

VSI OpenVMS on VMware ESXi

Configuration Guide

Table of contents

1. Introduction	4
2. Before You Begin	5
2.1 VSI OpenVMS Version Requirements	5
2.2 VMware ESXi Version Requirements	5
2.3 Hardware Requirements	5
2.4 Recommended ESXi Virtual Machine Settings	5
2.5 Setting up the ESXi Environment	7
3. Creating a VMware ESXi Virtual Machine	8
3.1 Preparing to Create a VMware ESXi Virtual Machine	8
3.1.1 Downloading the VSI OpenVMS x86-64 ISO	8
3.1.2 Creating a Datastore in the ESXi Host Client	8
3.2 ESXi Virtual Machine Creation Procedure	10
3.2.1 Additional Configuration	13
3.2.1.1 Mandatory Steps	13
3.2.1.2 Optional Steps	15
4. Booting VSI OpenVMS on VMware ESXi	16
5. Connecting to the OpenVMS Console	17
6. Administering a VMware ESXi Virtual Machine	23
6.1 Adding Disks to Your ESXi VM	23
6.2 Adding a VMware Paravirtual SCSI Controller	25
6.2.1 Verification on OpenVMS	27
6.3 Adding Network Adapters to your ESXi VM	29
6.3.1 Next Steps	32
7. VMware ESXi VM Advanced Configuration	33
7.1 Secure Boot	33
7.1.1 Secure Boot Overview	33
7.1.2 Secure Boot Option on ESXi Virtual Machine	34
7.1.3 Adding OpenVMS Certificate to the Machine Owner Key Database	35
7.2 Configuring VMware ESXi Firewall	37
7.2.1 Connecting to the ESXi Command-Line Interface	37
7.2.2 Editing Configuration Files	38
7.3 Allowing MAC Address Changes	41
7.4 Fibre Channel Passthrough on ESXi Virtual Machine	42
7.4.1 Supported Platforms and Hardware	42
7.4.2 Setting up Fibre Channel Passthrough	42
7.5 VMware vMotion	45
7.5.1 Overview	45

7.5.2	Requirements	45
7.5.2.1	CPU Requirements	45
7.5.2.2	Network Interface Requirements	45
7.5.2.3	Storage Requirements	45
7.5.3	Creating a vMotion-Capable Environment and Performing vMotion Outline	46
7.5.4	vMotion: Detailed Configuration and Migration Procedure	47
7.5.4.1	Step 1: Set a Static IP on the ESXi Hosts	47
7.5.4.2	Step 2: Create iSCSI Shared Storage	47
7.5.4.3	Step 3: Install VMware vSphere to Manage the VMware Cluster	49
	Installation: Stage 1	49
	Installation: Stage 2	55
7.5.4.4	Step 4: Create a VMware Cluster and Add Hosts	58
	Adding Hosts	59
	Connecting the Hosts to the iSCSI Storage	61
7.5.4.5	Step 5: Setting Up Networking	61
	Creating a Dedicated Network for vMotion Traffic	63
7.5.4.6	Step 6 (optional): Verify That vMotion Works	65
7.5.4.7	Step 7: Create the OpenVMS x86-64 Virtual Machine	67
7.5.4.8	Step 8: Install VSI OpenVMS x86-64 and Join the Cluster	70
7.5.4.9	Step 9: Perform vMotion on the OpenVMS Guest	71
8.	Troubleshooting	73
8.1	Troubleshooting a VMware ESXi Virtual Machine Configuration	73
8.1.1	Access Denied Error	73
8.1.2	OPAO: Session Is Hung	73
8.1.3	Blocked Network Traffic	74
8.2	Known Issues and Limitations	76
8.2.1	Changing Settings of a Running Virtual Machine May Cause a Hang	76
8.2.2	Time of Day May Not Be Maintained Correctly in Virtual Machine Environments	76
8.2.3	Possible Issues with VMware Virtual Machines	76
8.3	Finetuning and Best Practices	77
8.3.1	vCPU and Scheduling	77
8.3.2	Memory	77
8.3.3	Storage	77
8.3.4	Network	77
8.3.5	Console and Serial Behavior	77

1. Introduction

This guide contains step-by-step instructions on setting up VSI OpenVMS x86-64 on a VMware ESXi virtual machine from scratch.

Learn how to use the console, configure firewall, and set up advanced options for production use.

2. Before You Begin

Review the requirements and prerequisites below to prepare to configure your VMware ESXi virtual machine (VM).

