server reboot or idcgpu reload:

1. Get Device List:
   esxcli intdcgpu devices list
2. Specify Desired Profile:
   esxcli intdcgpu profiles set -d <device id> -p <profile number>
   profile number: specified in Section 2.5 Profile Map
   Example : esxcli intdcgpu profiles set -d 0000:bc:00.0 -p 2
3. Verify Selected Profile:
   esxcli intdcgpu profiles get -d <device id>
   Example : esxcli intdcgpu profiles get -d 0000:bc:00.0

These commands allow you to list the available devices, set a desired profile for a specific device, and verify the selected profile respectively.

Figure 2-8. Screenshot with intdcgpu

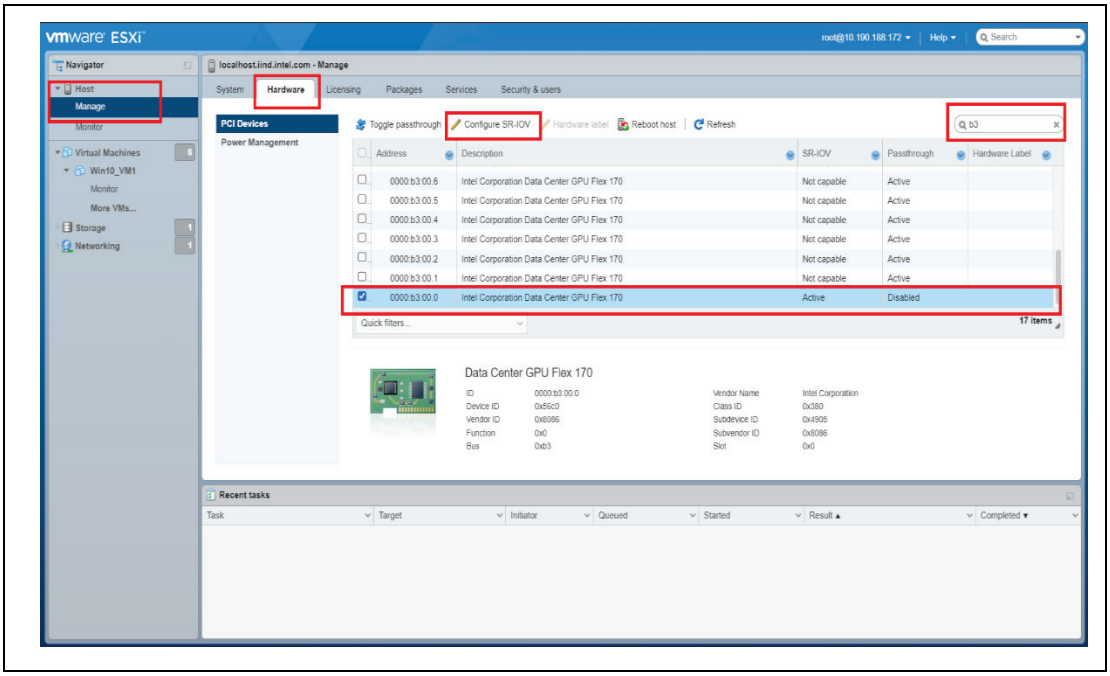


3 Enabling SR-IOV VFs for VMware ESXi Host

3.1 Enabling SR-IOV

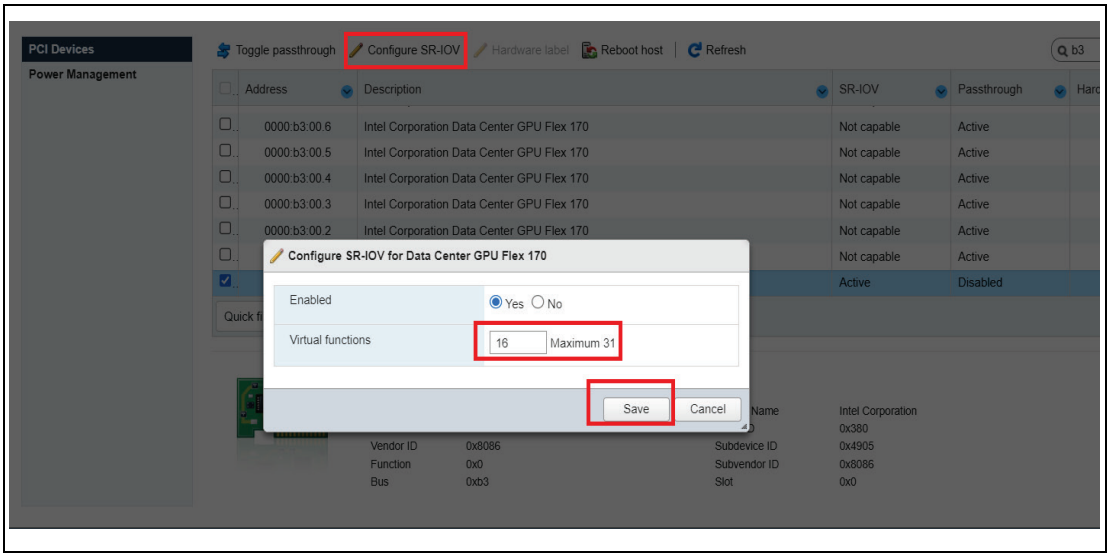
1. Access ESXi Host UI:
   - Log in to the ESXi Host UI.
   - Navigate to 'Host' → 'Manage' → 'Hardware' tab.

Figure 3-1. VMWare ESXi Window



2. Configure SR-IOV:
   a. Click on 'Configure SR-IOV'.
   b. A small window will pop up.
   c. Specify the number of VFs to be created, ensuring a 1:1 mapping between VFs and VMs.
   d. Click 'Save' and refresh the ESXi Host Page.

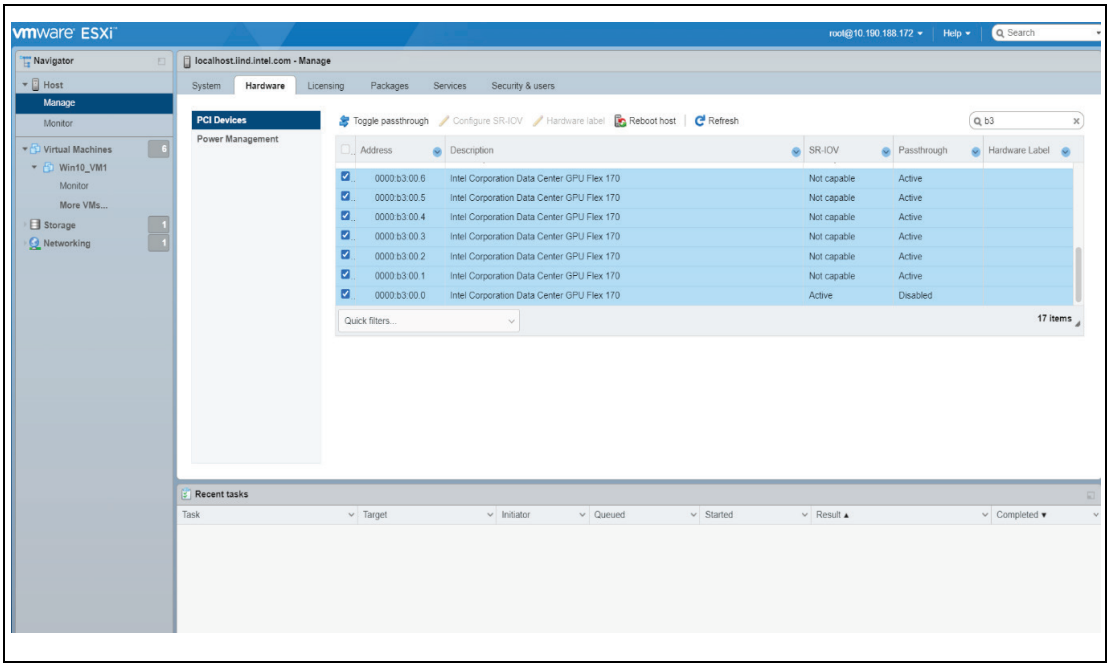
Figure 3-2. Configure SR-IOV for Data Center GPU Flex 170



3. Verify VF Creation:

If VF creation is successful, the BDF (Bus, Device, Function) details of all the VFs will be listed.

Figure 3-3. Hardware PCI Devices



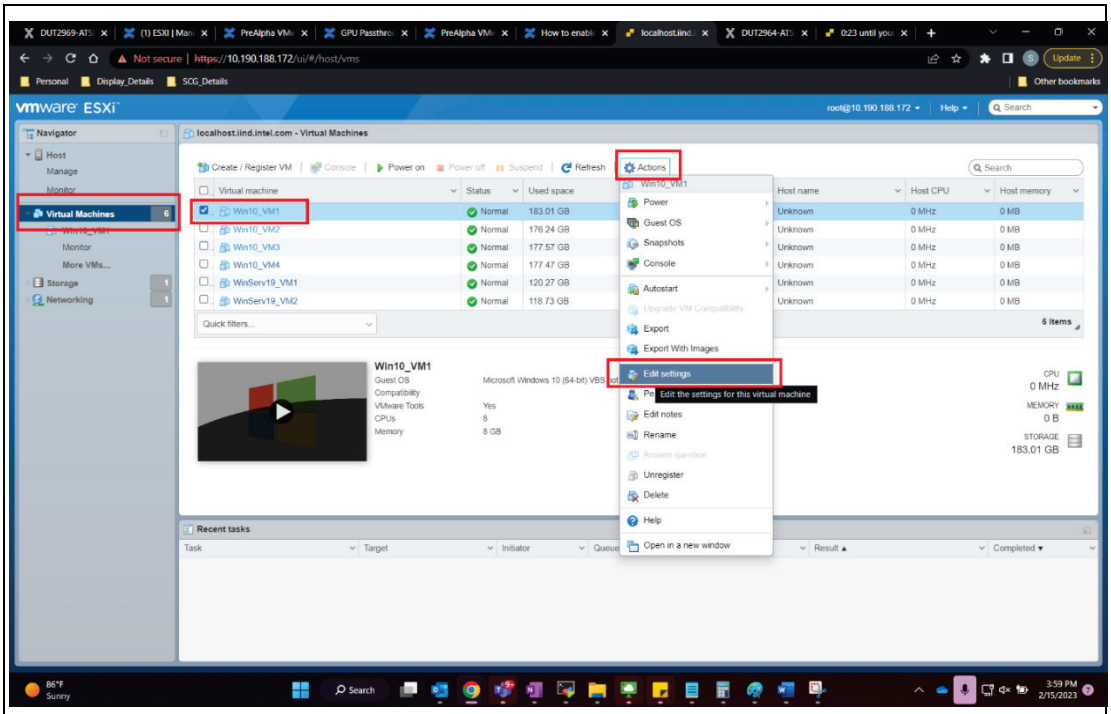
Attaching VFs to VMs:

1. Power Off VMs:
    a. Under 'Virtual Machines', power off all VMs if they were previously powered on.
2. Edit VM Settings:
    a. Select each VM.

b. Click on the 'Actions' button → 'Edit Settings'.

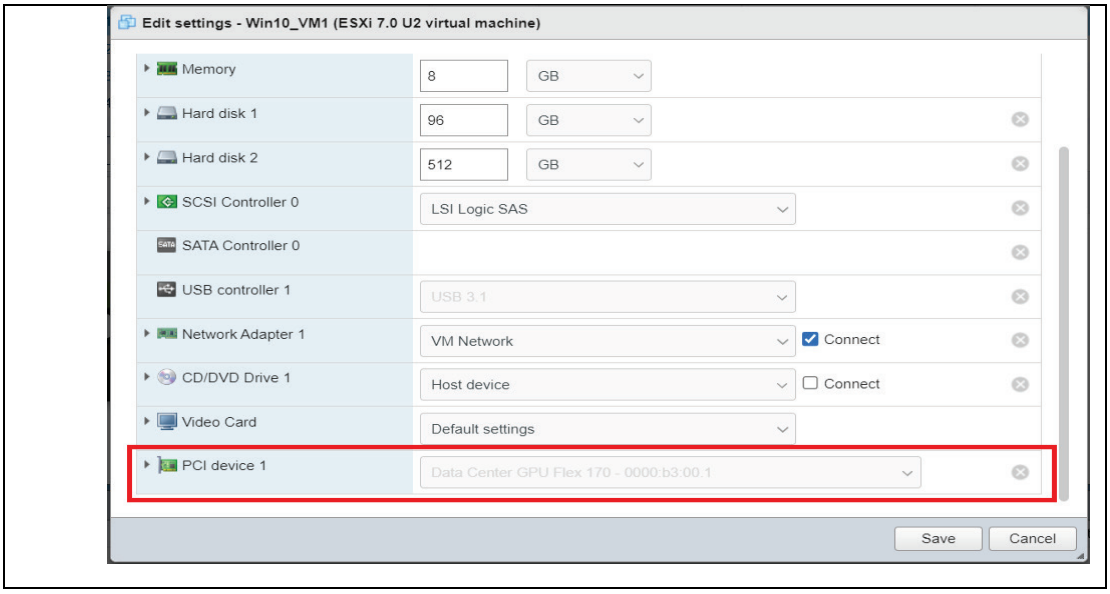
c. The PCI details will appear.

Figure 3-4. Virtual Machines Window



3. Attach VFs to VMs:
   a. Review the PCI details.
   b. Click 'Save' for each VM to attach VFs.
   c. Repeat the process for all intended VMs.
4. Refresh UI and Power On VMs:
   a. Refresh the ESXi UI page once all VFs have been attached.
   b. Power on all VMs.
   c. Log in to each VM using the respective IP address using any remote agents.

Figure 3-5. Edit Settings – Win10_VM1 (ESXi 7.0 U2 virtual machine)



3.2 Pass-through the VF PCI Device

Here are the steps to attach Intel® GPU Flex VFs to a virtual machine in VMware ESXi:

1. Log in to the target ESXi host via vSphere Host Client.
2. In the left pane, click on "VMs."
3. In the center pane, click on the desired Virtual Machine. Ensure that the VM is powered off.
4. To edit the virtual machine's settings, click "Edit." A pop-up window with the VM settings appears.
5. Click "Add other Device" and select "PCI device."
    a. The new PCI device has been added. By default, it selects the first VF in the system, which may not be an Intel® GPU Flex VF since there could be other PCI devices in the system.
    b. To select an Intel® GPU Flex VF, click the drop-down list and choose the desired PCI device with "GPU Flex" in the name. The BDFs listed here match the output of the `lspci | grep -i display` command. Add additional VFs by repeating this step.
6. All memory for the VM must be reserved. Expand "Memory" and set "Reserve all guest memory (All locked)" checkbox.
7. Click "Save."
8. To edit the virtual machine's settings, click "Edit."
9. Click the "VM Options" tab in the pop-up window.
10. Click the "Advanced" row to be expanded.

11. Click "Edit Configuration." A "Configuration Parameters" pop-up displays.
12. Click "+ Add parameter". A new row is inserted at the bottom, populated with the following text, "Click to edit key."
13. Enter "pciPassthru.use64bitMMIO" in the key box.
14. Enter "True" in the Value field on the right.
15. Repeat step 'f' and return here.
16. Enter "pciPassthru.64bitMMIOSizeGB" in the key box.
17. Enter "64" in the Value field on the right.
18. To dismiss the pop-up, click OK.
19. To commit the changes, click Save.

Now the server has one or more VFs attached to your guest, and the VM is ready to be powered on.

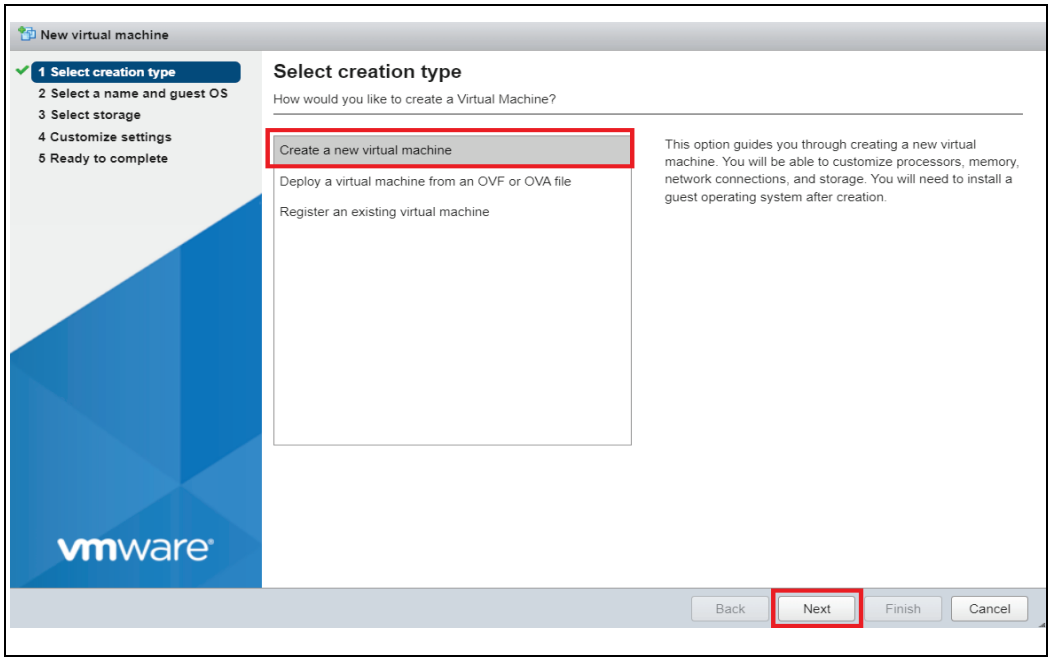
4 Citrix* VM Setup

This section contains information and instructions for setting up VMware VM.

4.1 Installing Windows* Enterprise OS

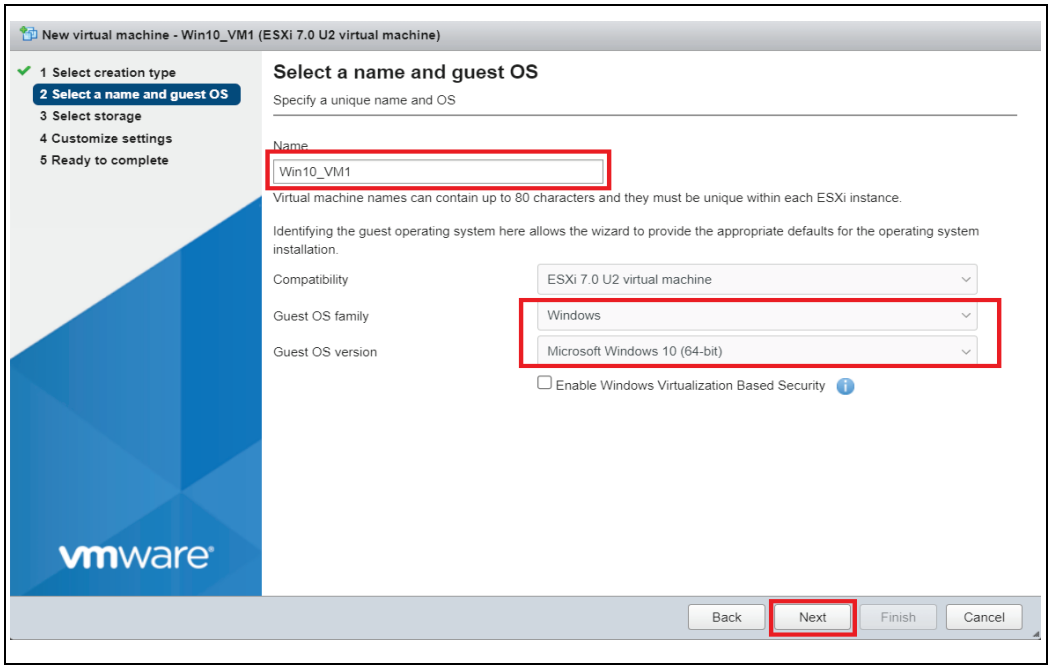
1. Initiate VM Creation:
   In the system where VF creation and provisioning are completed, click on 'Create a new virtual machine' and click Next.

Figure 4-1. New Virtual Machine Select Creation Type Window



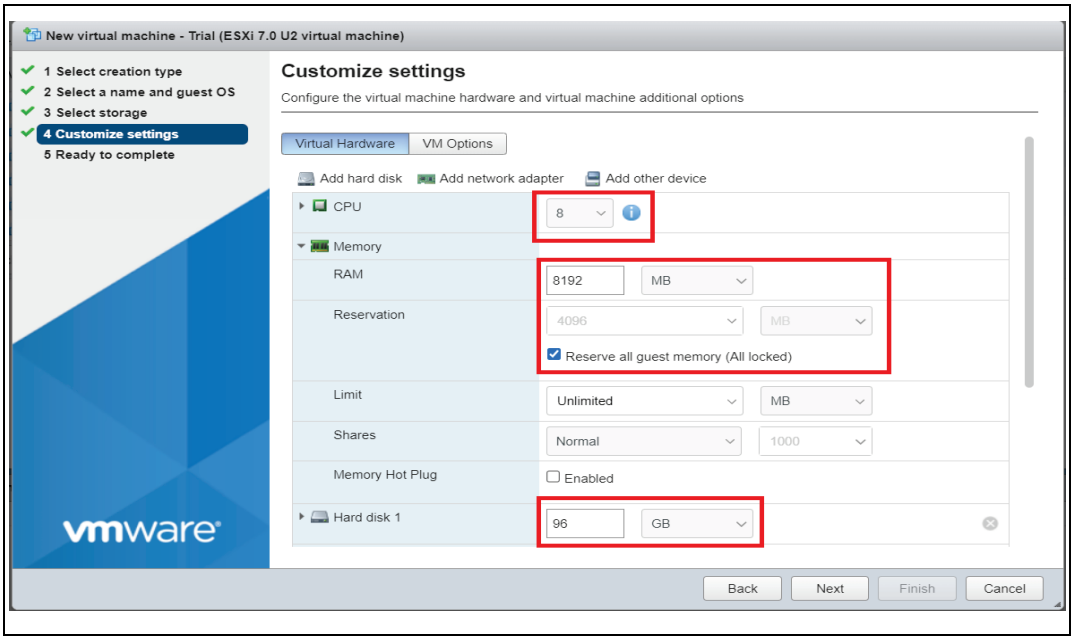
2. Specify VM Details:
   Provide an appropriate name for the VM and choose the OS details.

Figure 4-2. New Virtual Machine Select a name and Guest OS



3. Storage Configuration:
    - Choose the appropriate storage details in the next tab and click 'Next'.

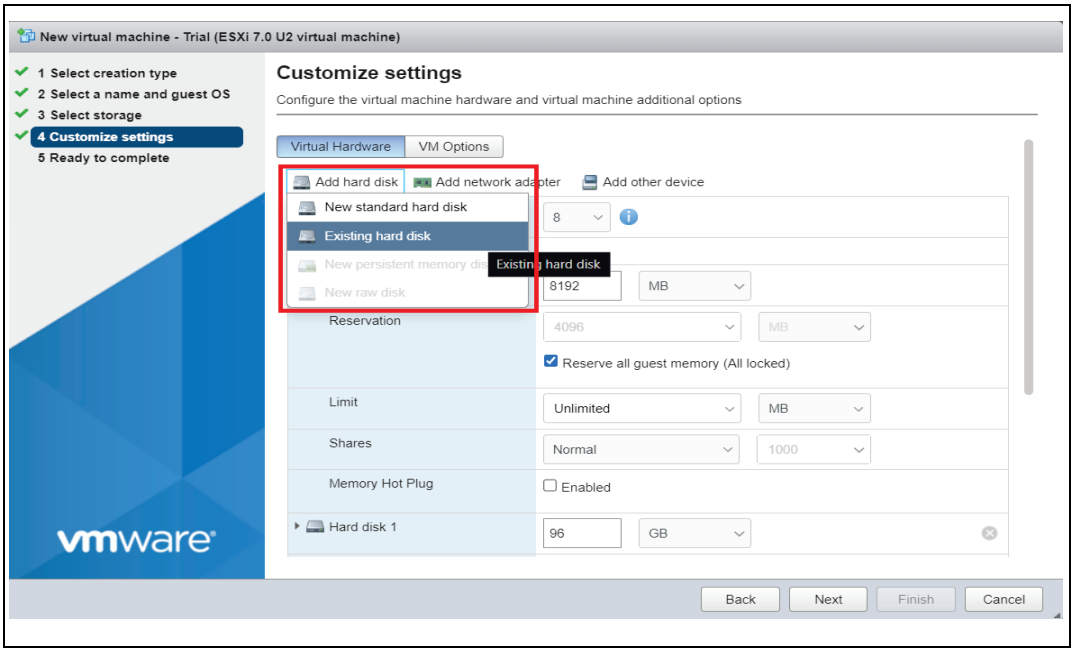
Figure 4-3. New Virtual Machine Customize Settings



4. Customize Virtual Hardware:
   In the 'Customize Settings' page under the 'Virtual Hardware' tab:
   Attach the thin vmdk image that has been created by clicking on 'Add Hard Disk' → 'Add Existing Hard disk'.

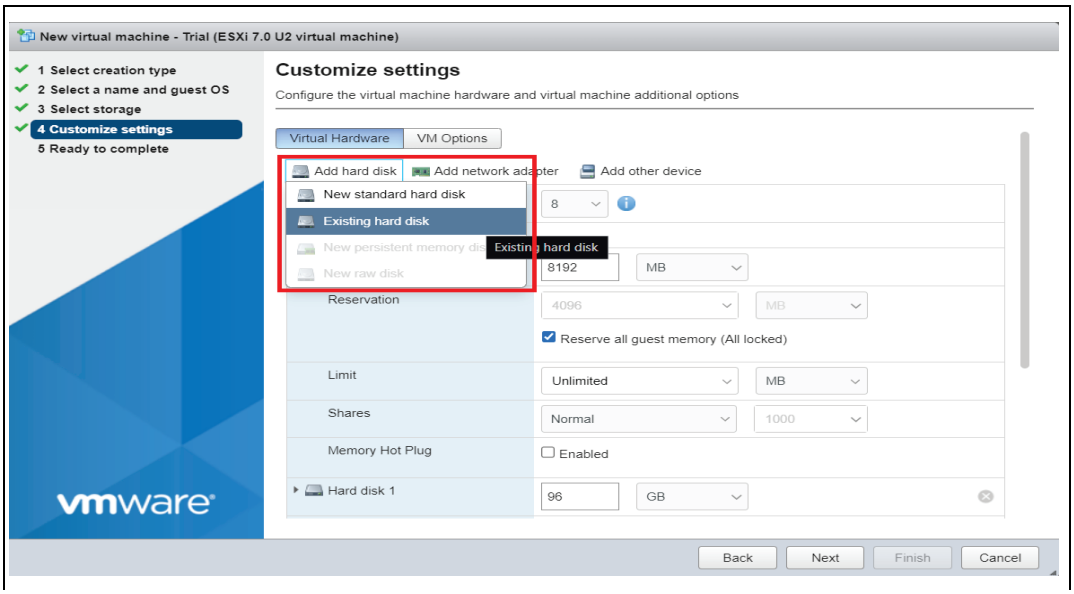
- Click on the 'VM Options' and update the highlighted options under 'Boot Options' and 'Advanced' options.
- Click on 'Edit Configuration' to open a new window.

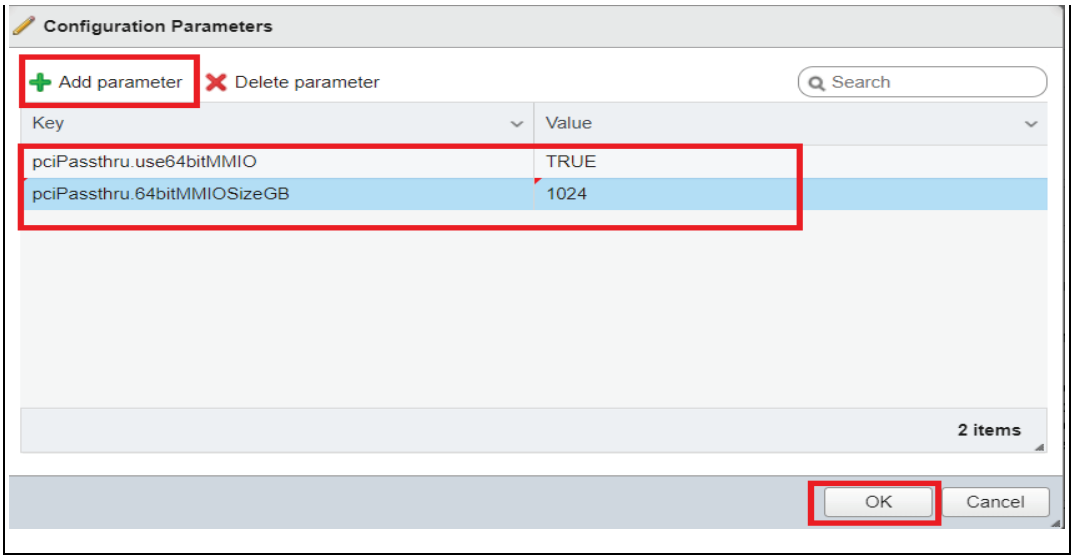
Figure 4-4. Customize settings – existing hard disk



5. Edit Configuration:
   In the new window, click on 'Add Parameter'.
   Add the following key-value pairs:
   p**ciPassthru.use64bitMMIO=TRUE**
   pciPassthru.64bitMMIOSizeGB=1024

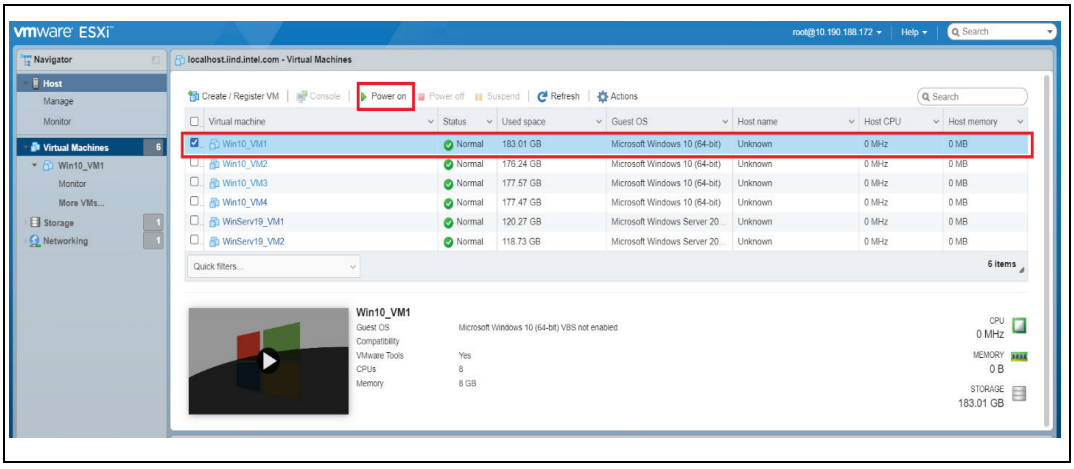
Figure 4-5. Customize settings – existing hard disk: Configuration Parameters





2. **Finalize VM Creation**:
    - Click 'Next' and 'Finish' to complete the VM creation process.
3. **Power On VM**:
    - After the VM is successfully created, it will appear in the list.
    - Click on 'Power On' to login to the VM.

Figure 4-6. Virtual Machines – Power On



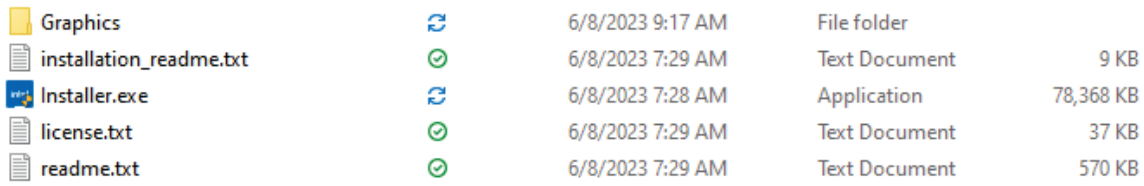
5 Guest OS Setup

5.1 Guest OS Driver Setup

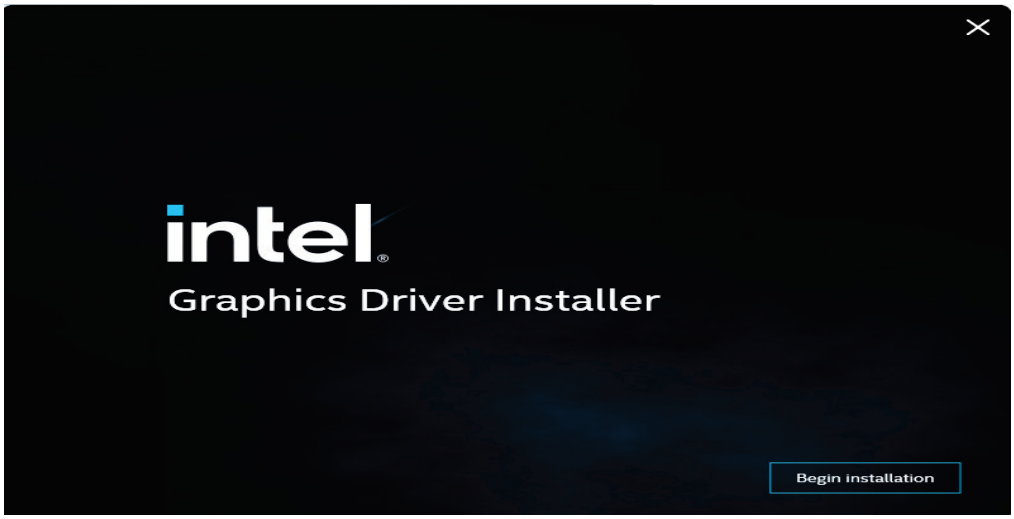
Download Windows Graphics Driver from Intel website to the Guest VM and follow steps:

https://www.intel.com/content/www/us/en/download/780185/intel-data-center-gpu-flex-series-windows.html

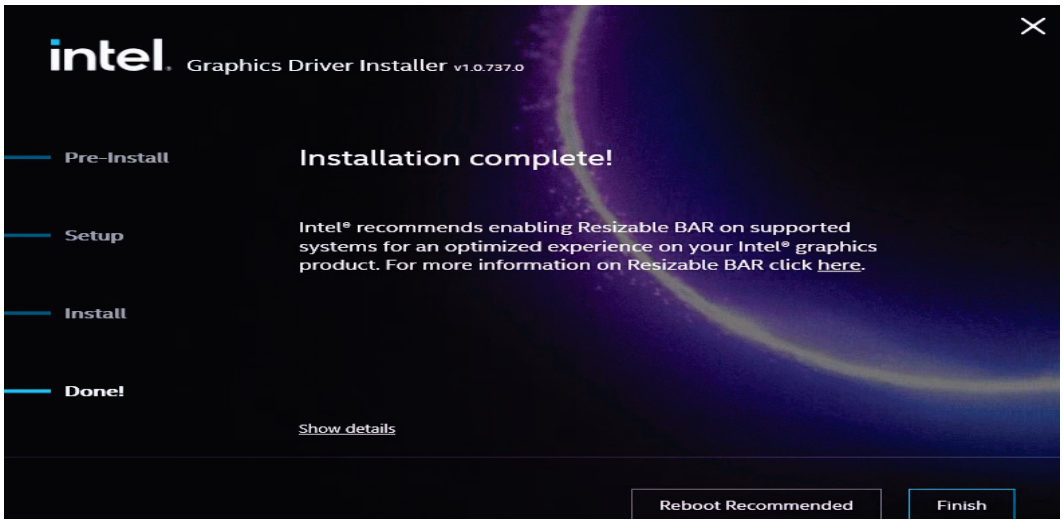
1. Unzip the windows driver and double click Installer.exe



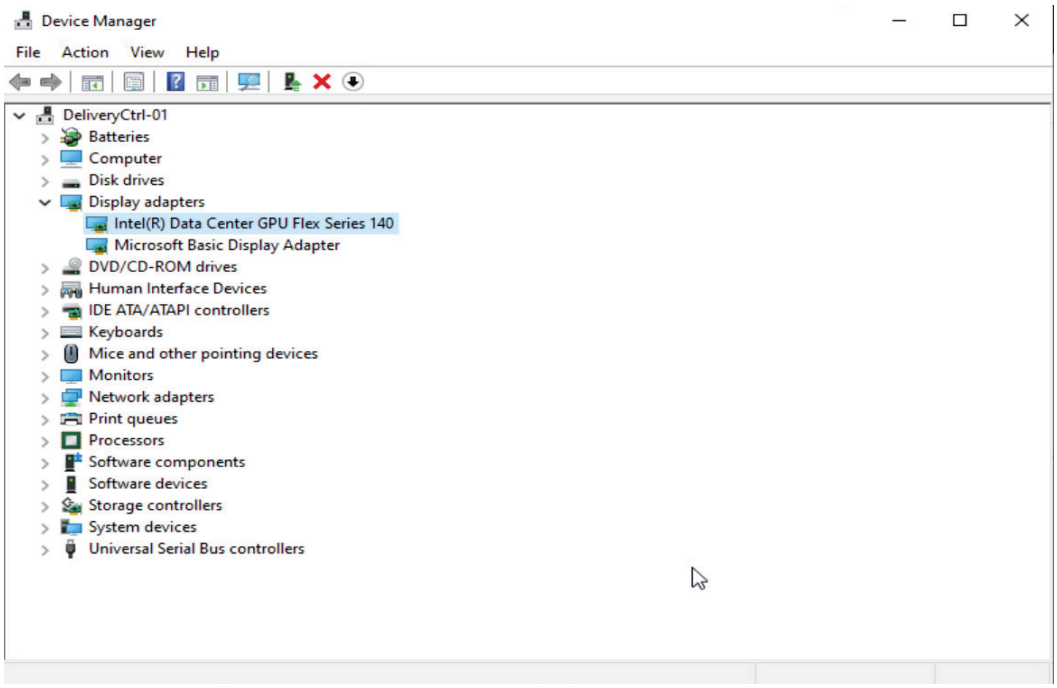
2. Click Begin Installation button:



3. Once driver Installation completes, Reboot the VM


intel Graphics Driver Installer v1.0.737.0
Pre-Install
Setup
Install
Done!
Installation complete!
Intel® recommends enabling Resizable BAR on supported systems for an optimized experience on your Intel® graphics product. For more information on Resizable BAR click here.
Show details
Reboot Recommended
Finish

4. After Reboot, assigned Intel Graphics card can be verified from Display Adapters in the device manager:



6 Citrix Virtual Apps and Desktops configuration

The following sample Citrix* Virtual Apps and Desktops configuration explain about how to virtualize the apps and Desktops.

The sample configuration is not a best practices configuration and uses minimal virtual machines for testing and validation purposes only. For a complete setup guide for Citrix Virtual Apps and Desktops, refer to the Citrix documentation pages: https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/install-configure

In the sample configuration 3 VMs are used:

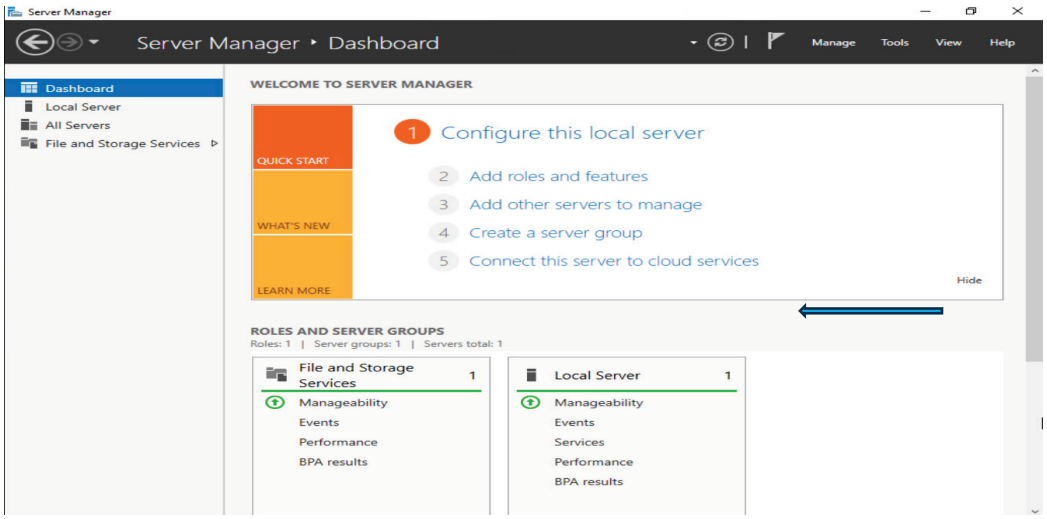
1. Active Directory Domain controller.
2. Citrix Delivery Controller. Citrix recommends using CVAD 2311 and onward for use with Intel Flex Datacenter GPUs.
3. Virtual Delivery Agent (VDA)

6.1 Active directory Domain controlled setup

Follow the steps to install the Active Directory

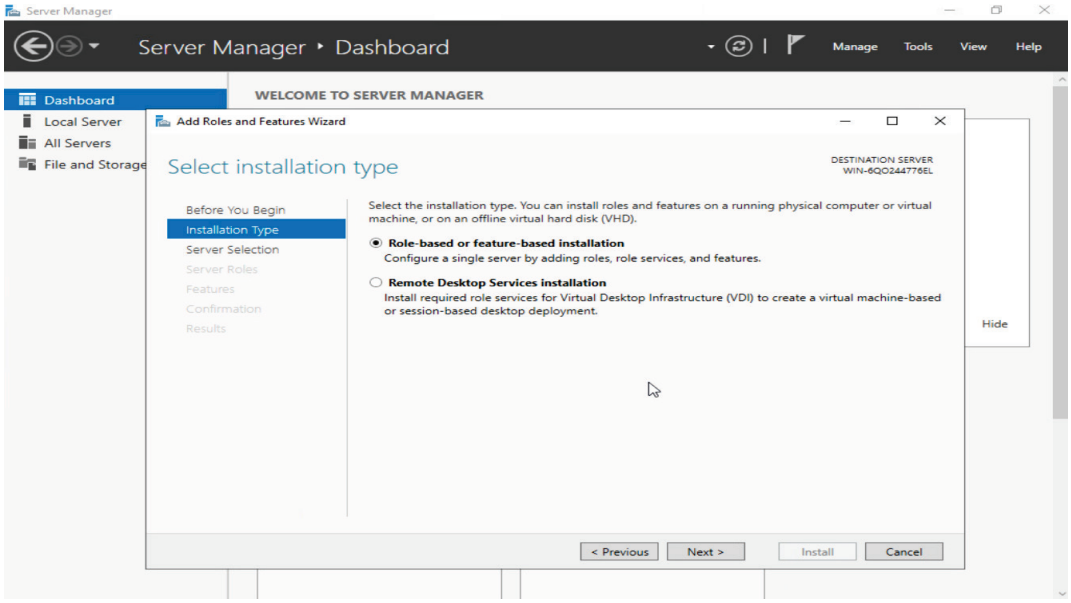
1: Open the Server Manager and select Add Roles and Features which proceeds with the Active Directory installation. Click on “Next.”

Figure 6-1. Screenshot with Server Dashboard



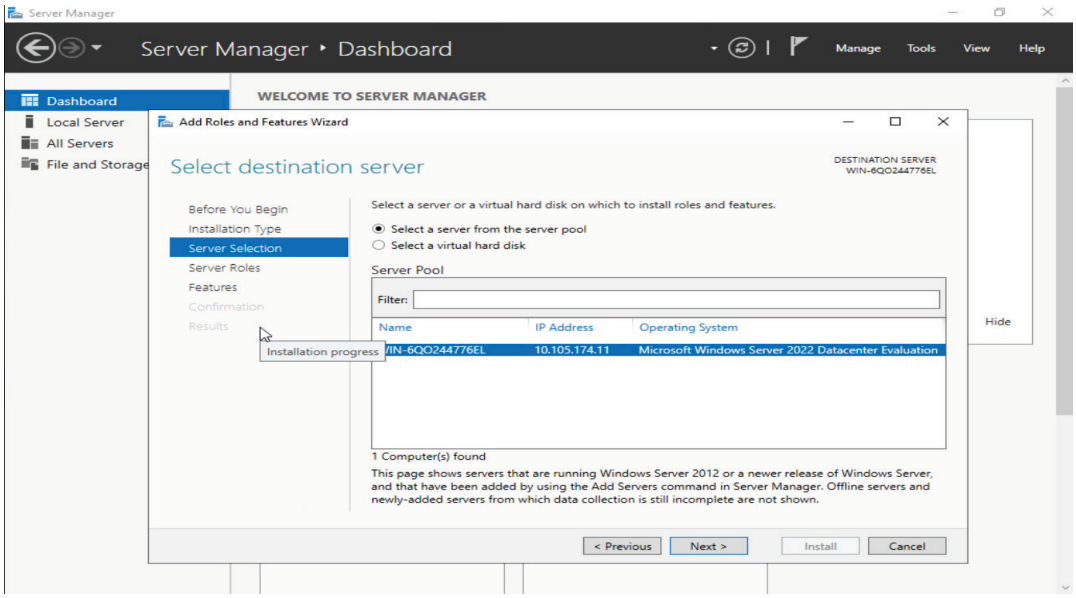
2: Select Role-based or feature-based installation and Click Next.

Figure 6-2. Screenshot with Add Roles and Features Wizard



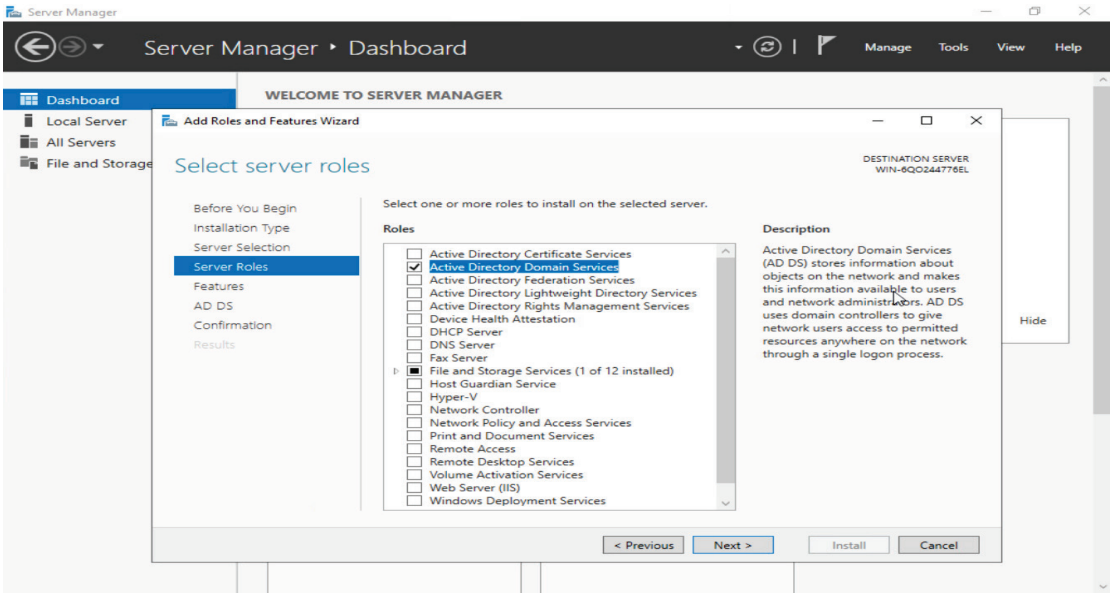
3: Select a server from the server pool and select a server and click next.

Figure 6-3. Screenshot with Add Roles and Features Wizard



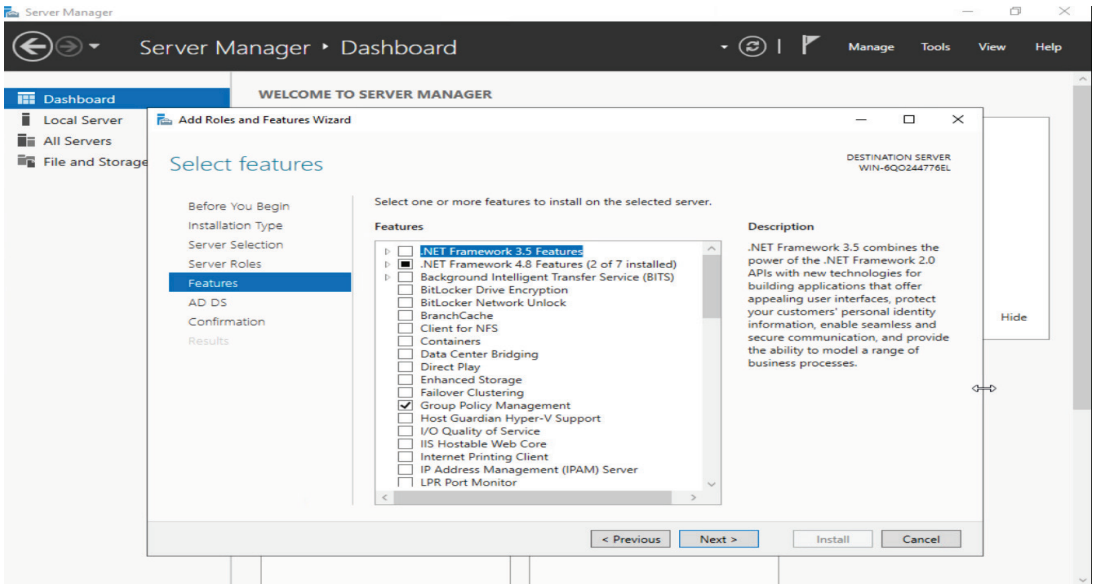
4: Select Active Directory Domain Services and click Next.

Figure 6-4. Screenshot with Select Server Roles



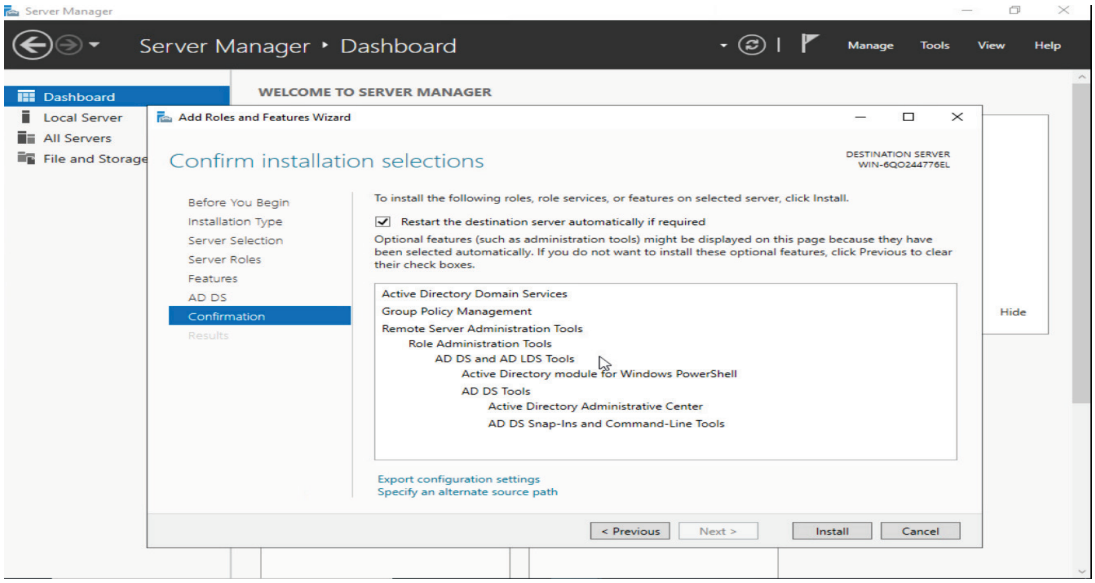
5: Select Group policy Management and click Next.