2.1 VSI OpenVMS Version Requirements

VSI OpenVMS [Version 9.2-2](#) + [Update 2](#) or higher

2.2 VMware ESXi Version Requirements

VMware ESXi Version 8.0.x

2.3 Hardware Requirements

See the [Supported Platforms](#) page for the currently supported hardware.

2.4 Recommended ESXi Virtual Machine Settings

VSI recommends that your OpenVMS x86-64 virtual machine be configured with the following settings depending on your version of VSI OpenVMS:

V9.2-2

Component	Requirements
Minimum number of CPUs	2
Memory	8 GB. If the installation fails due to lack of memory, you can temporarily increase it for the installation and reduce it afterwards if your host system has enough RAM to allocate.
Operating system	Other 64-bit
Virtual disk size	At least 15 GB for the system files. Optionally, if disk space is limited, use a dump off system disk (DOSD); the recommended minimum DOSD size is 8 GB.
Boot option	• Disable Secure Boot (if present) • Enable UEFI or EFI (BIOS is not supported)
Console communication	Serial port using a raw TCP connection. Note that only COM1 serial port is supported.
Serial line	An additional serial line for non-console login.
Network	Up to 10 E1000 adapters.

Component	Requirements
CD/DVD device	Physical or virtual, with the OpenVMS installation kit (.ISO file).

V9.2-3

Component	Requirements
CPU cores	A minimum of 2 and a maximum of 32.
Memory	6 GB. If the installation fails due to lack of memory, you can temporarily increase it for the installation and reduce it afterwards if your host system has enough RAM to allocate.
Operating system	Other 64-bit
Virtual disk size	A minimum of 30 GB and a maximum of 1.98 TB. Optionally, if disk space is limited, use a dump off system disk (DOSD); the recommended minimum DOSD size is 8 GB.
Boot option	• Disable Secure Boot (if present) • Enable UEFI or EFI (BIOS is not supported)
Console communication	Serial port using a raw TCP connection. Note that only COM1 serial port is currently supported. Guest Console can be used as an alternative to serial ports.
Serial line	Optionally, an additional serial line for non-console login.
Network	• An E1000 or an E1000e adapter. • A para-virtualized Network Interface Card (NIC): VMXNET 3. Up to 10 network adapters in total.
CD/DVD device	Physical or virtual, with the OpenVMS installation kit (.ISO file).

E9.2-4

Component	Requirements
CPU cores	A minimum of 2 and a maximum of 32.
Memory	6 GB. If the installation fails due to lack of memory, you can temporarily increase it for the installation and reduce it afterwards if your host system has enough RAM to allocate.
Operating system	Other 64-bit

Component	Requirements
Virtual disk size	A minimum of 30 GB and a maximum of 1.98 TB. Optionally, if disk space is limited, use a dump off system disk (DOSD); the recommended minimum DOSD size is 8 GB.
Boot option	Enable UEFI or EFI (BIOS is not supported)
Console communication	Serial port using a raw TCP connection. Note that only COM1 serial port is currently supported. Guest Console can be used as an alternative to serial ports.
Serial line	Optionally, an additional serial line for non-console login.
Network	• An E1000 or an E1000e adapter. • A para-virtualized Network Interface Card (NIC): VMXNET 3. Up to 10 network adapters in total.
CD/DVD device	Physical or virtual, with the OpenVMS installation kit (.ISO file).

2.5 Setting up the ESXi Environment

Before you can begin to configure your ESXi virtual machine, you need to set up your ESXi environment.

1. Familiarize yourself with the requirements and supported platforms listed in the following resources:
 - Find the list of supported platforms in the [Broadcom Hardware Compatibility Guide](#).
 - Learn about hardware requirements for the ESXi environment on the [Broadcom website](#).
 - Use the information published on your hardware vendor's website to make sure your hardware is compatible with VMware ESXi.
2. Download and install the ESXi operating system. For instructions on how to do so, refer to the [Broadcom support portal](#).