Figure 6-5. Screenshot with Group policy Management



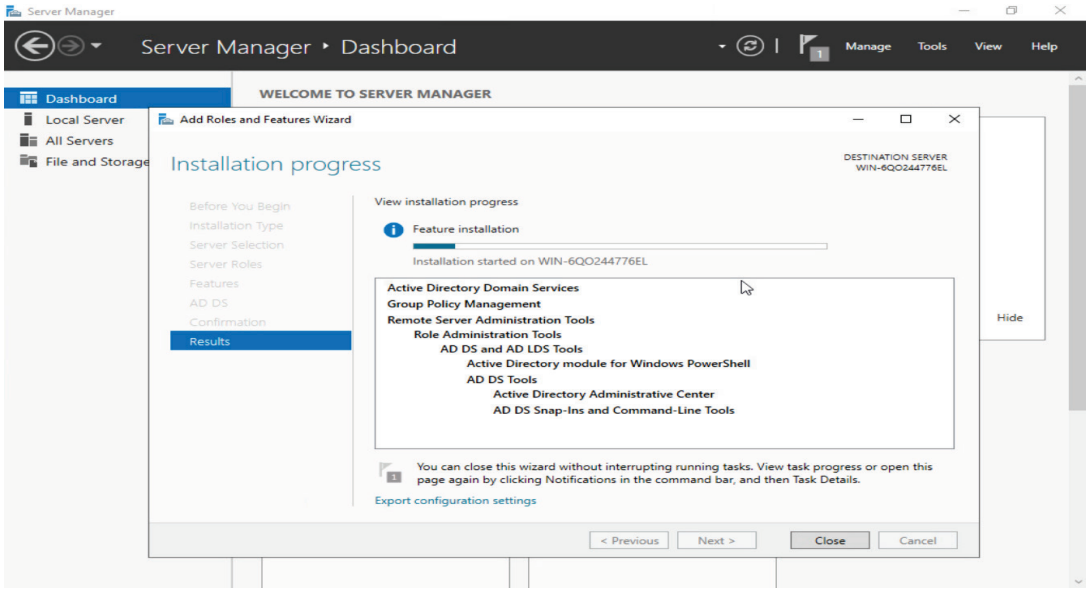
6: Select Restart the destination server automatically if required and click install.

Figure 6-6. Screenshot with Confirm Installation Selections



7: Once installation is complete, click close.

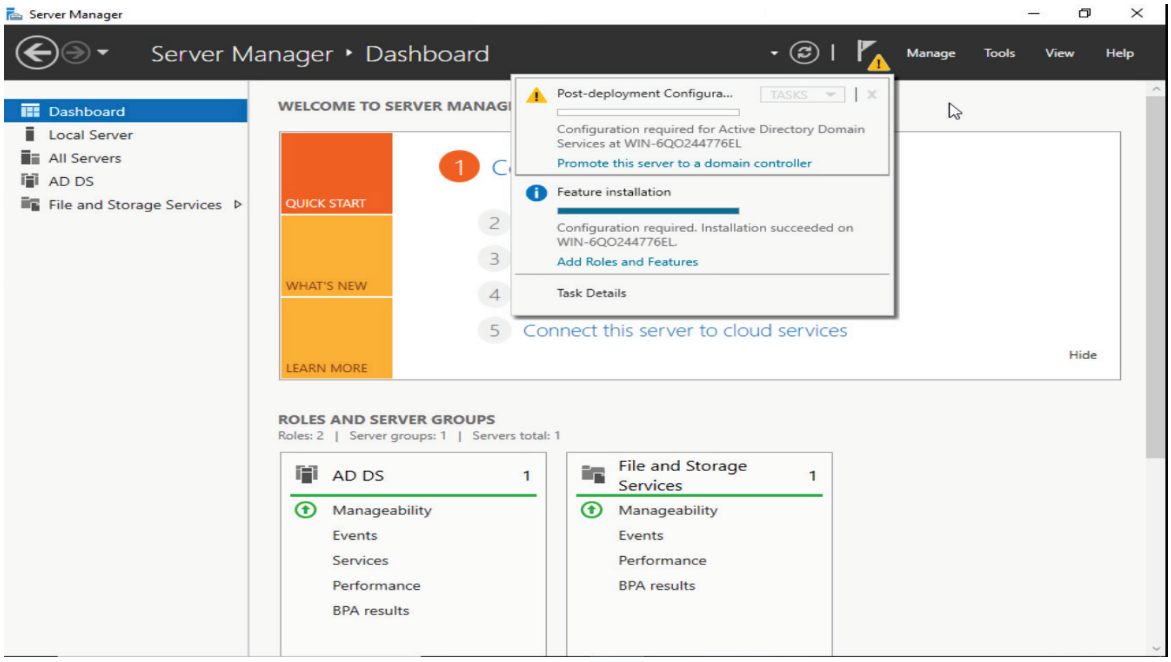
Figure 6-7. Screenshot with installation progress



8: Configure Active Directory Domain Services

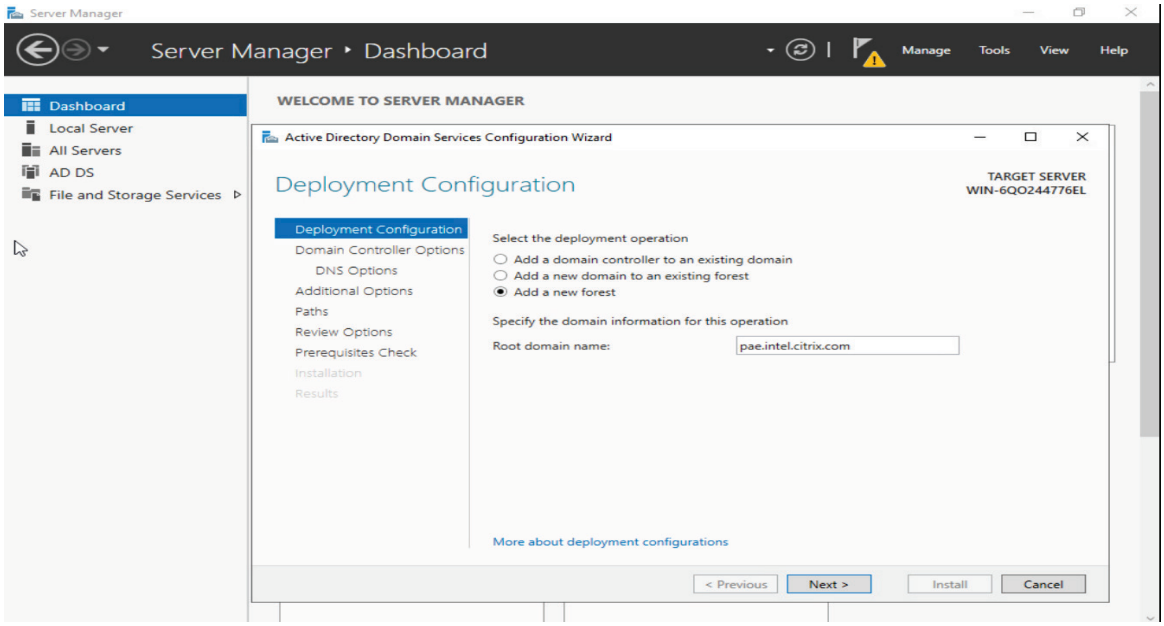
Locate the "Manage" tab with yellow exclamation. Click on it and select "Promote this server to a domain controller".

Figure 6-8. Screenshot with post-deployment Configuration



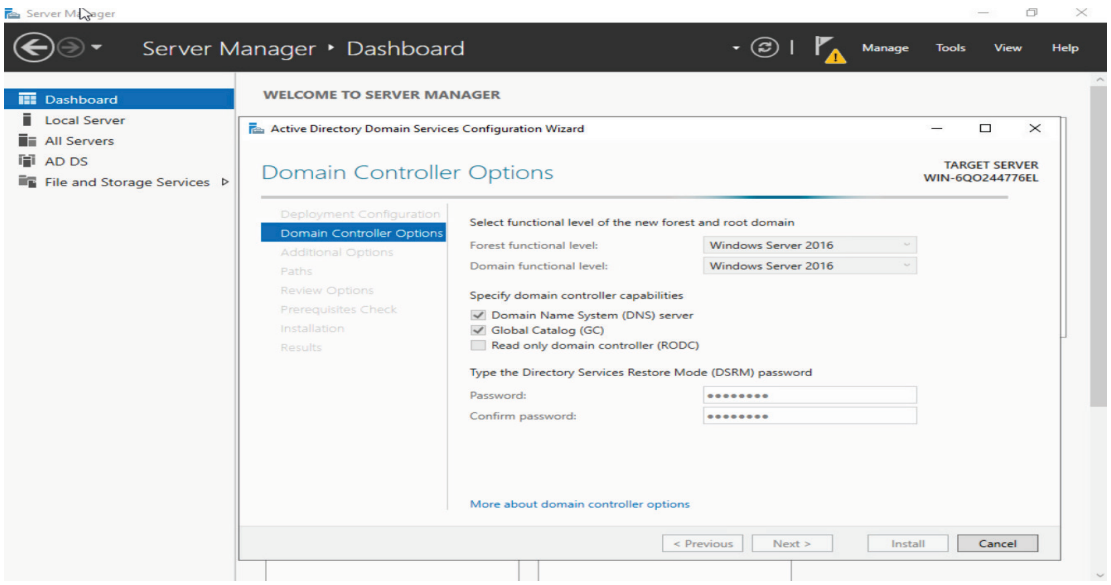
9: Select Add a new forest and enter forest name.

Figure 6-9. Screenshot with forest name selection



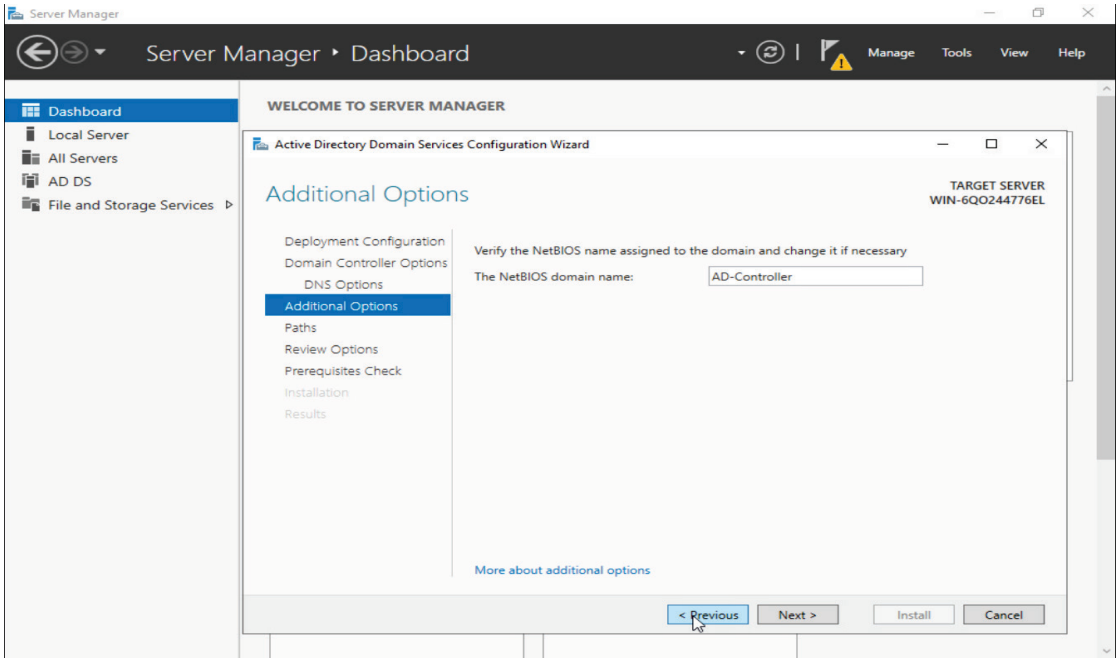
10: Enter Password and confirm Password, and click next, ignore Create DNS delegation.

Figure 6-10. Screenshot with Domain Controller Options



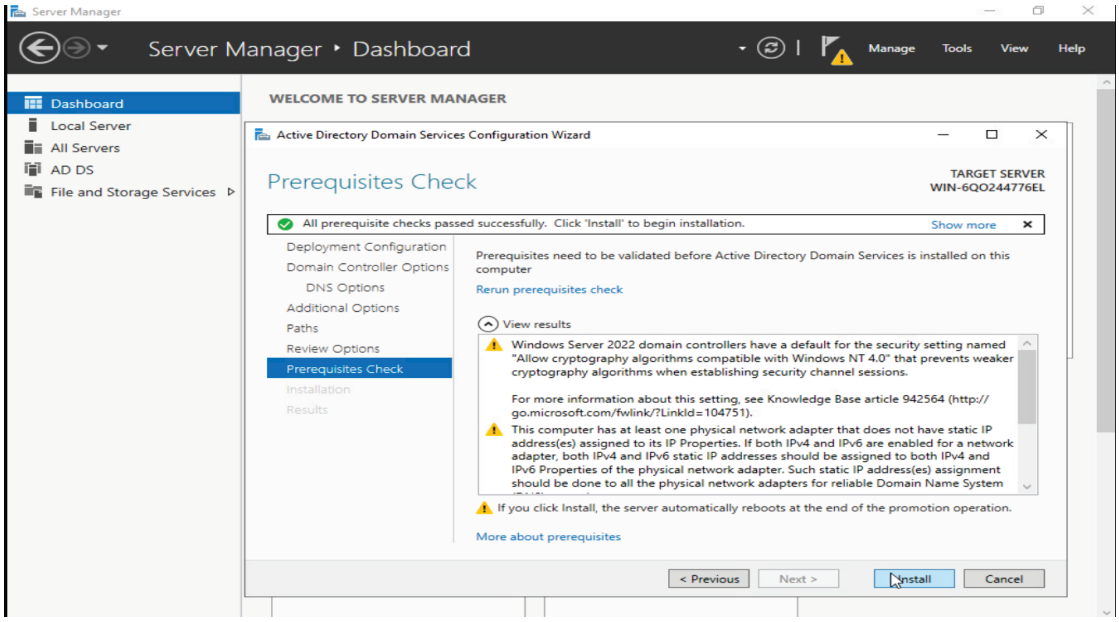
11: Enter the NetBIOS domain name, click next.

Figure 6-11. Screenshot with NetBIOS domain name



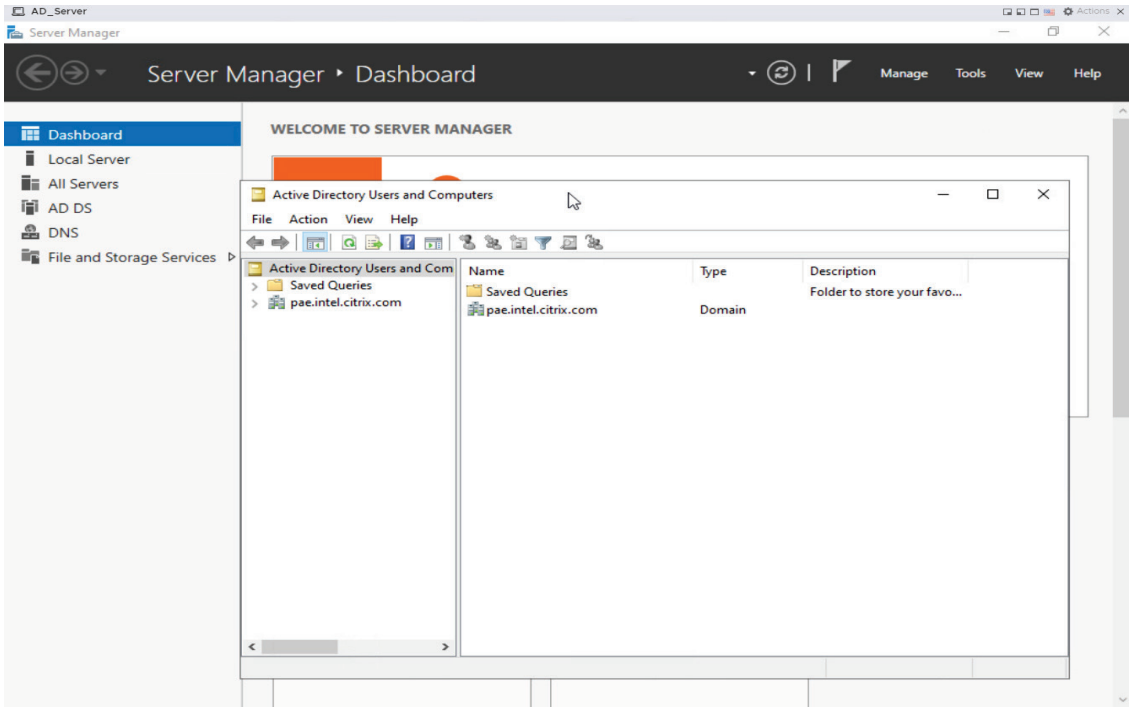
12: On Prerequisites Check click install.

Figure 6-12. Screenshot with Prerequisites Check



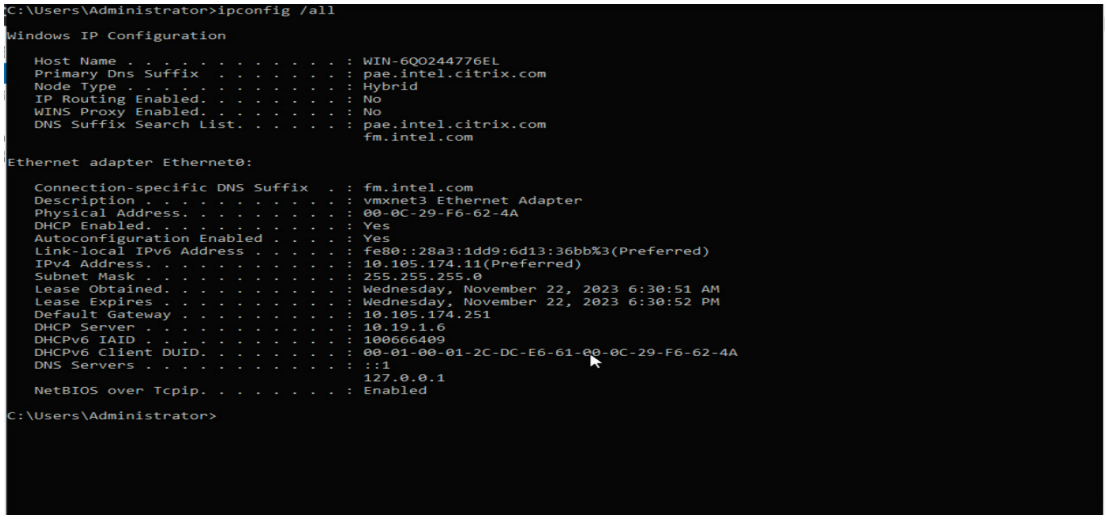
13: Once the installation is completed, the server will reboot. Now login as domain administrator.

Figure 6-13. Screenshot with AD Users and Computers



14: Open command prompt and run ipconfig /all command and note the IP address.

Figure 6-14. Screenshot with IPConfig command



6.2 Setup Citrix Delivery Controller

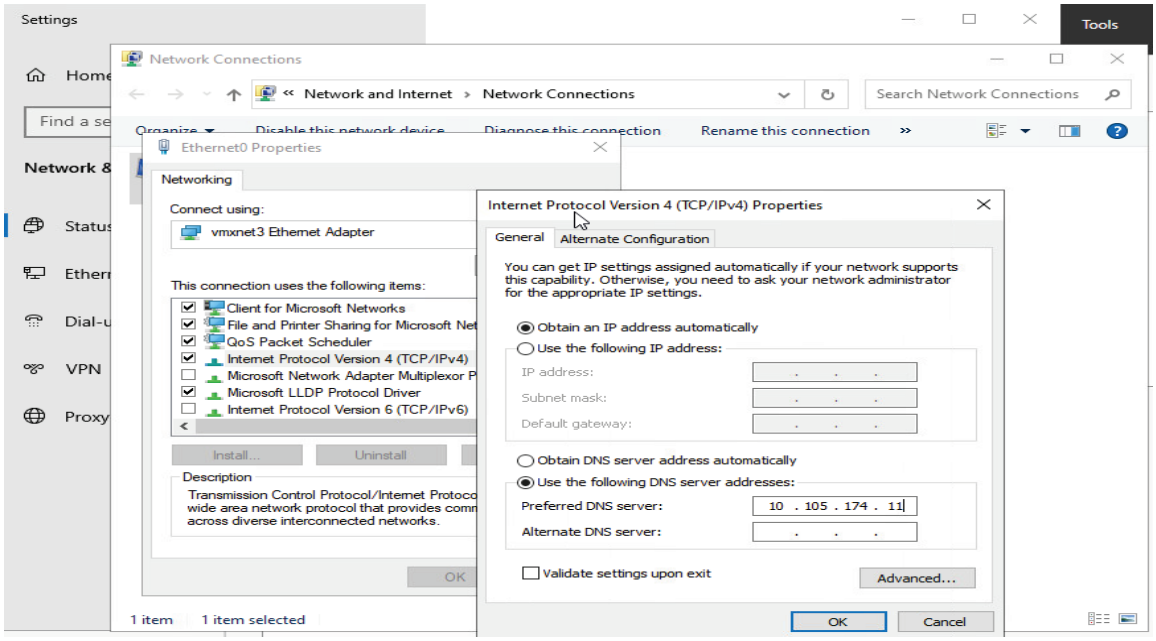
Citrix Delivery Controller setup has two parts.

1. Join the server (VM2) into the domain, created in Section 5.1.
2. Install the Citrix Delivery Controller and Citrix Studio

6.2.1 Join the server to the Domain.

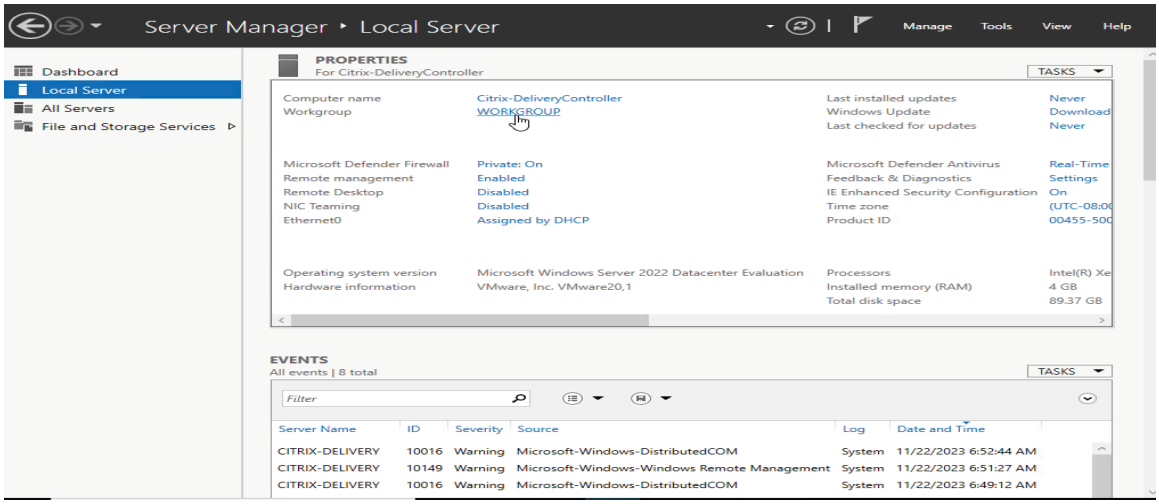
1: Open the network properties and update IPV4 properties. Select Use the following DNS server address. Enter the Active directory domain control Ip address as Preferred DNS server.

Figure 6-15. Screenshot with Updating DNS server details



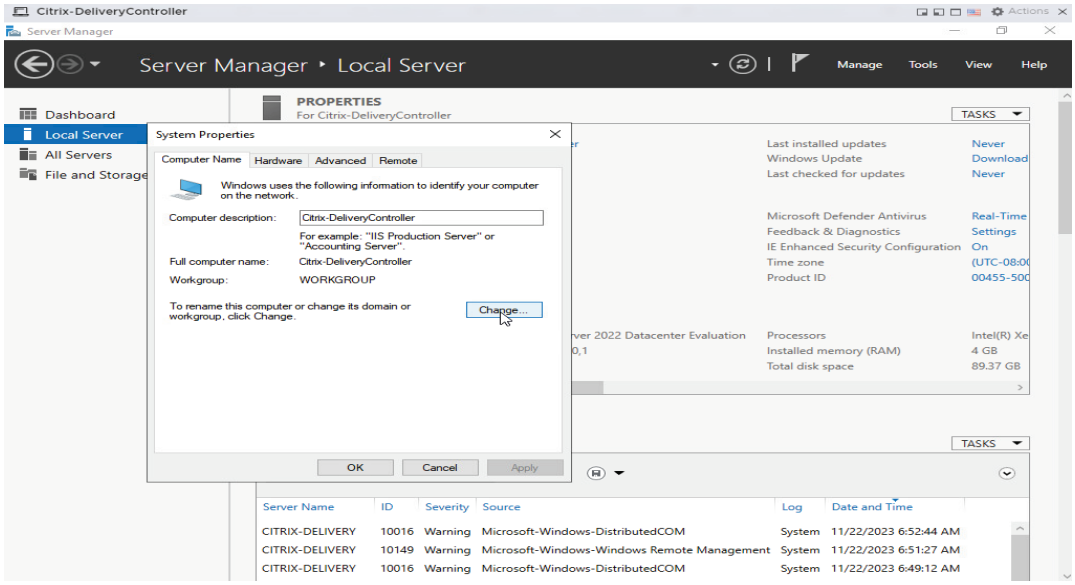
2: In the Server Manager select Local Server and Click on WORKGROUP

Figure 6-16. Screenshot with Updating DNS server details.