3. Creating a VMware ESXi Virtual Machine

3.1 Preparing to Create a VMware ESXi Virtual Machine

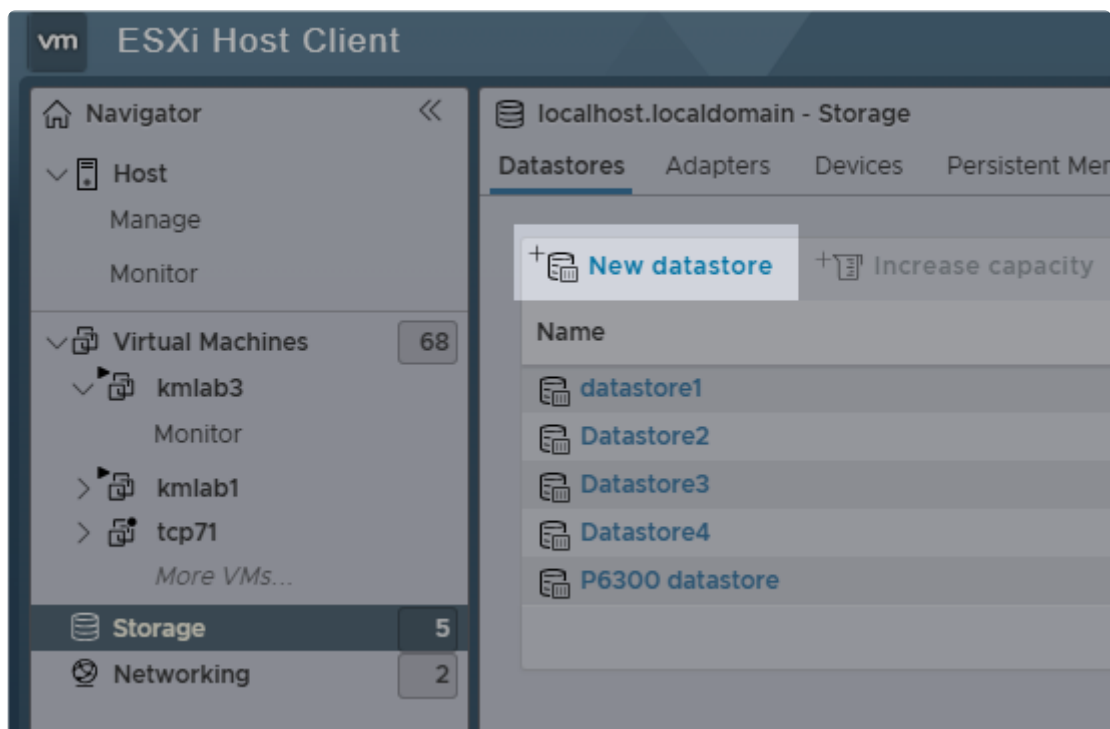
3.1.1 Downloading the VSI OpenVMS x86-64 ISO

Download the archive containing the VSI OpenVMS x86-64 operating environment image file (ISO) from the [VSI Service Portal](#). Unzip it and copy the ISO file to a location locally accessible to the browser that you will use to connect to the **ESXi Host Client**.

3.1.2 Creating a Datastore in the ESXi Host Client

Before you create your virtual machine, you must create a datastore.

1. In the browser, enter the ESXi host IP address to bring up the **ESXi Host Client**. At the login screen, enter your credentials (created during the ESXi installation) and click **Log in**.
2. In the left pane of the VMware ESXi window, go to **Navigator > Storage**. In the right pane, click **New datastore**.



A new window will pop up.

3. The **New datastore** wizard will guide you through the steps necessary to create a datastore.
 - a. **Select creation type:** Make sure that the **Create new VMFS datastore** option is selected and click **Next**.
 - b. **Select device:** Enter a name for the new datastore and select a device where the datastore will be created. Click **Next**.

- c. **Select partitioning options:** Adjust the size of your datastore as appropriate for your environment needs and make sure that **VMFS6** version is selected in the drop-down list.

Click **Next**.

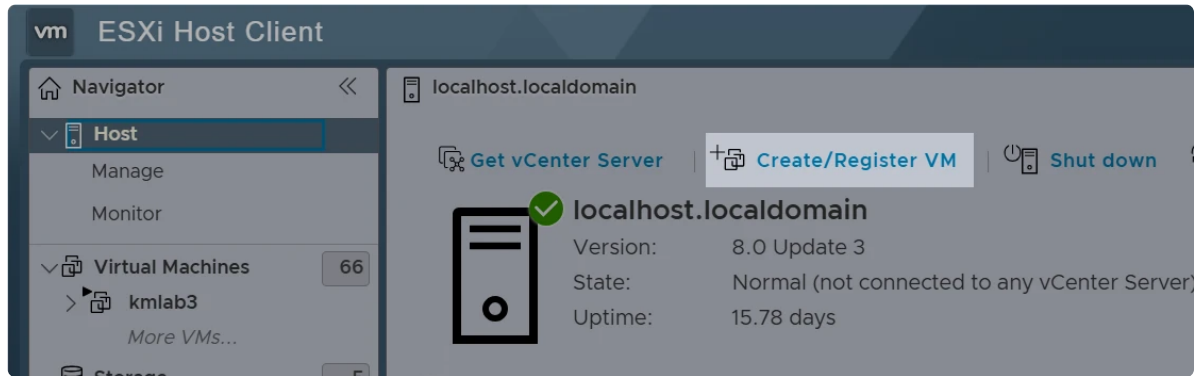
- d. **Ready to complete:** Check your configuration and, if necessary, click the **Back** button and edit the values.