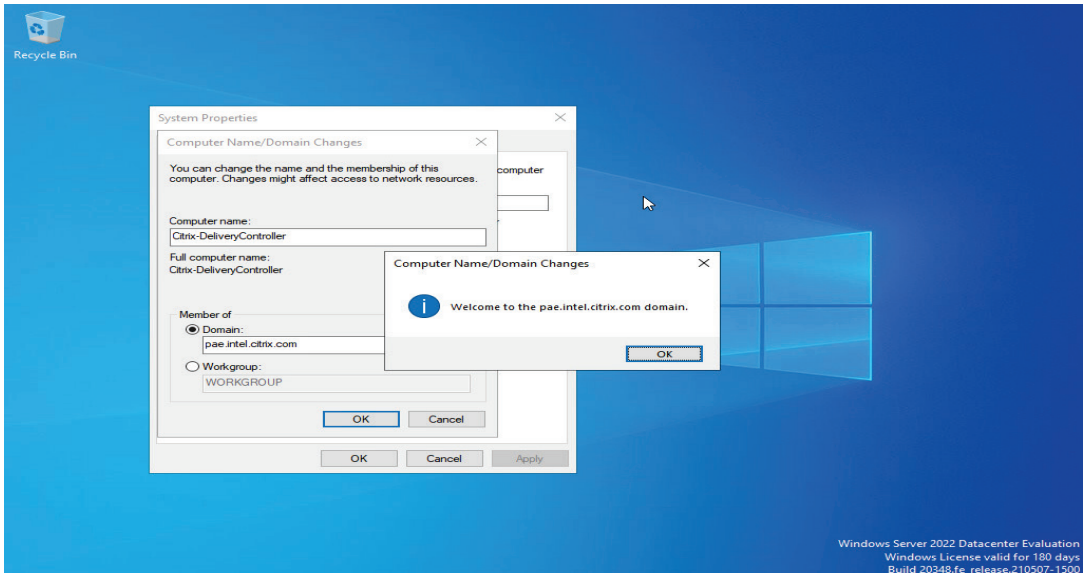
2: System Properties, click on Change button.

Figure 6-17. Screenshot with Updating System Properties.



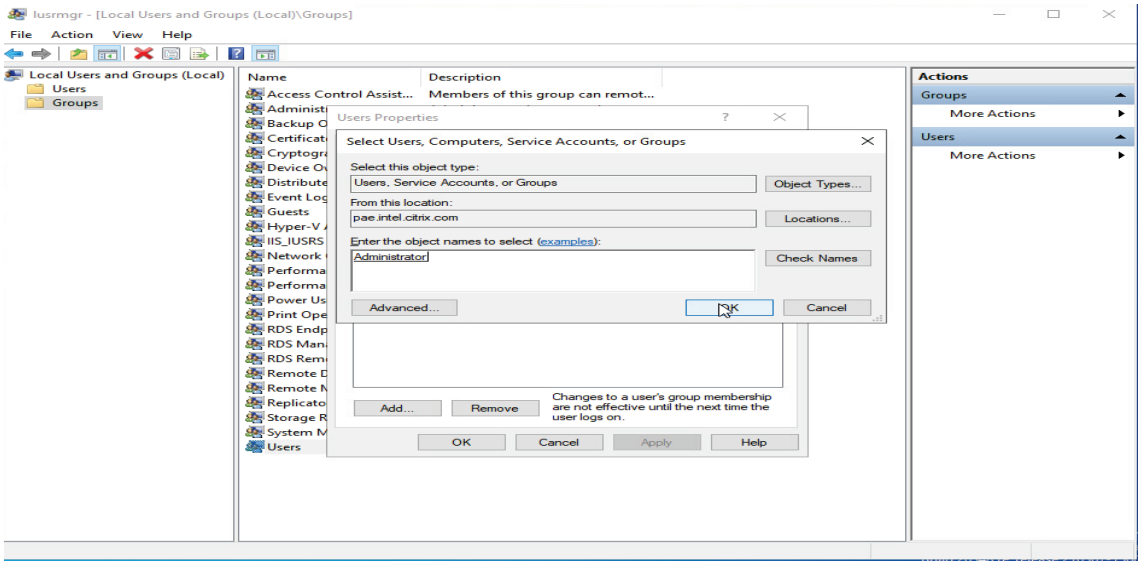
3: Select the Domain option, enter the Domain name, and click Ok button, enter Administrator and password. The server will reboot.

Figure 6-18. Screenshot with Joining the Domain.



4: Once the server is up, in the Windows command processor, enter the CMD command “lusrmgr.msc”, add Domain Administrator to local Administrators Group.

Figure 6-19. Screenshot with Add Domain Administrator to local Administrators Group.



5: Log off the server from local administrator and log in as Domain Administrator (Domain name/Administrator).

6.2.2 Install the Citrix Delivery Controller and Citrix Studio

1: Download Citrix Virtual Apps and Desktops ISO image from Citrix site.

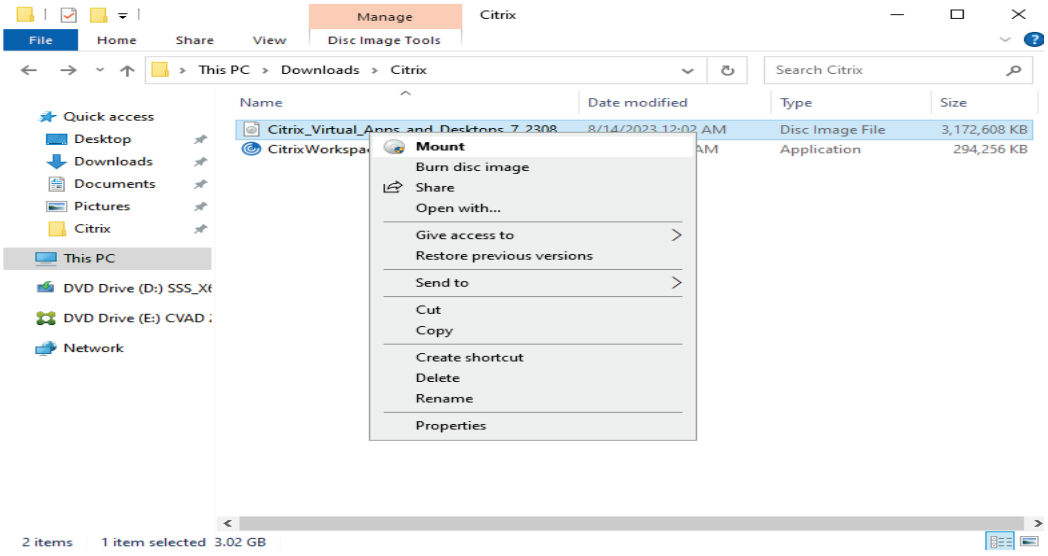
https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/

2: Refer the following web site to configure the Delivery controller.

https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/install-configure

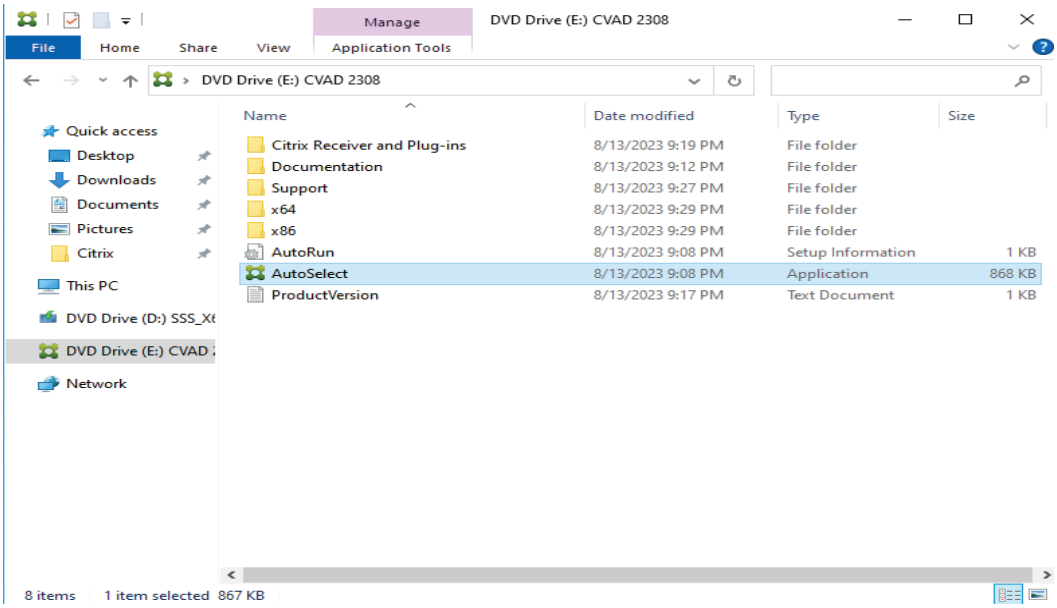
3: Right click on the ISO file and select the Mount.

Figure 6-20. Screenshot with Mount Citrix VAD ISO image



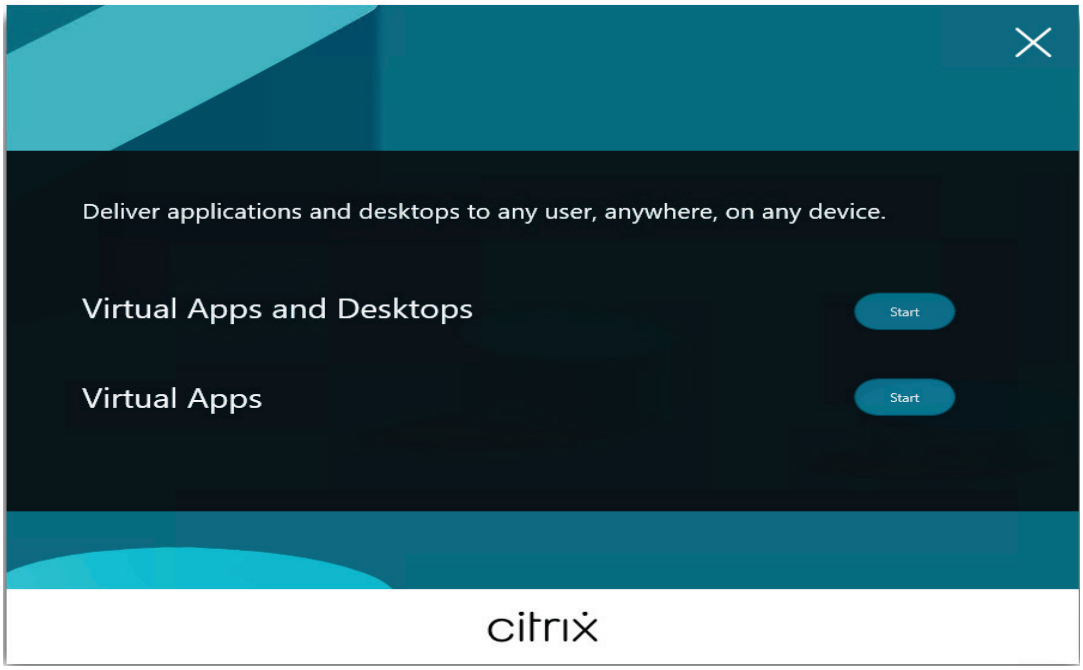
4: Double click on AutoSelect.exe

Figure 6-21. Screenshot with AutoSelect



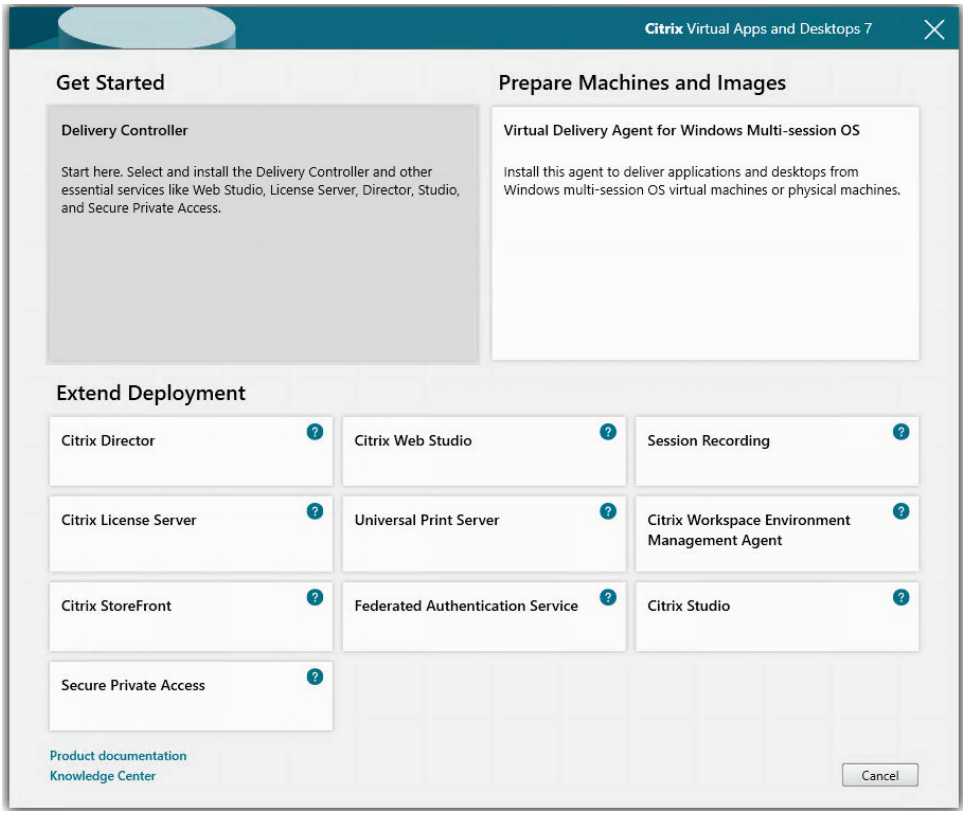
5: Select Virtual App and Desktops and Click Start

Figure 6-22. Screenshot with VAD



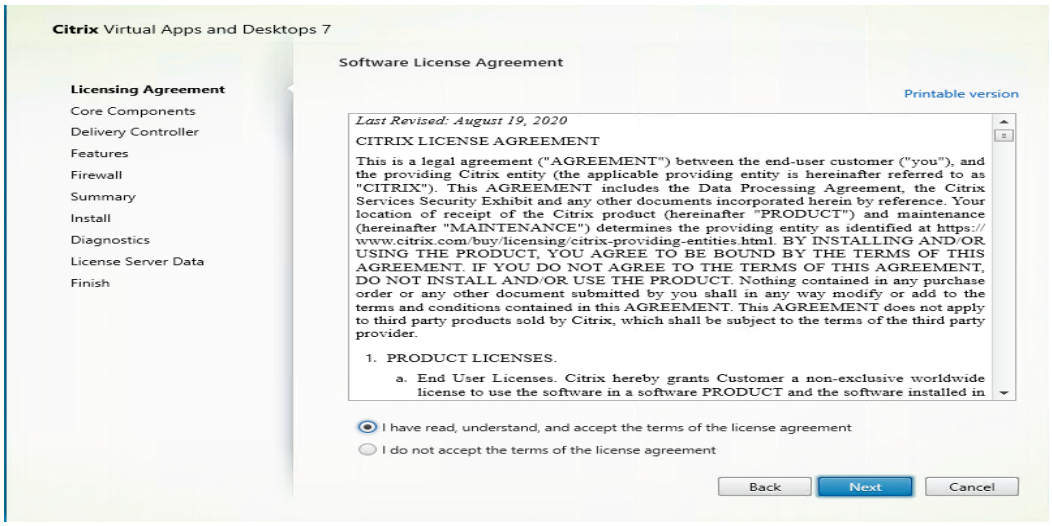
6: Click on Delivery controller.

Figure 6-23. Screenshot with Delivery controller



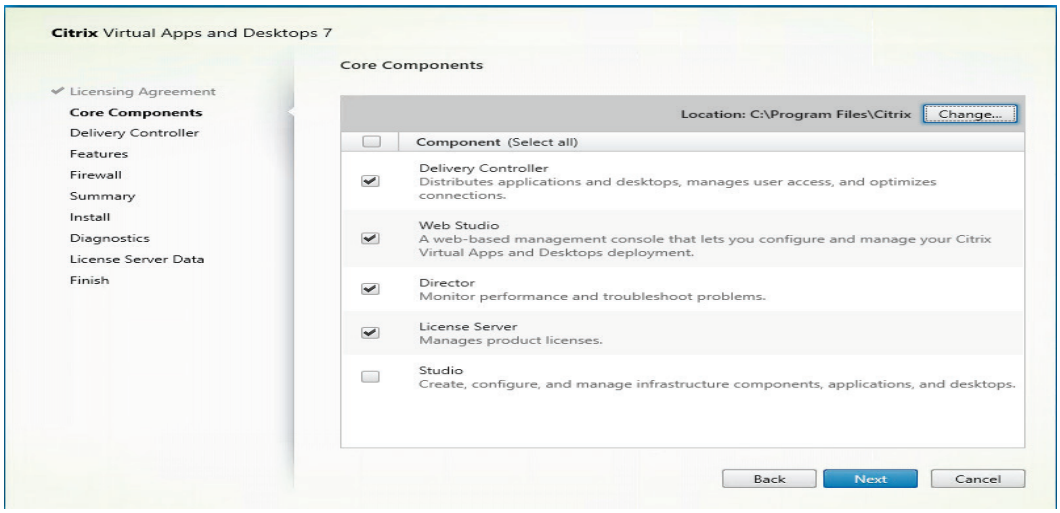
7: Select I have read, understand, and accept the terms of the license agreement and click Next.

Figure 6-24. Screenshot with Software License agreement



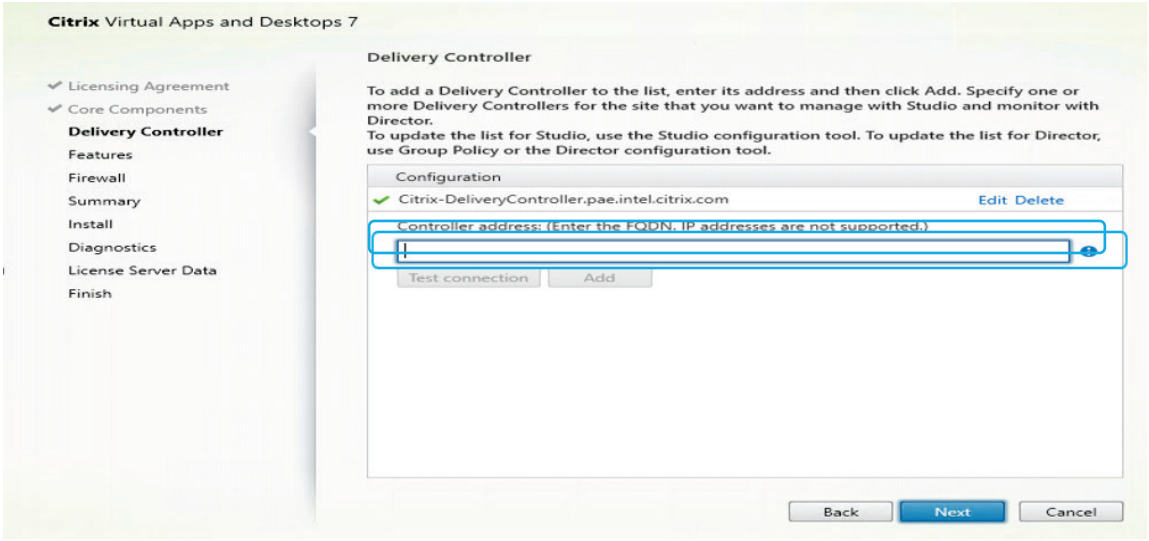
7: Select the following core components and click Next.

Figure 6-25. Screenshot with Core components



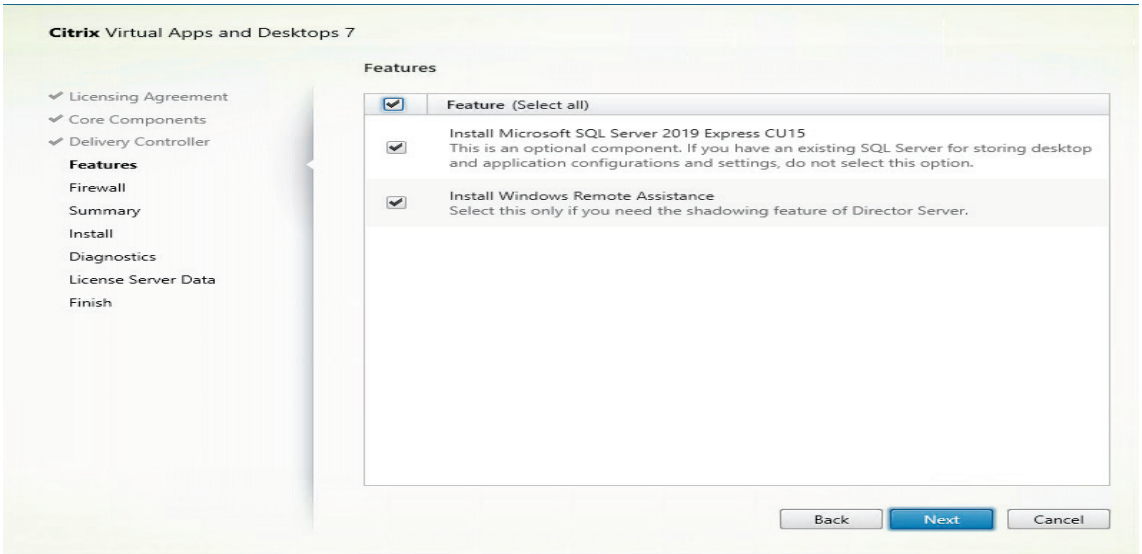
8: By default, Controller address will be selected, Other enter the FQDN (Servername.DomainName.com) and click Next.

Figure 6-26. Screenshot with Delivery Controller selection



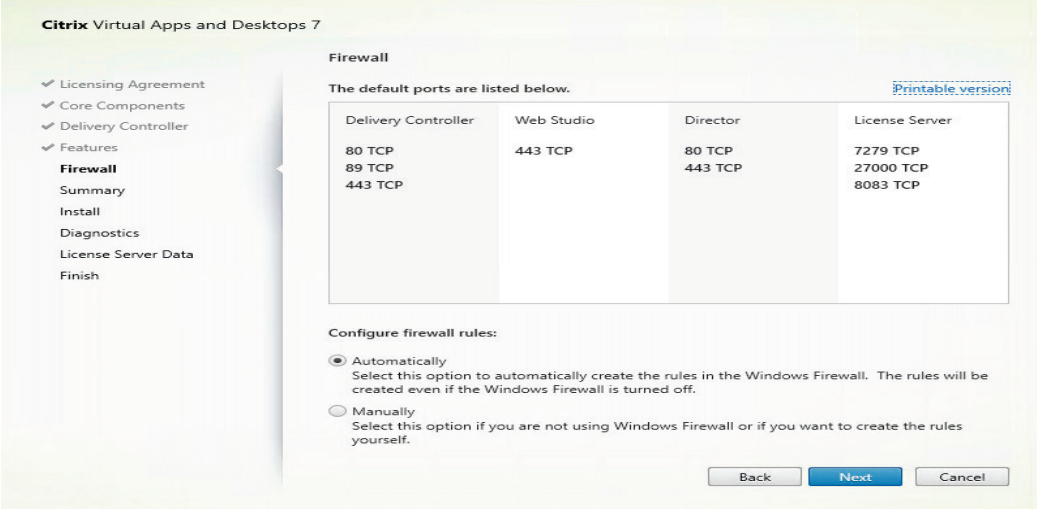
9: Select the following features and click Next.

Figure 6-27. Screenshot with Features selection



10: Select Firewall rules Automatically and click Next.

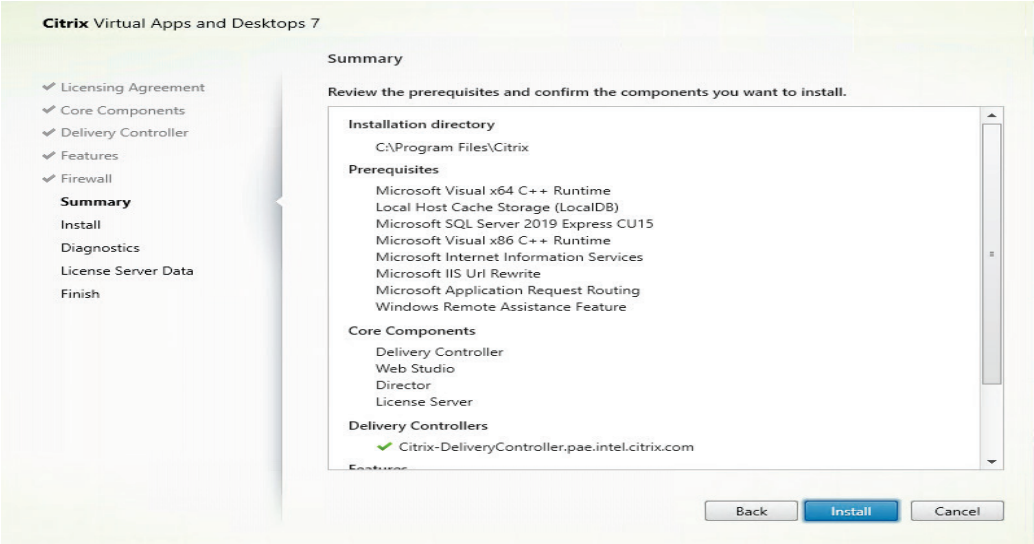
Figure 6-28. Screenshot with Firewall Rules



11: On Summary page click Install. The installation may take around 10-15 minutes based on network bandwidth and server configuration.

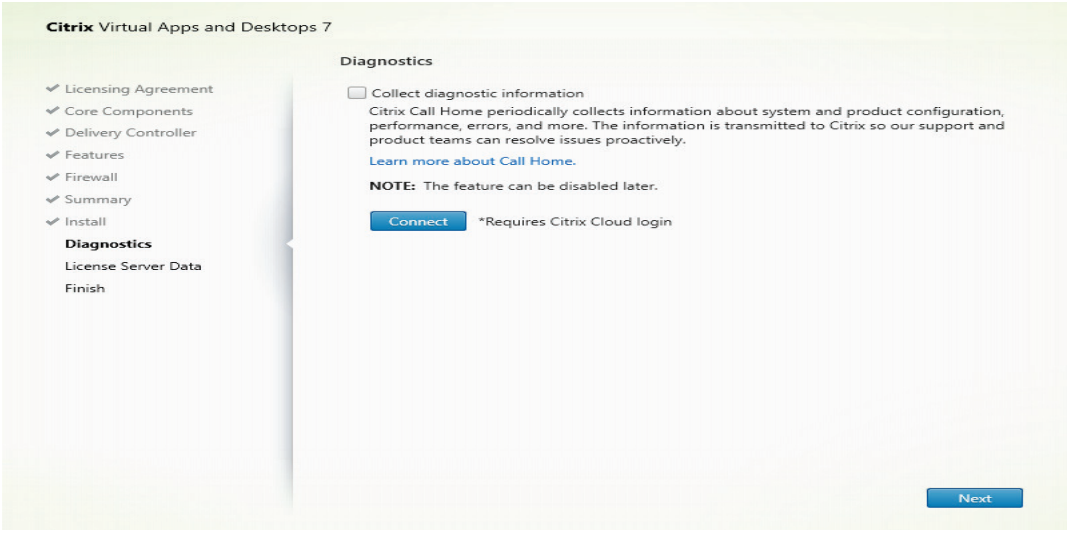
Note: If the server reboots while installing the prerequisite, repeat the same steps from Step 3. The installation process persists the selected option and jump on to the Install section.

Figure 6-29. Screenshot with Firewall Rules



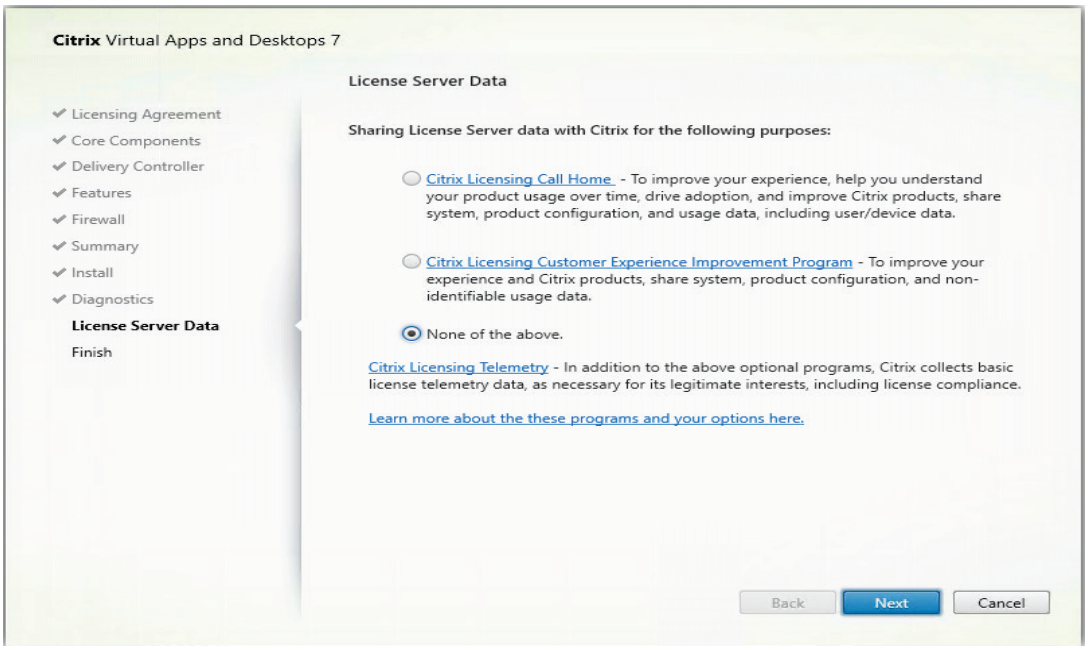
12: Keep the default options and click Next.

Figure 6-30. Screenshot with Diagnostics



13: Select Neither of the previous options and click Next.

Figure 6-31. Screenshot with License Server data



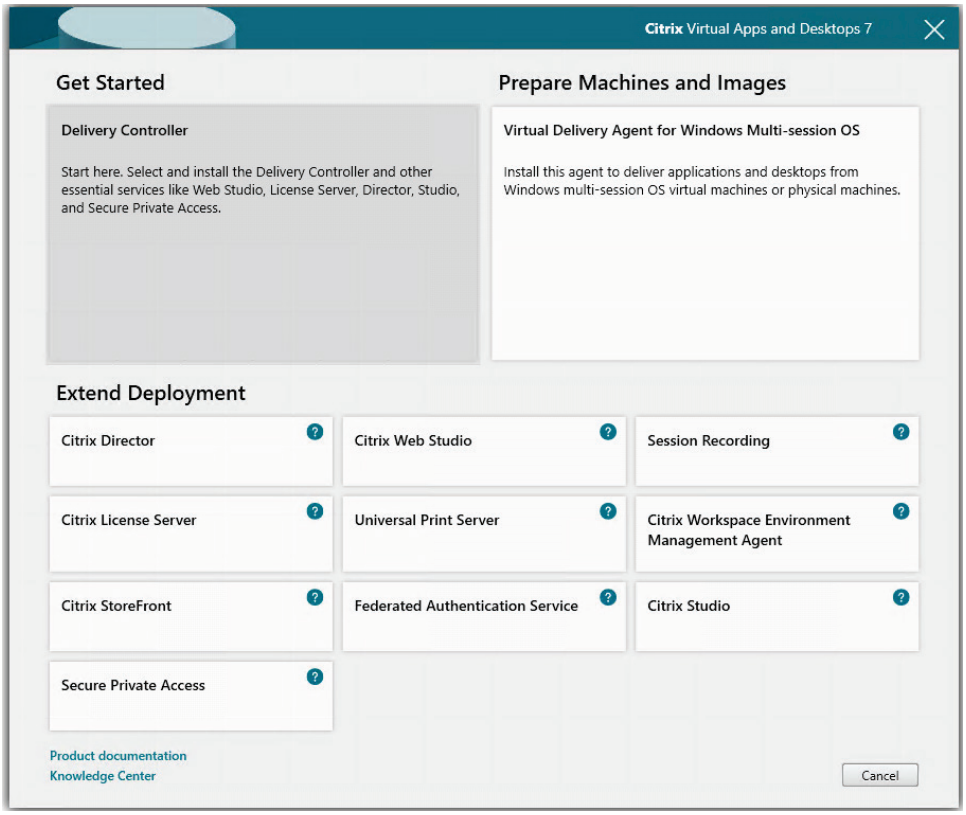
14: Click Finish.

6.2.3 Install Citrix Studio

1: Repeat the steps from 3 to 5 specified in section 5.2.2.

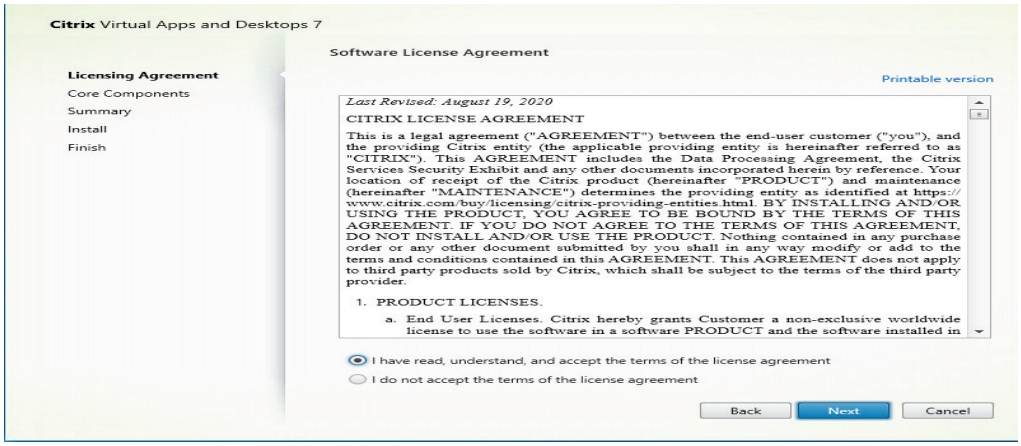
2: Select Citrix Studio.

Figure 6-32. Screenshot with VAD Get Started



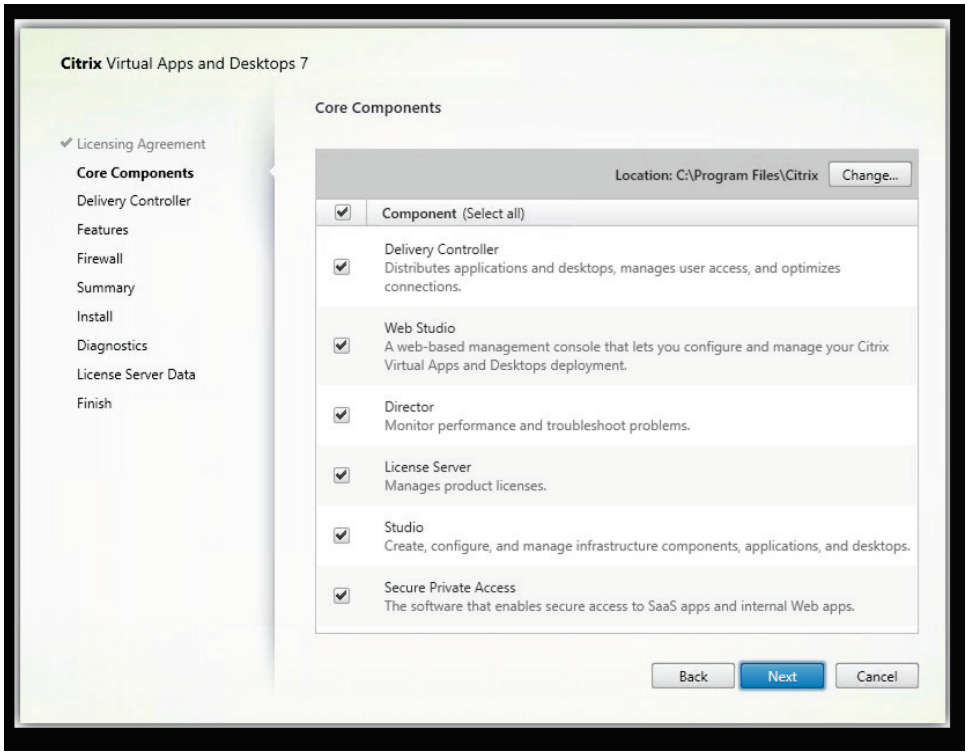
3: Select "I have read, understand, and accept" the terms of the license agreement and click "Next".

Figure 6-33. Screenshot with License Agreement



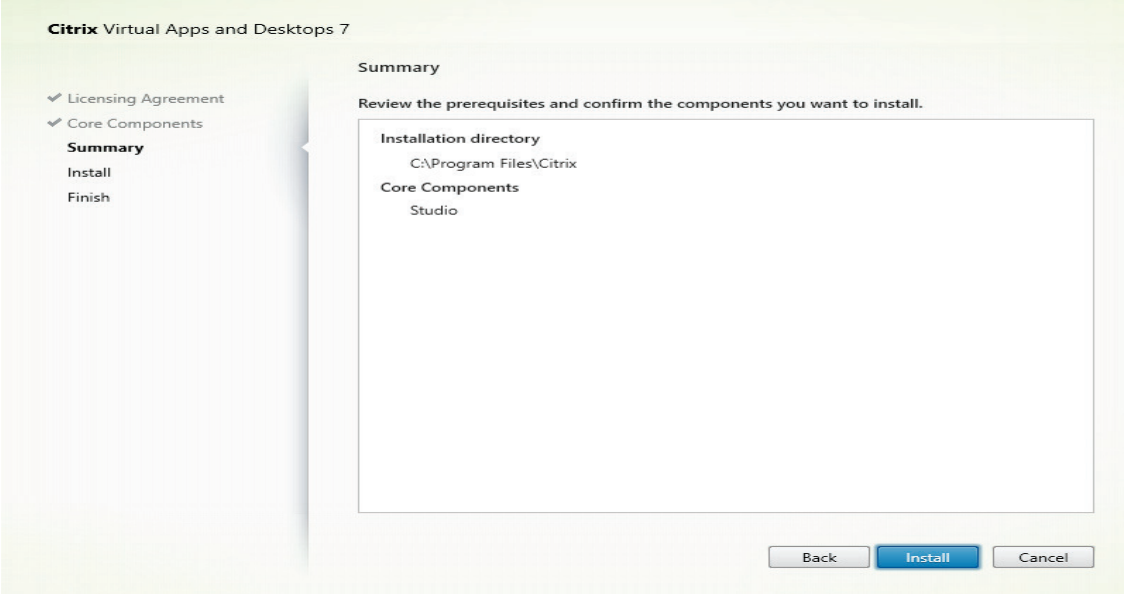
4: Click next on Core Components.

Figure 6-34. Screenshot with Core Components



5: Click Install and then Finish.

Figure 6-35. Screenshot with Summary

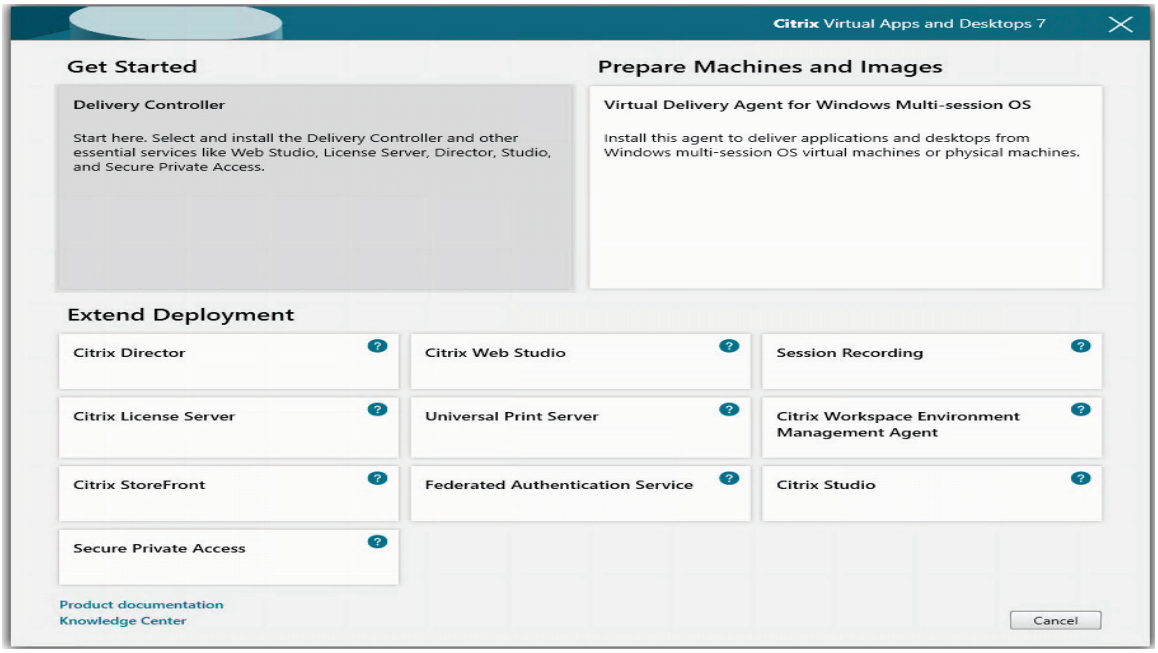


6.2.4 Install Citrix StoreFront

1: Repeat the steps from 3 to 5 specified in the section 6.2.2.

2: Select Citrix StoreFront.

Figure 6-36. Screenshot with Get Started

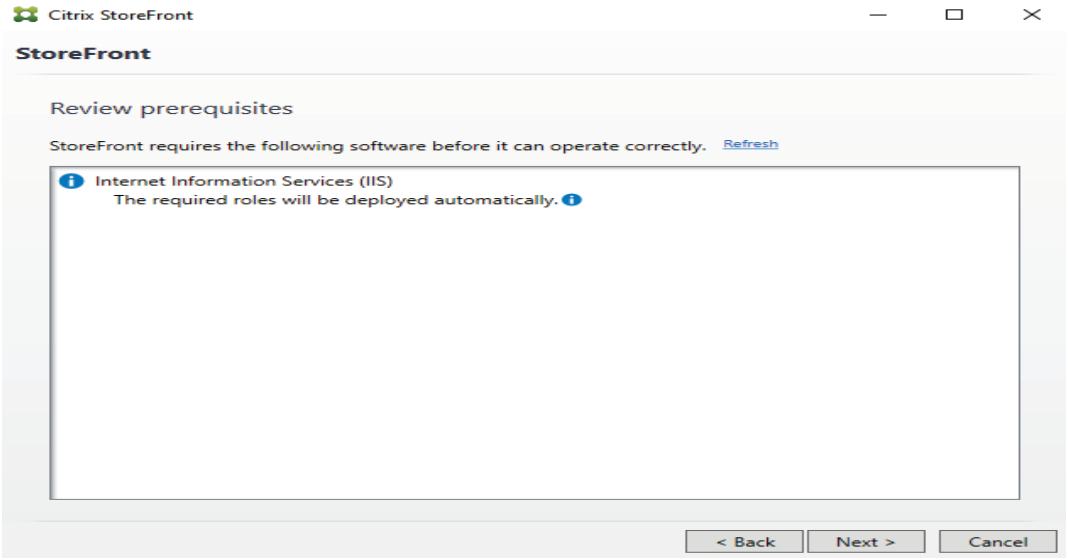


3: Accept the License Agreement and click Next.

Figure 6-37. Screenshot with StoreFront License Agreement

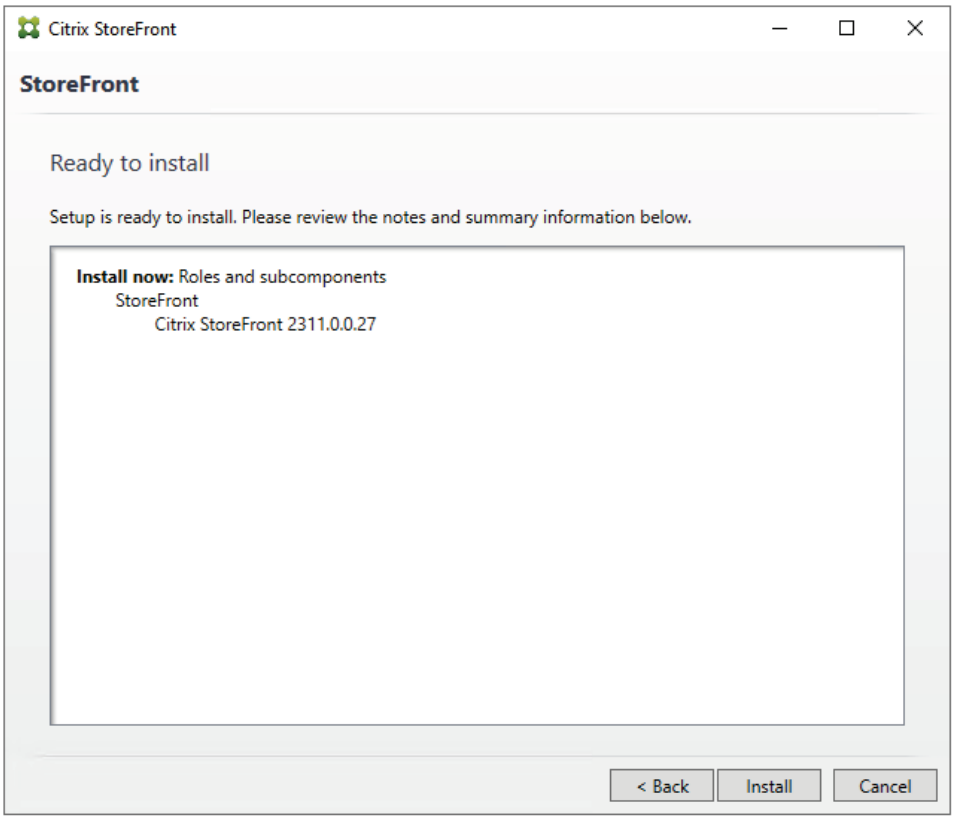
4: Review prerequisites and click Next.

Figure 6-38. Screenshot with Review Prerequisites



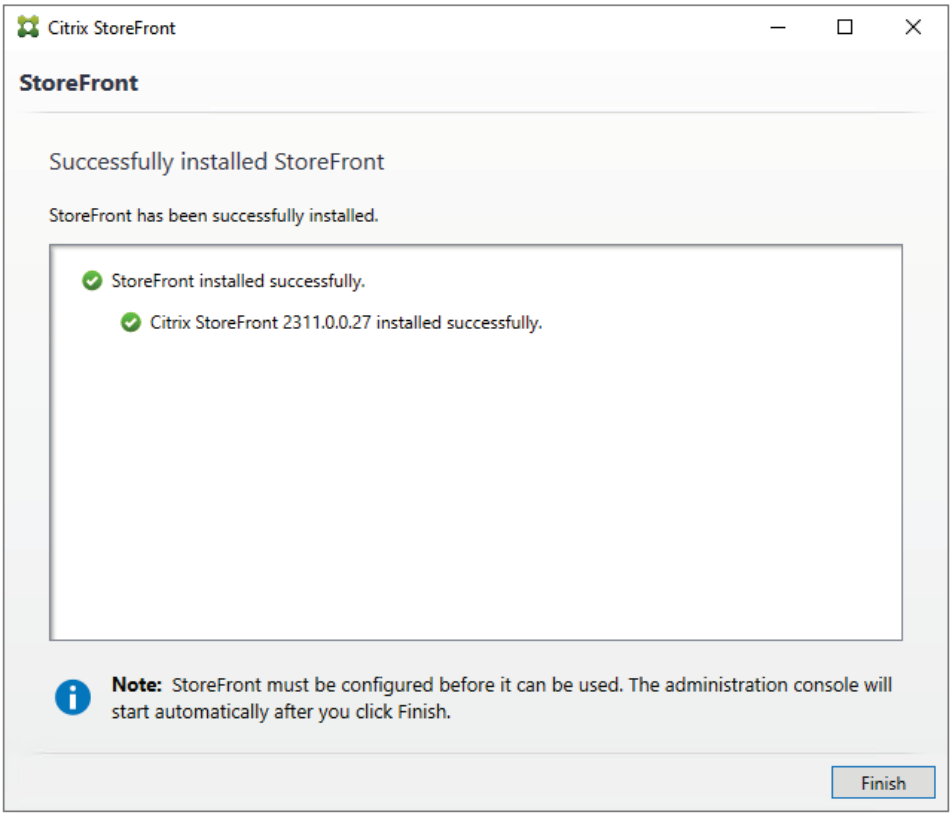
5: Click Install.

Figure 6-39. Screenshot with Ready to Install



6: Click Finish. After successful installation, the server will reboot.

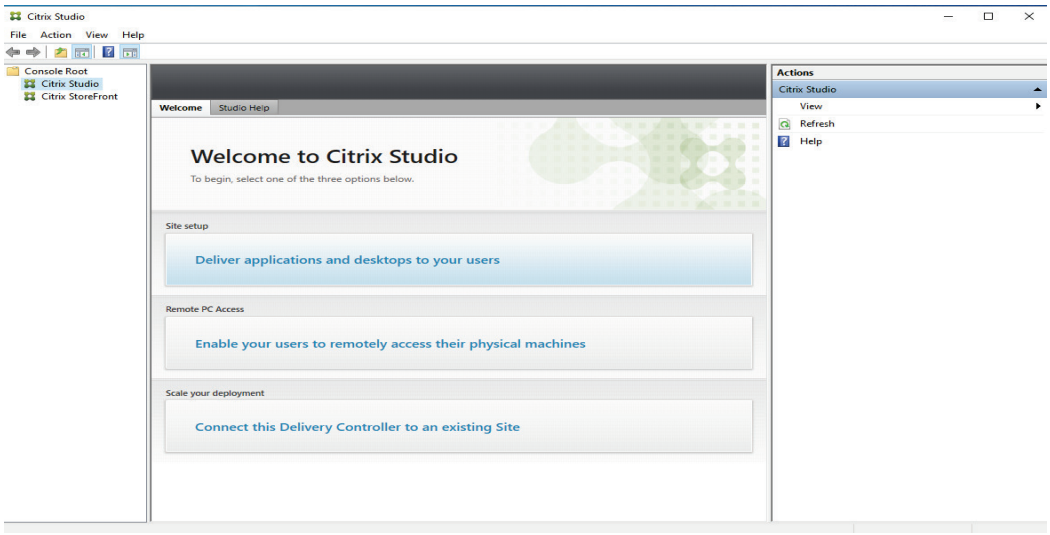
Figure 6-40. Screenshot with Successfully Installed



6.2.5 Delivery Controller Configuration

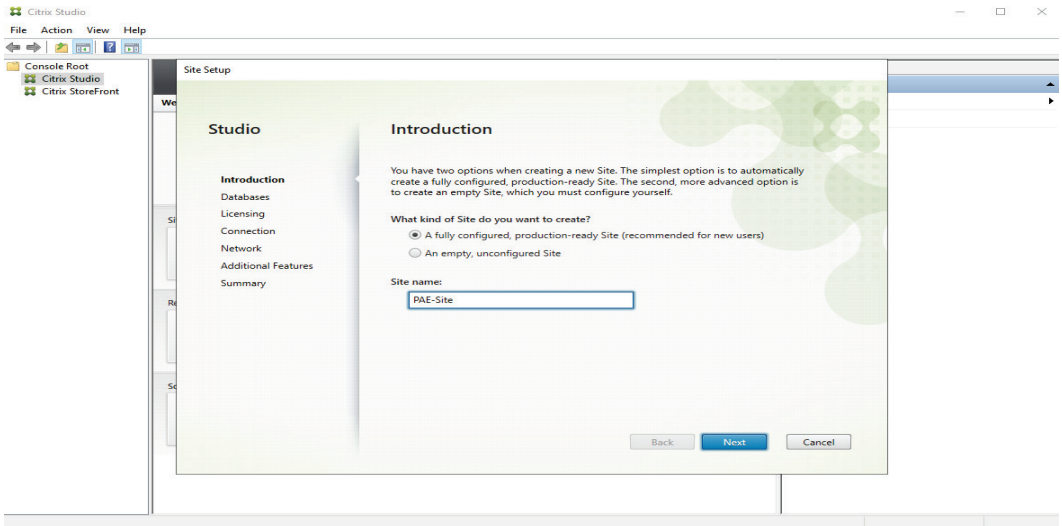
1: Open Citrix Studio and click on Deliver applications and desktops to your users.