- 4. Click **Finish**.

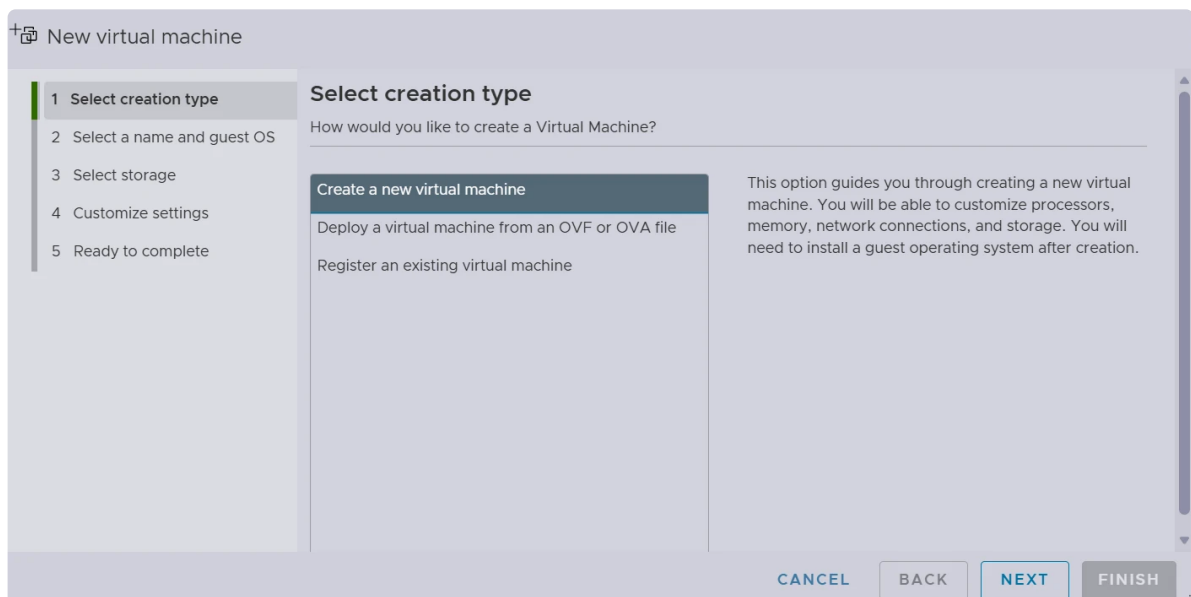
3.2 ESXi Virtual Machine Creation Procedure

Perform the following steps to create a VMware ESXi virtual machine for use with VSI OpenVMS x86-64. The instructions in this section were tested on VMware ESXi 8.0.

1. In the left pane of the **ESXi Host Client** window, click **Host**, then click **Create/Register VM** in the right pane.



2. A **New virtual machine** wizard will open. It will guide you through the steps needed to create a new ESXi virtual machine. In the right pane, you will be able to choose the parameters and specify values to be used in your virtual machine configuration.



3. **Select creation type:** Make sure that the **Create a new virtual machine** option is selected, then click **Next**.
4. **Select a name and guest OS:**
 - In the **Name** field, enter a name for your VM.
 - In the **Compatibility** drop-down menu, choose the desired version of the ESXi virtual machine.
 - In the **Guest OS family** drop-down menu, select **Other**.
 - In the **Guest OS version** drop-down menu, select **Other (64-bit)**.

Click **Next**.

5. **Select Storage:** Choose the datastore that you created in [the previous section](#).
6. **Customize settings:** At this stage, you must specify certain values that are required for VSI OpenVMS. Scroll down or expand categories to find the necessary parameters and specify the following mandatory values for the **Virtual Hardware**:

- **CPU:** a minimum of 2 and up to 32.¹
- **Memory:** a minimum of 6 GB.
- **Hard disk 1:** a minimum of 30 GB and a maximum of 1.98 TB.
 - **Disk provisioning:** Thick-provisioned, lazily zeroed. Thin provisioning is *not* supported on OpenVMS.
 - **Controller location:** Choose the appropriate controller.