Figure 6-41. Screenshot with Welcome to Citrix Studio



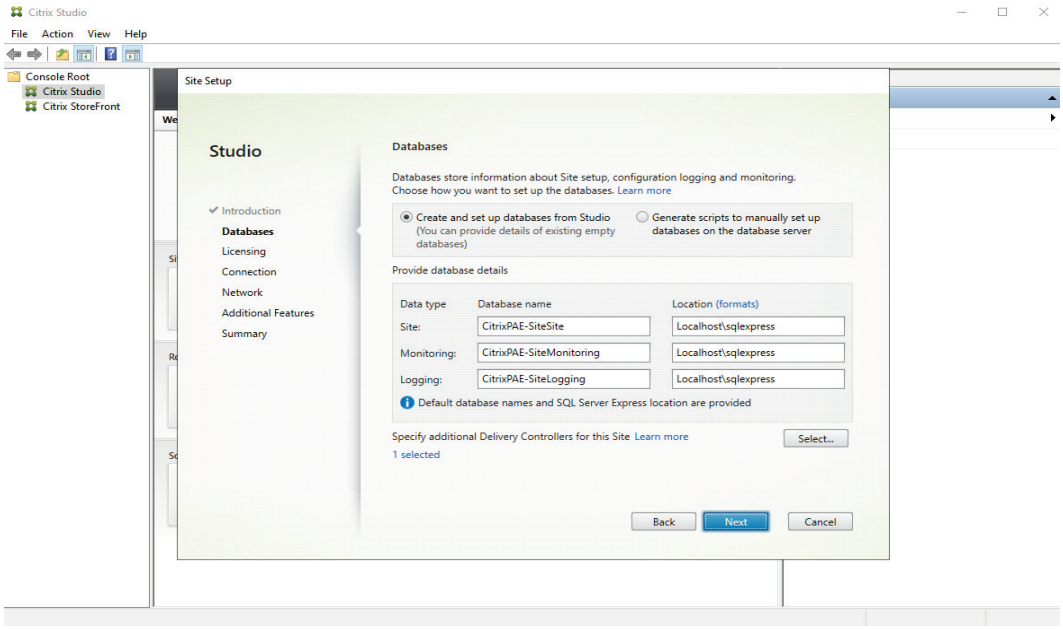
2: Enter the Site Name and click Next.

Figure 6-42. Screenshot with Site Name



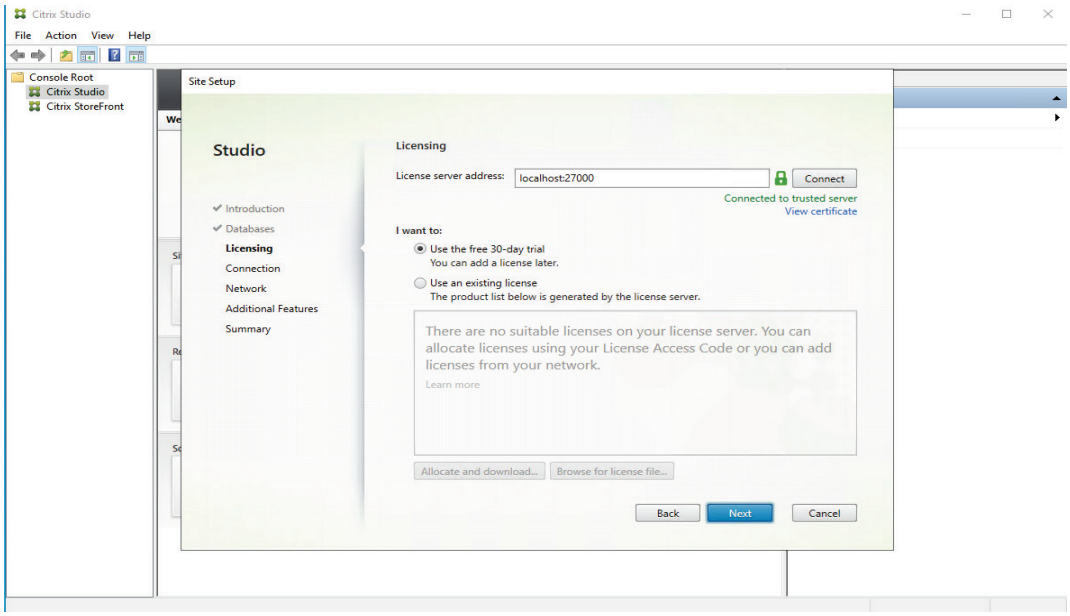
3: Prefer to keep the default options and click next. If required changes the Database and location

Figure 6-43. Screenshot with Database



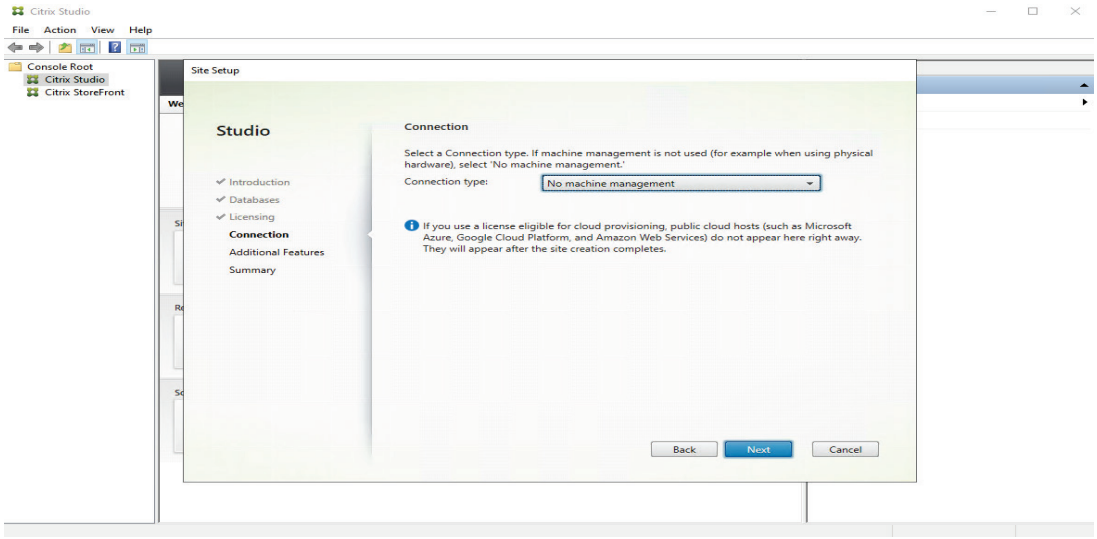
4: Select the appropriate licensing option and click Next.

Figure 6-44. Screenshot with License Server



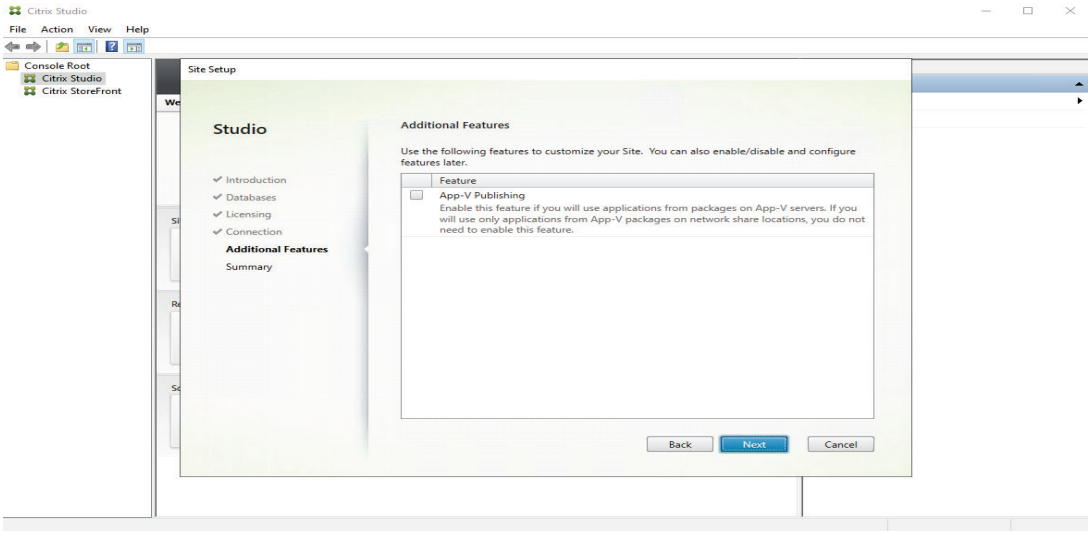
5: Select Connection type as No machine management and click Next.

Figure 6-45. Screenshot with Connection type



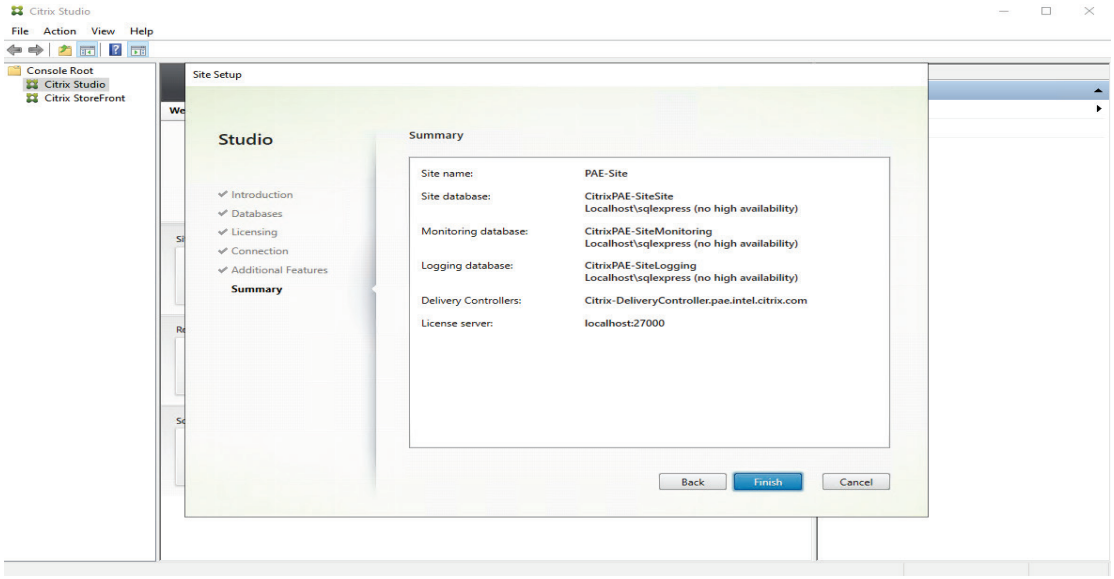
6: Keep the default option and click Next.

Figure 6-46. Screenshot with Additional Features



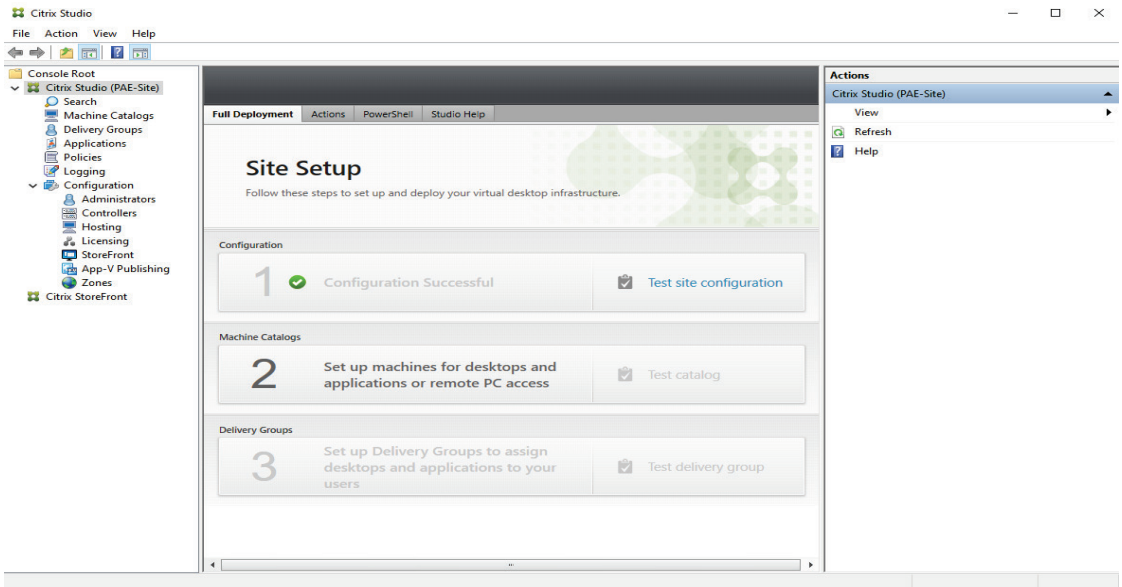
7: Click Finish

Figure 6-47. Screenshot with Finish Studio Installation



8: On successful site configuration

Figure 6-48. Screenshot with Successful configuration of Citrix Studio



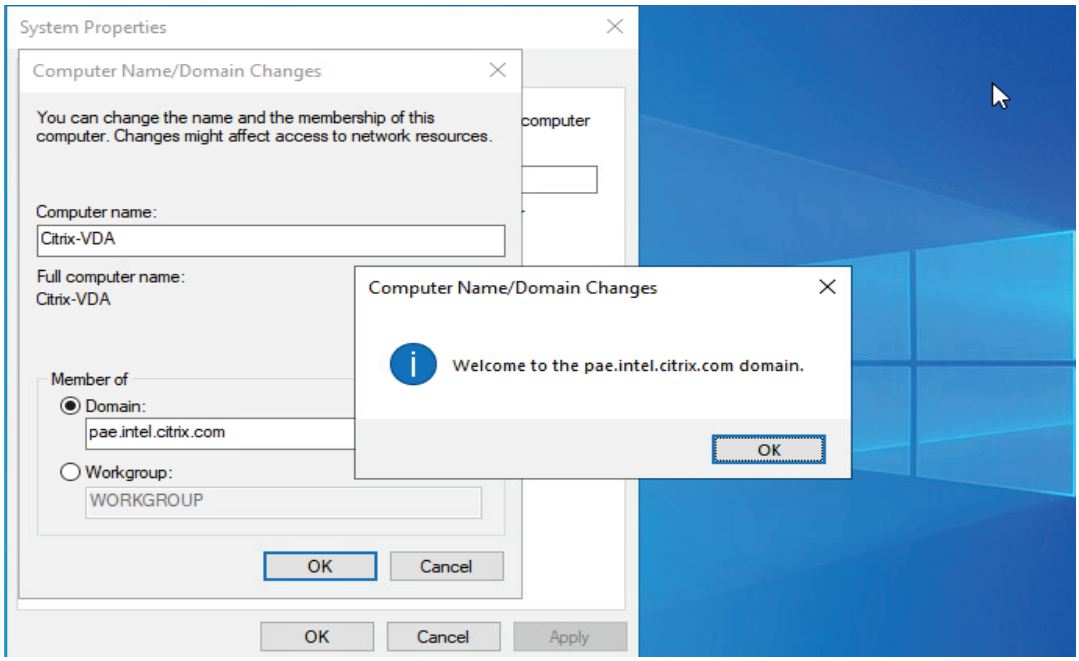
6.3 Setup Citrix Virtual Delivery Agent

The following steps describes setting up the Virtual Delivery Agent (VDA) on third VM.

6.3.1 Join the server to the Domain.

To join the server to the domain, follow the steps specified in the Section 6.2.1.

Figure 6-49. Screenshot with Delivery Agent joining the domain.

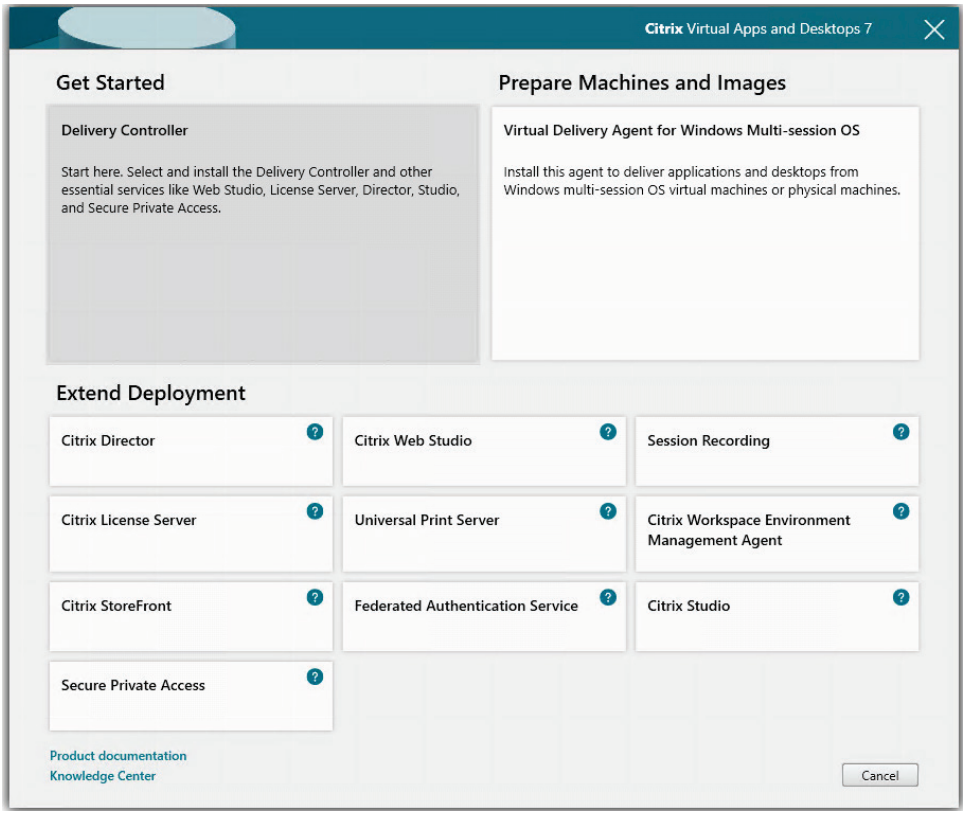


6.3.2 Install the Virtual Delivery Agent.

1: Repeat the steps from 1 to 5 specified in the section 6.2.2.

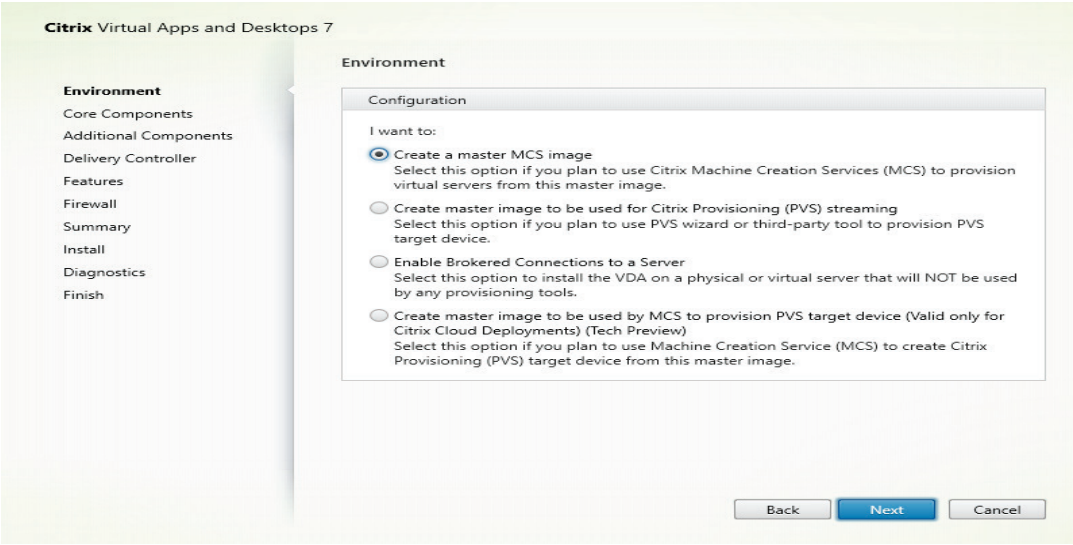
2: Click Virtual Delivery Agent for Windows Multi-Session OS.

Figure 6-50. Screenshot with Get Started



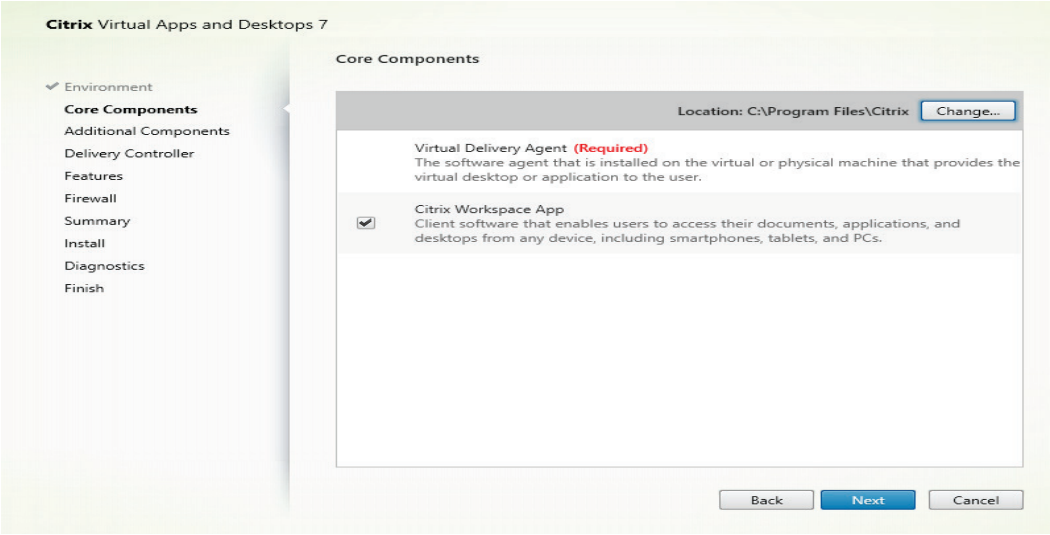
3: Select the MCS image and click Next.

Figure 6-51. Screenshot with Environment Configuration



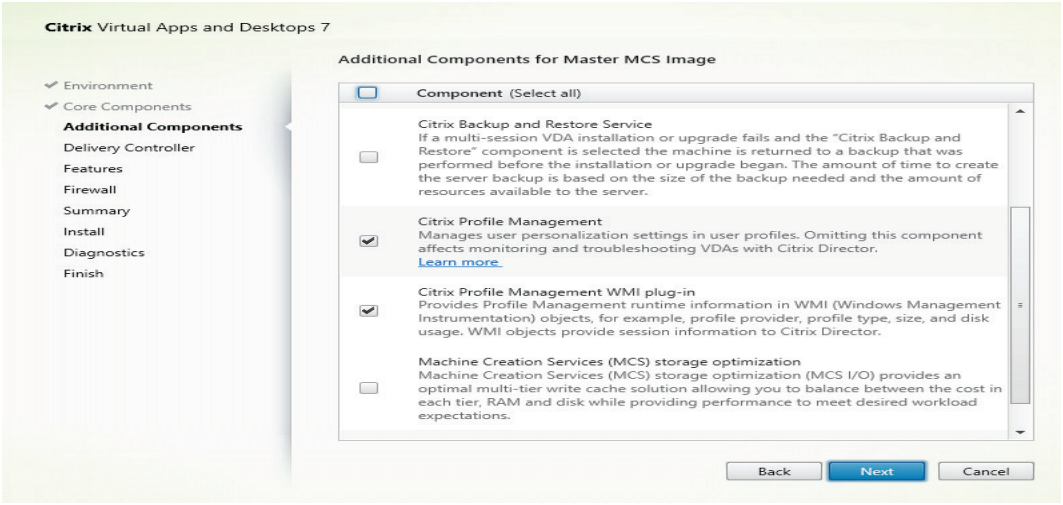
4: Select the following core components and click Next.

Figure 6-52. Screenshot with Core Components



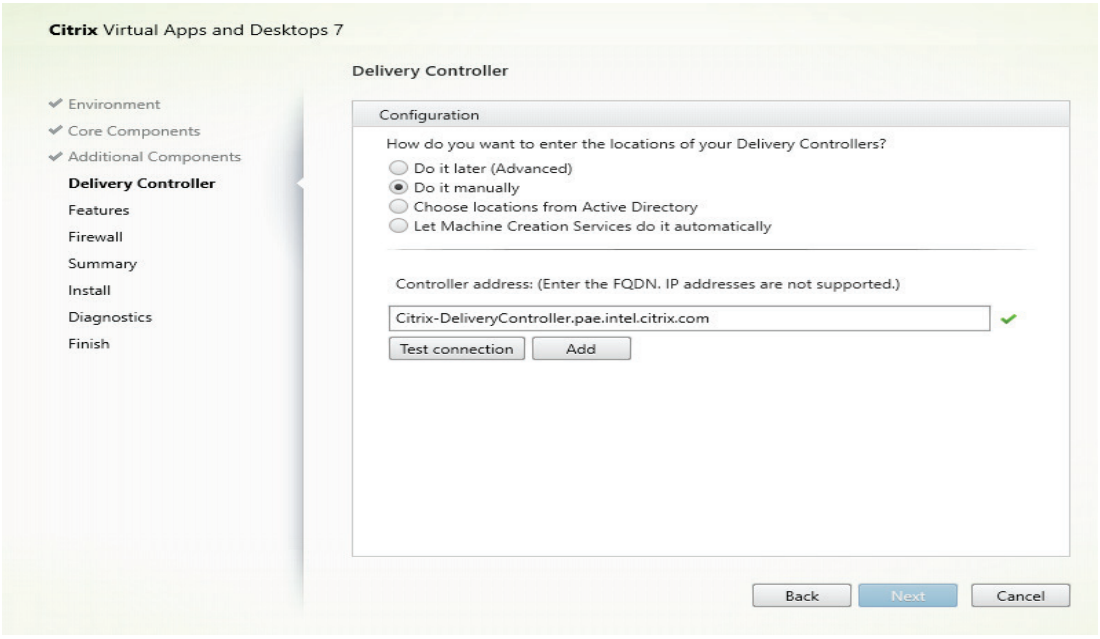
5: Select the following additional components and click Next.

Figure 6-53. Screenshot with Additional components



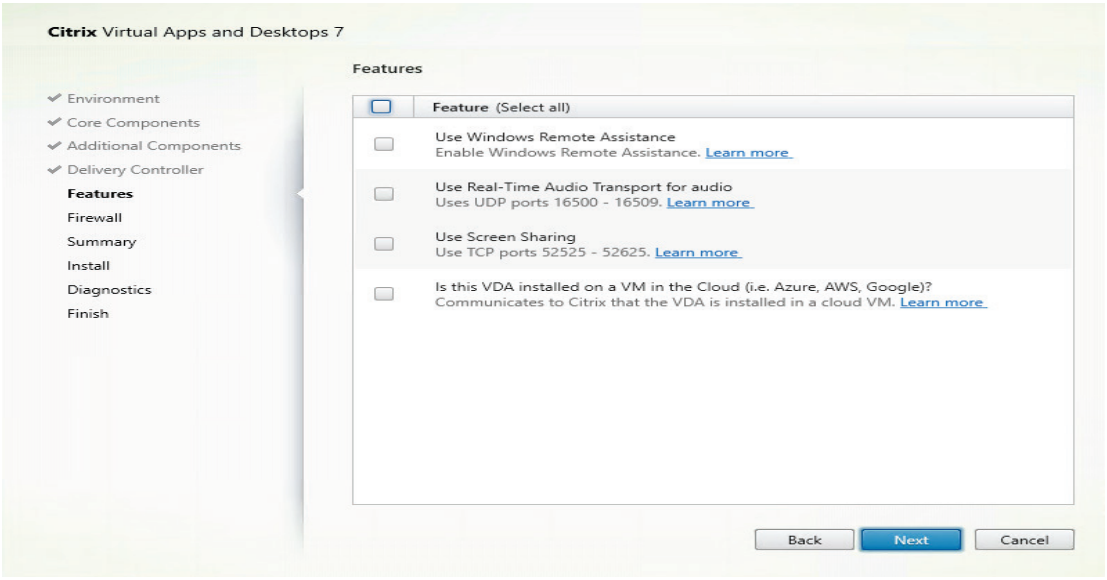
6: Enter the Delivery controller name specified Section 5.2.2 Step 8 and click Test Connection. Once the connection test is passed (green check mark) click Add. Click Next.

Figure 6-54. Screenshot with Configure Delivery Controller



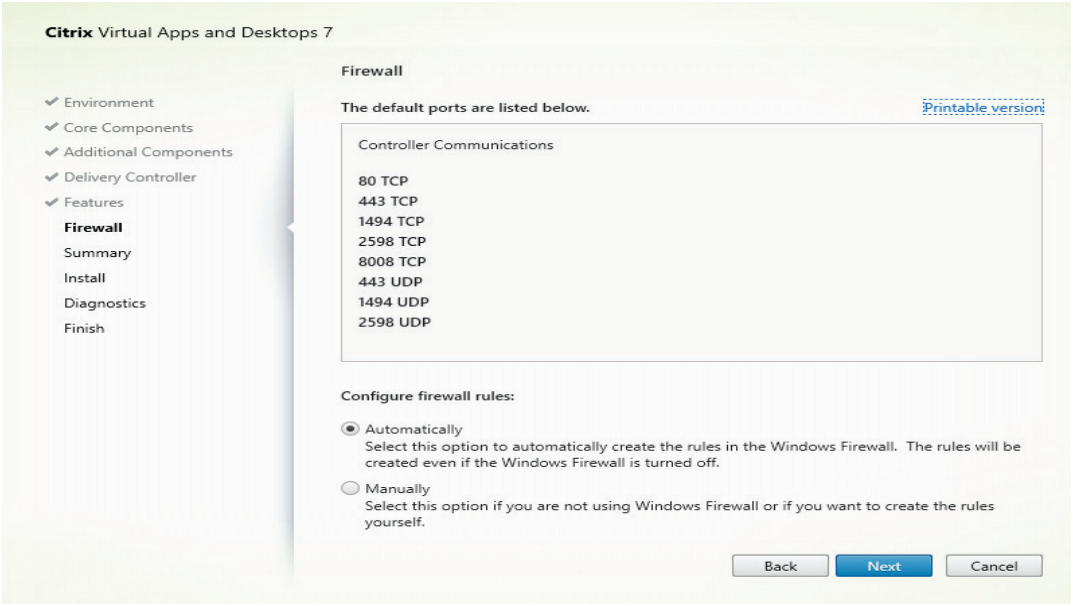
7: Keep the default selection, click Next.

Figure 6-55. Screenshot with Features selection



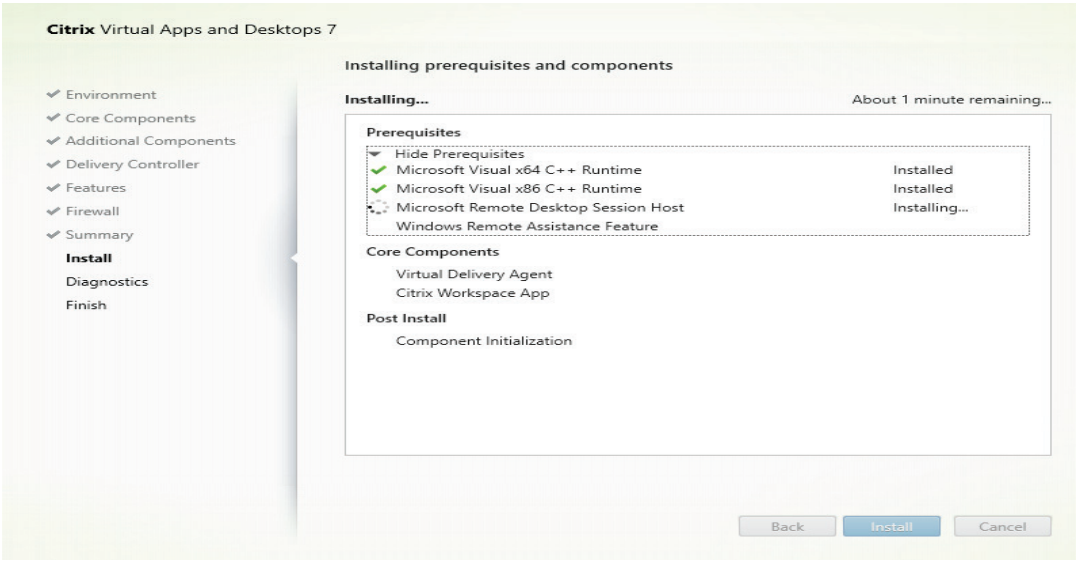
8: Select Automatically in the Firewall port selection and click Next.

Figure 6-56. Screenshot with Firewall configuration



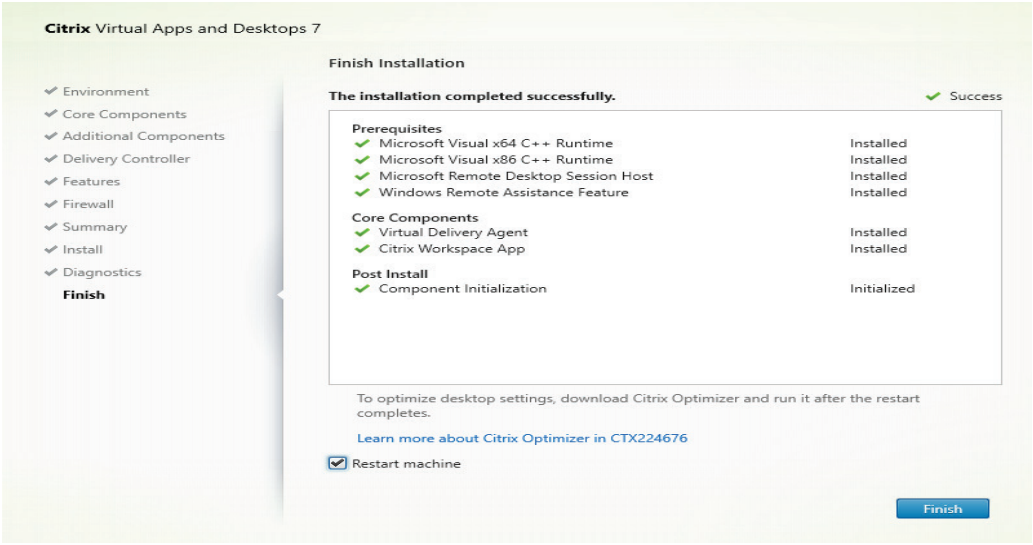
9: On the summary screen click Install. Once the installation is complete, the server may reboot automatically.

Figure 6-57. Screenshot with Install prerequisites

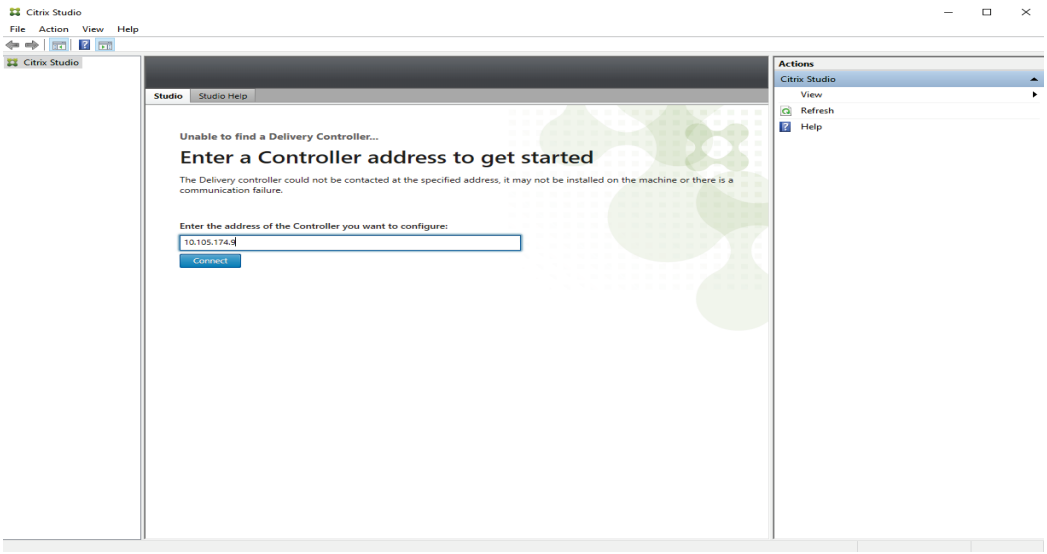


10: One the server reboots, restart the installation and make sure the All the following components are installed. And click Finish.

Figure 6-58. Screenshot with Finish Installation



11: Open the Citrix Studio and enter the Delivery controller address configured in section 5.2.5 and click connect.



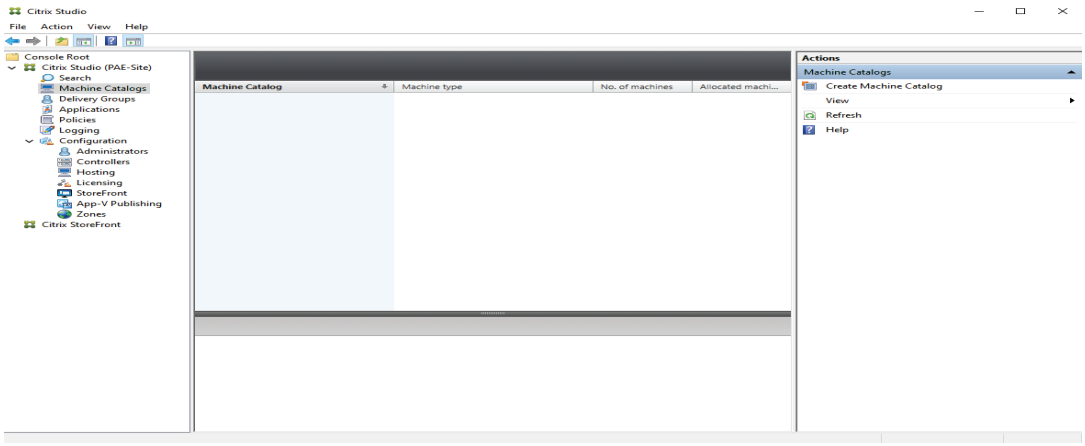
The VDA server is now connected to the Delivery controller.

6.4 Apps and Desktop Virtualization

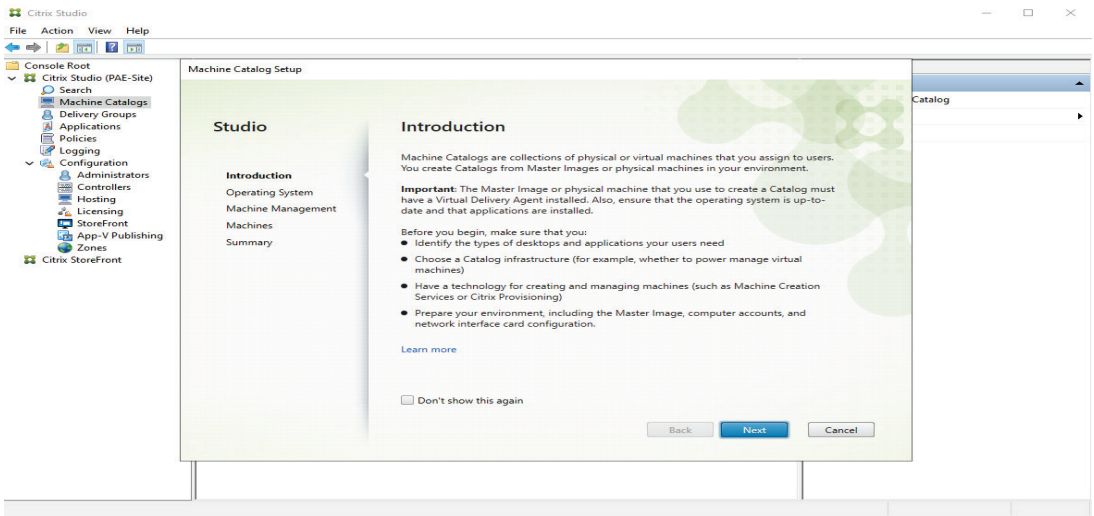
6.4.1 Create Machine Catalogs.

CVAD 2311 is needed for use with Machine Creation Services (MCS). More information about MCS, creating a Master VM for MCS and how to create MCS machine catalogs can be found in the Citrix documentation: https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/install-configure/machine-catalogs-create/create-machine-catalog-vmware

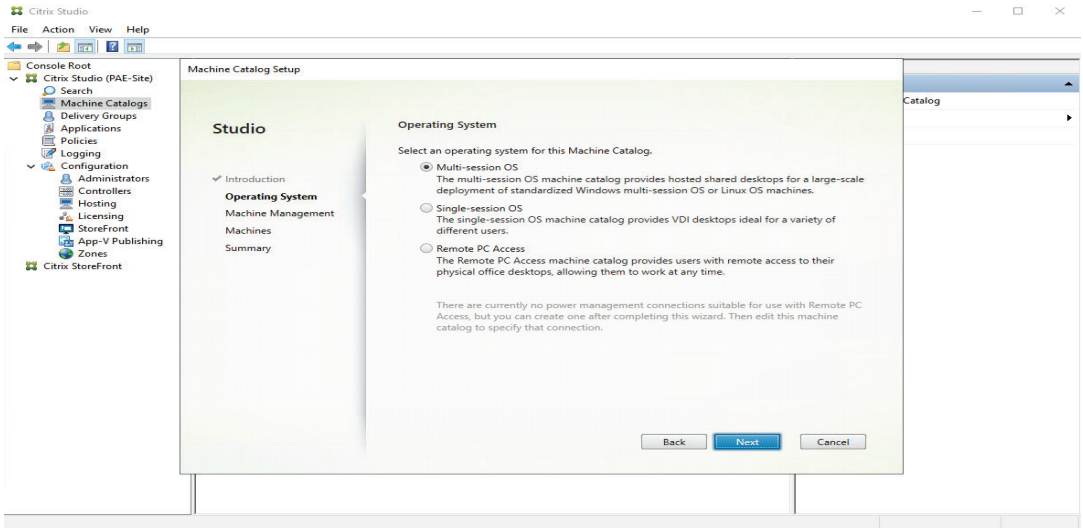
1: Login to the Delivery Controller VM and open Citrix Studio MMC application.



2: Select Machine Catalogs in the left pane, and then select Create Machine Catalog in the action bar on the Right pane. And click Next.

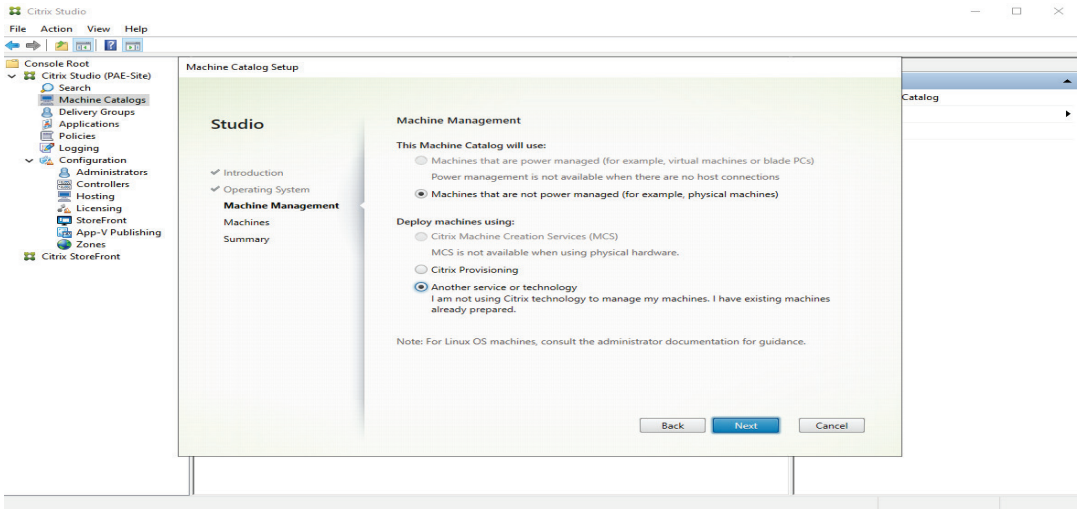


3: Select Multi-session OS and click Next.

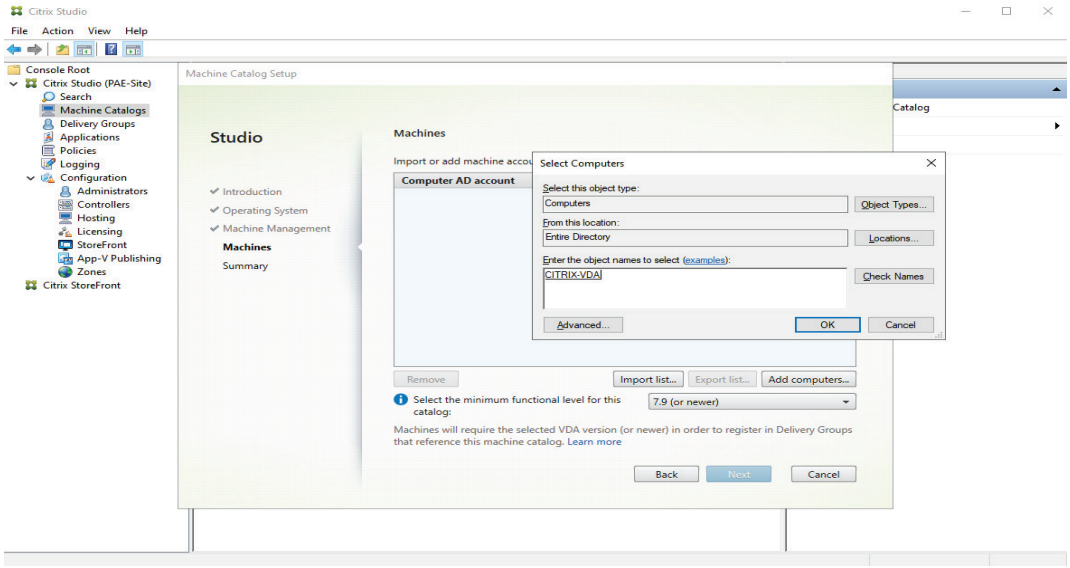


4: Select Another service or technology and click Next.

Hardware encoding is supported and active when using MCS on CVAD 2311 or later versions.

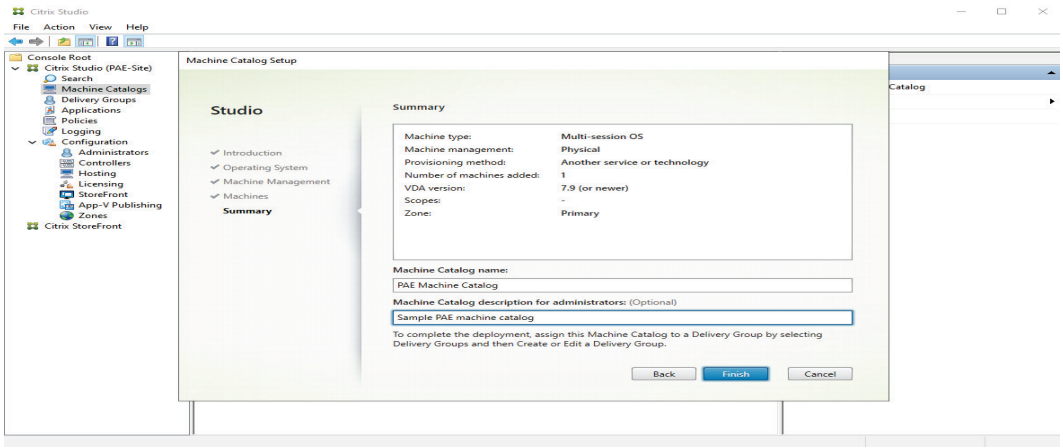


5: Click on Add computers and enter VM host name.



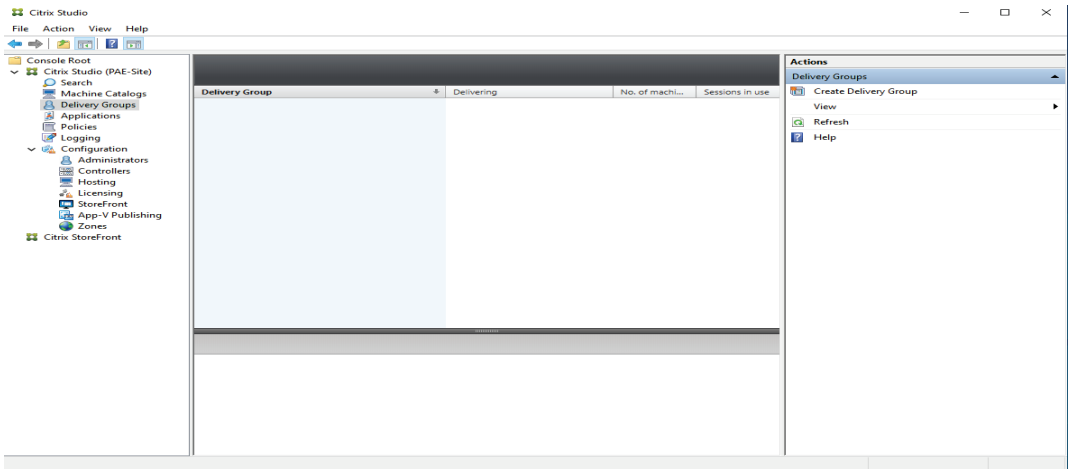
The VDA server will be added to the catalog and click Next.

6: Enter Machine Catalog name and description and click Finish.

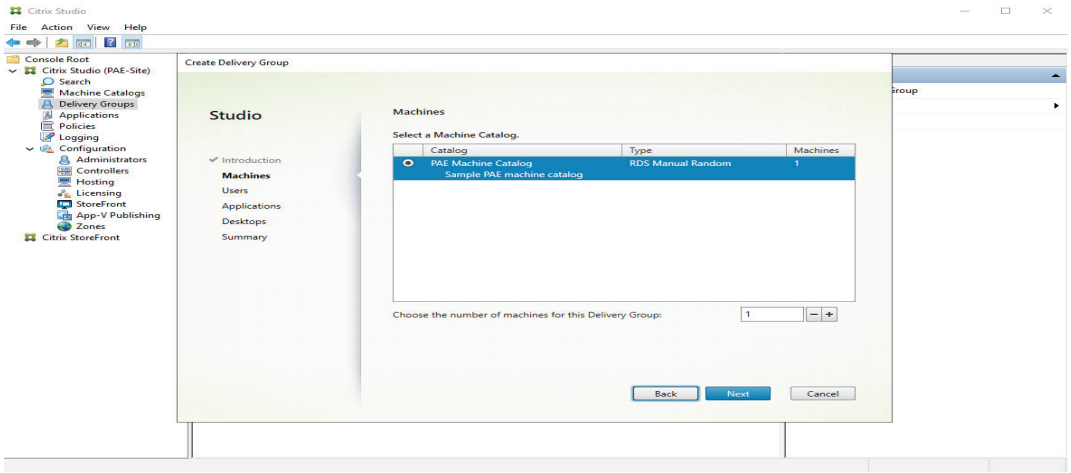


6.4.2 Create Delivery Group.

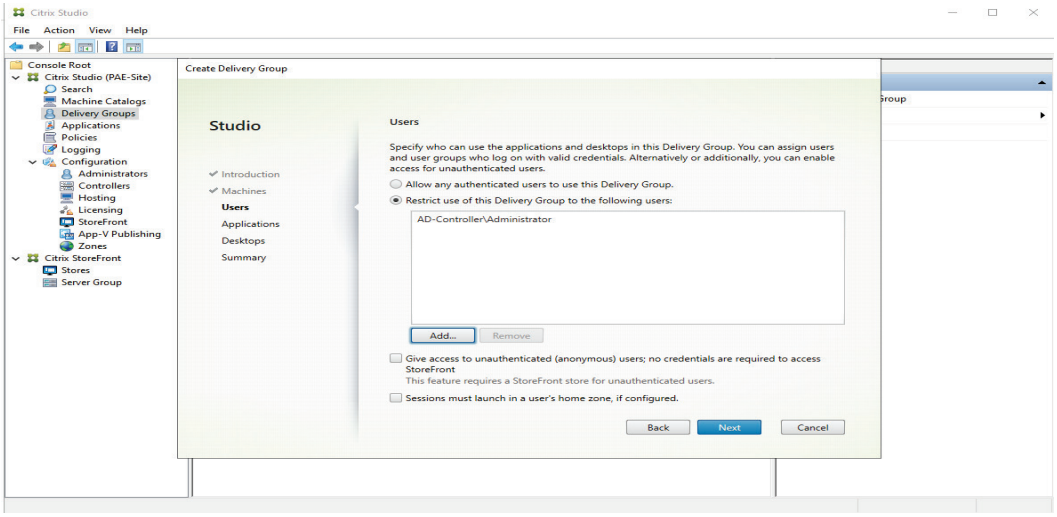
1: Select Delivery Group in the left pane, and then select Create Delivery Group in the action bar on the Right pane. And click Next.



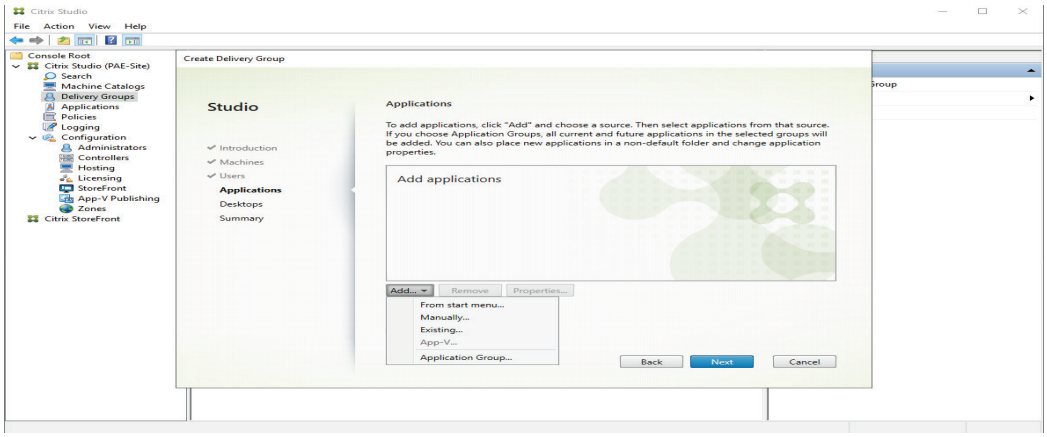
2: Select a Machine Catalog and click Next.



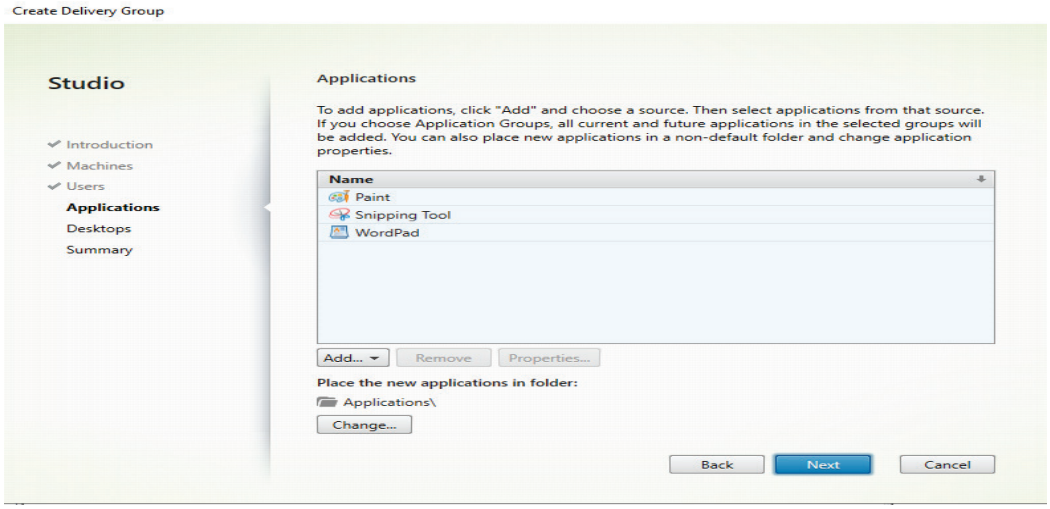
3: Keep the default option and click Next or select the Restrict use of the Delivery Group to the following users.



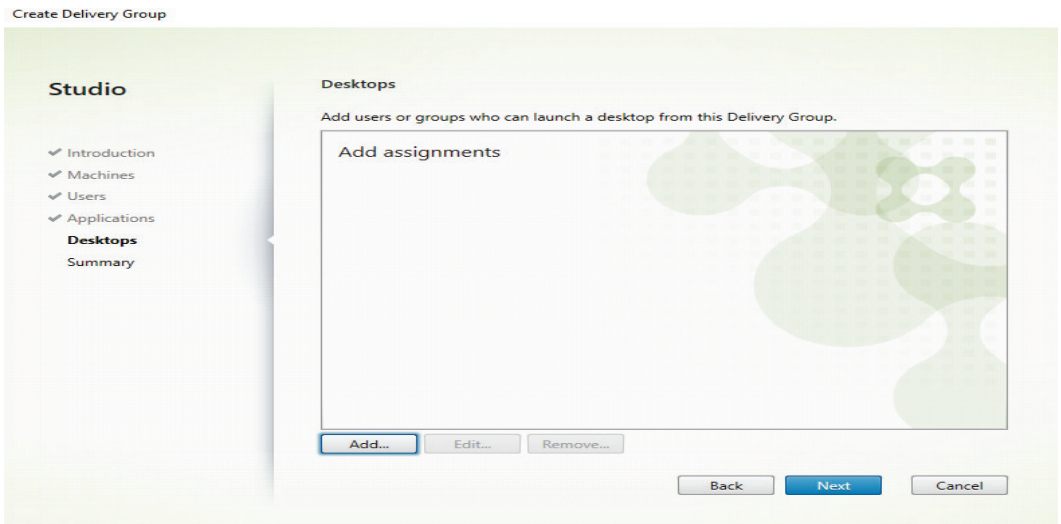
4: (Optional) Select the Applications by clicking Add and click on from start menu.



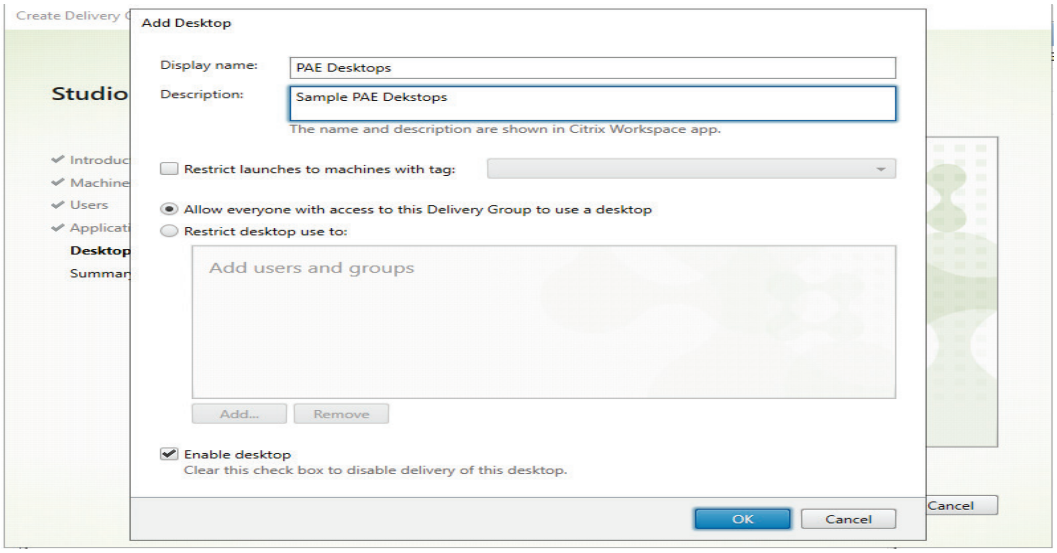
5: (Optional) Select the application for Virtualization and click Next.



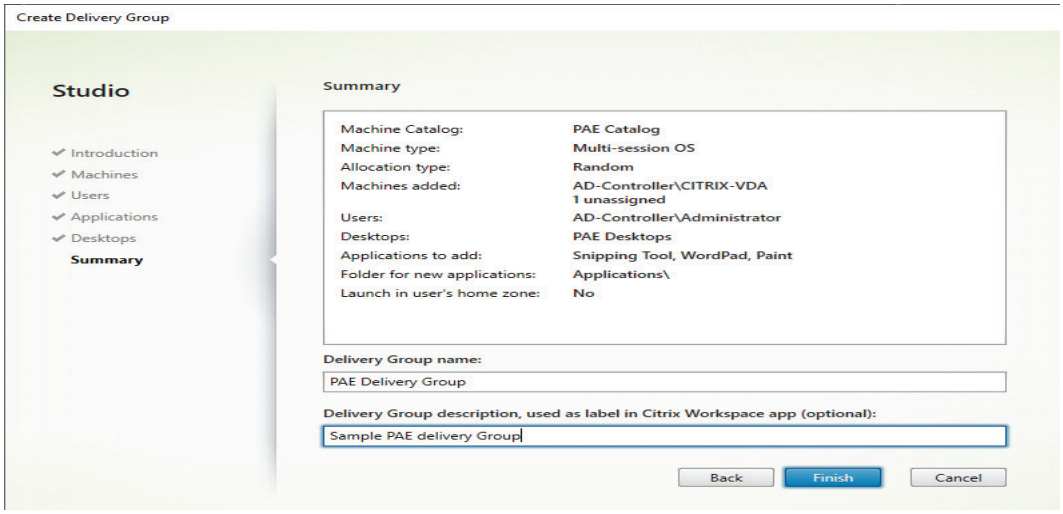
6: On Desktops page click Add button and add VDA server.



7: Enter Desktop Display name and Description, click OK.

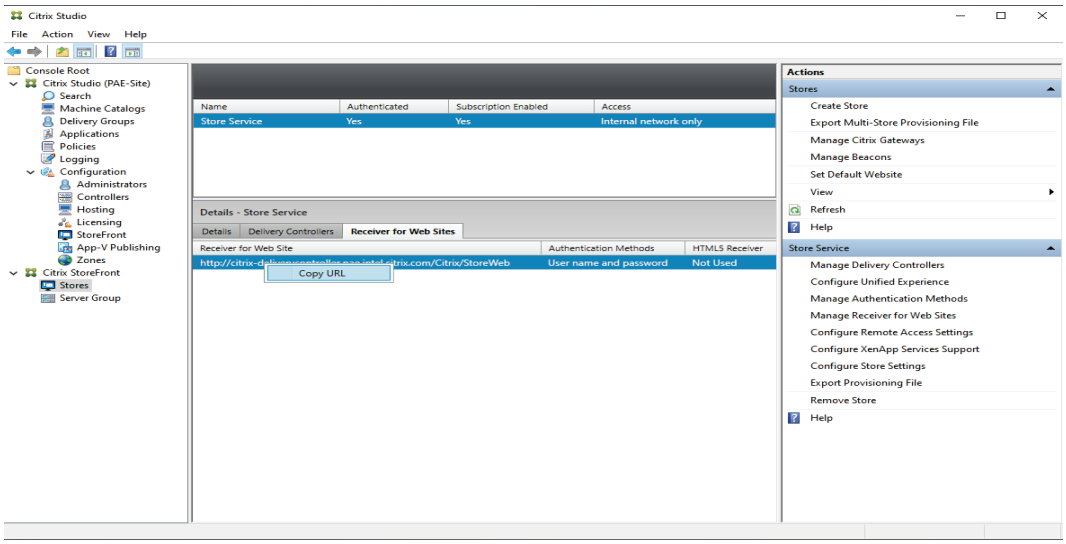


8: On the Summary page enter the Delivery Group Name and description. And click Finish.

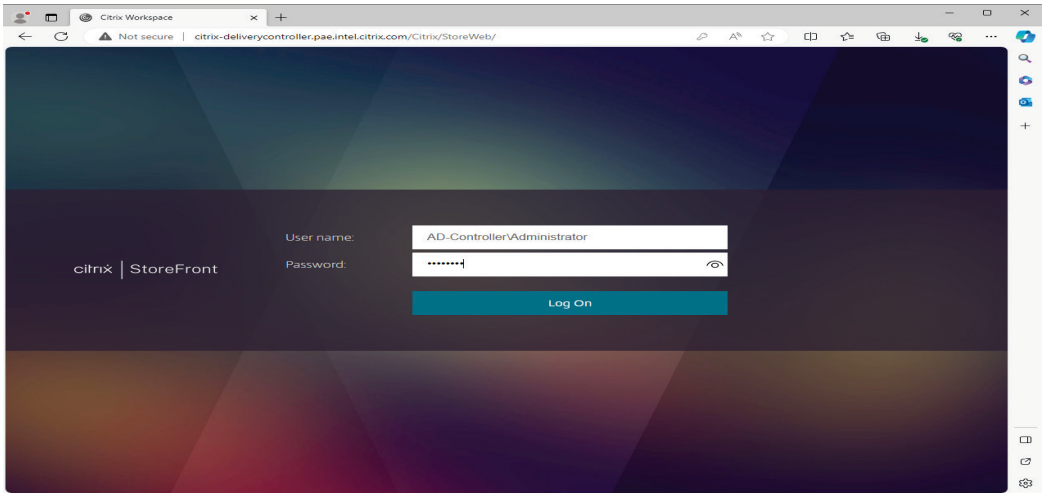


6.4.3 Access Virtualized App and Desktop

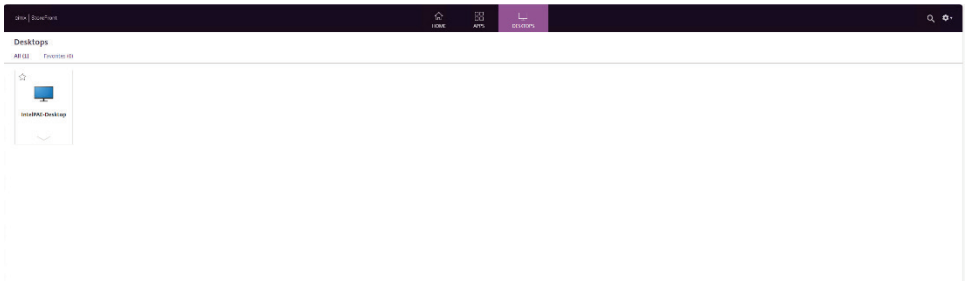
1: Login to the Delivery Controller VM and open Citrix Studio MMC application. Copy the Receiver for Web site URL.



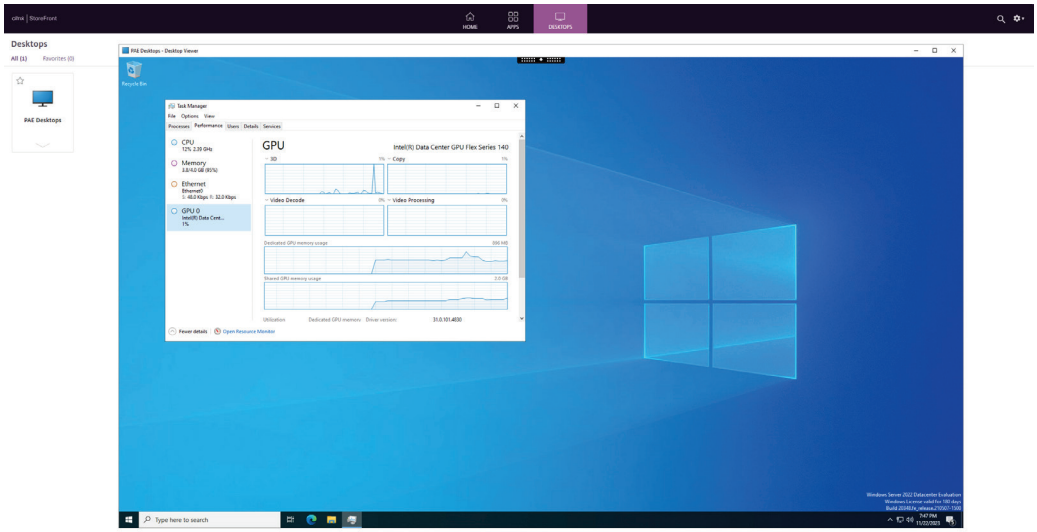
2: Open the web browser and past the URL, and Login to the StoreFront using Domain control credentials.



3: Click on the Desktops



4: Click on Desktops and verify the GPU utilization.



7 Known Issues and Workarounds

7.1 Anti-Aliasing

Issue: When running benchmarks or games with Anti-Aliasing set to ON or at AA level greater than two, it is observed that the overall performance is affected in terms of the benchmark scores and FPS.

Workaround: Intel has known issues with Anti-Aliasing (AA/MSAA). So, it is recommended to disable AA in the application settings before running them on Intel Data Center GPU Flex.

7.2 GPU Benchmarking with >1VF/SoC

Issue: During the execution of benchmarks or GPU-heavy workloads in a multi-VM/SOC scenario, users may encounter application hangs, VM disconnects, or Timeout Detection and Recovery (TDR) occurrences.

Workaround: This issue may stem from the safeguarding mechanism of Quality of Service (QoS) by the VF Scheduler. While it is generally recommended to adhere to default parameters according to official vGPU profiles, it is feasible to adjust parameters, particularly when benchmarking in profiles with more than one VF/SoC, to potentially enhance performance or alleviate functional failures.

To address this:

Execute the following command on the host shell:

```
esxcli intdcgpu configuration set -d $pci_address -v <VF Number> -p
<Option> -i <Value>
```

For instance:

- Set PT to 128 milliseconds for VM1:

```
esxcli intdcgpu configuration set -d 0000:56:00.0 -v 1 -p 11 -i
128000
```

If the issue persists, consider increasing the Execution_Quantum (EQ) value in multiples of the default EQ value:

- Set EQ to 32 for VM1:

```
esxcli intdcgpu configuration set -d 0000:56:00.0 -v 1 -p 10 -i 32
```

Note: It is crucial to proceed with caution when making these adjustments, particularly in production deployments, as they have the potential to cause QoS issues. Setting excessively high PT values may lead to complete Denial of Service (DoS) instances, which could manifest as GPU hangs or TDRs if certain VMs are running prolonged or malicious workloads.

7.3 Custom Configuration of VF Local Memory

Issue: Errors related to Base Address Register (BAR) size may be observed when attempting to change the Lmem of VF to certain values. This limitation is inherent in the ESXi Hypervisor with Resizable BAR support, where it is not feasible to allocate Lmem values greater than the allocated BAR size for the given VF count.

For example, in the V3 profile:

- Combinations that will work: 1 GB, 2 GB, 2 GB
- Combinations that may fail: 1 GB, 3 GB, 2 GB; 500 MB, 500 MB, 5 GB

Workaround: Currently, there is no workaround available. This issue stems from a limitation within the ESXi hypervisor. Intel is collaborating with VMware to address this matter.

7.4 SpecviewPerf Performance

Issue: Low scores are observed in SpecViewPerf when comparing against the Intel's Alchemist GPU.

Workaround: Currently, intel does not have a solution for this issue. Intel anticipates that it will be addressed and released in future Windows Graphics Driver builds.

7.5 Long Windows Driver Installation Times in Multiple GPU Case (>4 GPUs)

Issue: It may be observed that the installer takes a long time to complete the GPU driver installation in the case of multiple GPUs installed on the system. This is expected OS behavior. While installing the driver, the OS attempts to update the driver for devices that already have the driver installed.

Workaround: It has been noticed that the use of "DIIRFLAG_FORCE_INF" (which guarantees that every INF contained in the base INF will be installed) is the reason why the driver installation is taking longer than usual. This approach is authorized by Microsoft*. The installer team has introduced an external command-line option to disable the 'DIIRFLAG_FORCE_INF' flag to work around this problem. The usage command would be: **Installer.exe --doNotForceInf --unsigned**.

7.6 IGCC Support for Flex GPUs

Issue: IGCC is not enabled on Intel Data Center GPU Flex (VMs or Baremetal) to control the GPU Display settings.

Workaround: Since Flex GPU is in headless mode, it has been decided not to support IGCC on Intel Data Center GPU Flex Series.

7.7 Fixed Mode Scheduling

Issue: Performance drop is observed when using Fixed mode scheduling (schedule_if_idle=1).

Workaround: This issue is acknowledged, and efforts are underway to address it through updates to the scheduler. In the interim, Intel advises using Flexible mode to achieve better performance.

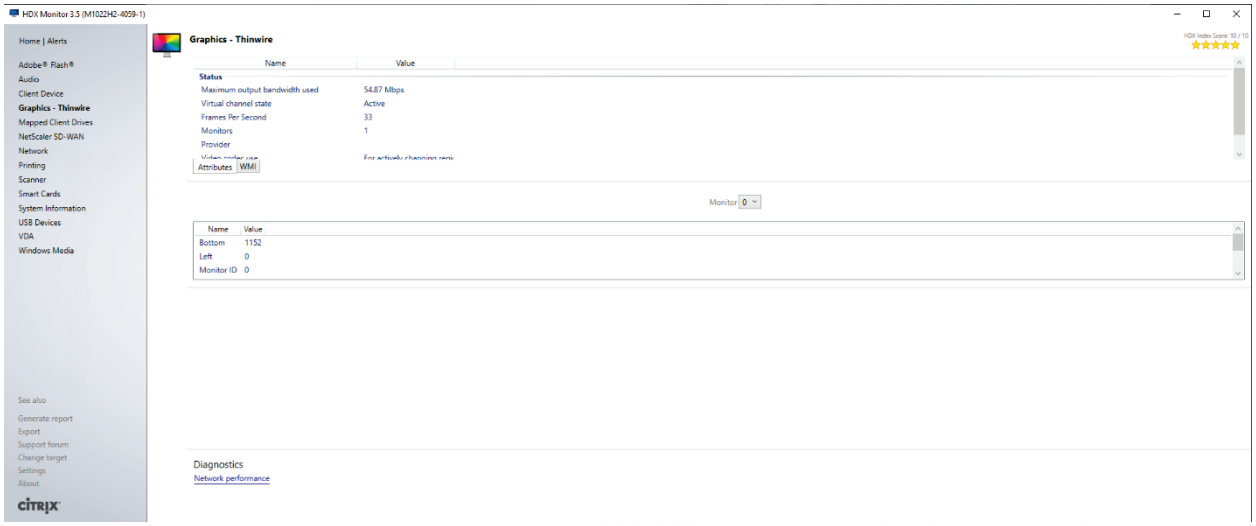
7.8 VF Telemetry Using Intel® XPU Manager (Intel® XPUM)

Issue: Intel XPUM does not display full GPU telemetry data inside the VM (in SRIOV mode).

Workaround: In the case of SRIOV, Intel XPUM will not be able to extract all the hardware telemetry information from inside the VM due to security reasons and hypervisor restrictions on accessing the hardware. It is recommended to utilize Microsoft tools such as Task Manager, GPU View, WMI API, PerfMon, and others.

8 References

- Admins can use the HDX monitor tool use validate the correct usage of the GPU and video encoding: https://support.citrix.com/article/CTX135817/hdx-monitor-3x



- Citrix recommends to install the Citrix Workspace App for Windows version 2311.1 or later: https://www.citrix.com/downloads/workspace-app/windows/workspace-app-for-windows-latest.html.

- More information on the HDX graphics policies and best practices can be found in the Tech Zone article: Design Decision HDX Graphics Overview