 Note

- In order to assign a VMware Paravirtual controller to the disk, refer to the [Adding a VMware Paravirtual Controller](#) section.
- OpenVMS on VMware ESXi supports up to four LSI Logic Parallel SCSI controllers per virtual machine.

Find an up-to-date list of supported controllers on the [Supported Platforms](#) page.

- **Network adapter 1:** VM Network.
 - **Adapter type:** For a list of supported adapters, refer to the [Recommended ESXi Virtual Machine Settings](#) for your version of OpenVMS. Click the **Add network adapter** tab to add multiple adapters.

You can add up to 10 network adapters.

- **CD/DVD drive 1:** Select **Datastore ISO file** from the drop-down menu. In the pop-up window, find and select your VSI OpenVMS ISO installer file.

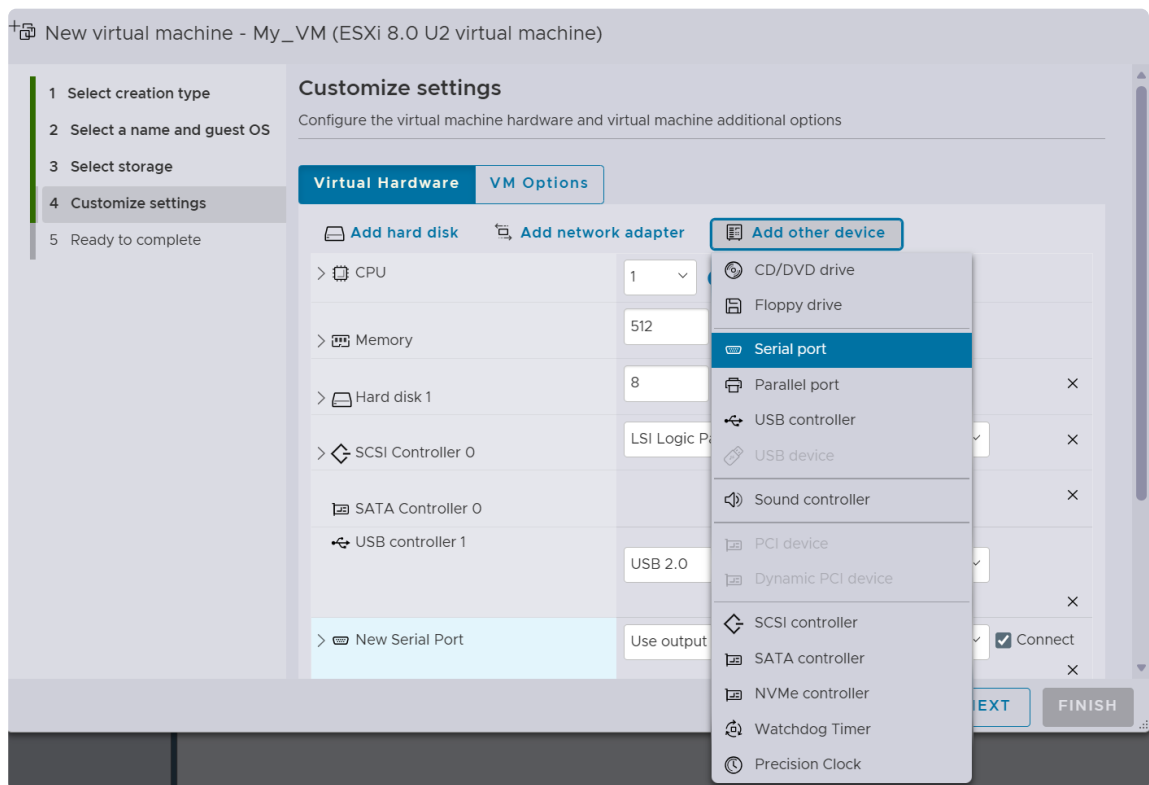
After you click **Select** in the pop-up window, the **CD/DVD media** field in the **New virtual machine** window will automatically display the path to your VSI OpenVMS ISO file.

 Attention

Make sure that the ISO file is mapped to the SATA controller by selecting **SATA controller *n*** from the **Controller location** drop-down menu.

- Add a serial port by clicking the **Add other device** tab at the top of the window and selecting **Serial port**. You will see the **New Serial Port** category appear among other categories.

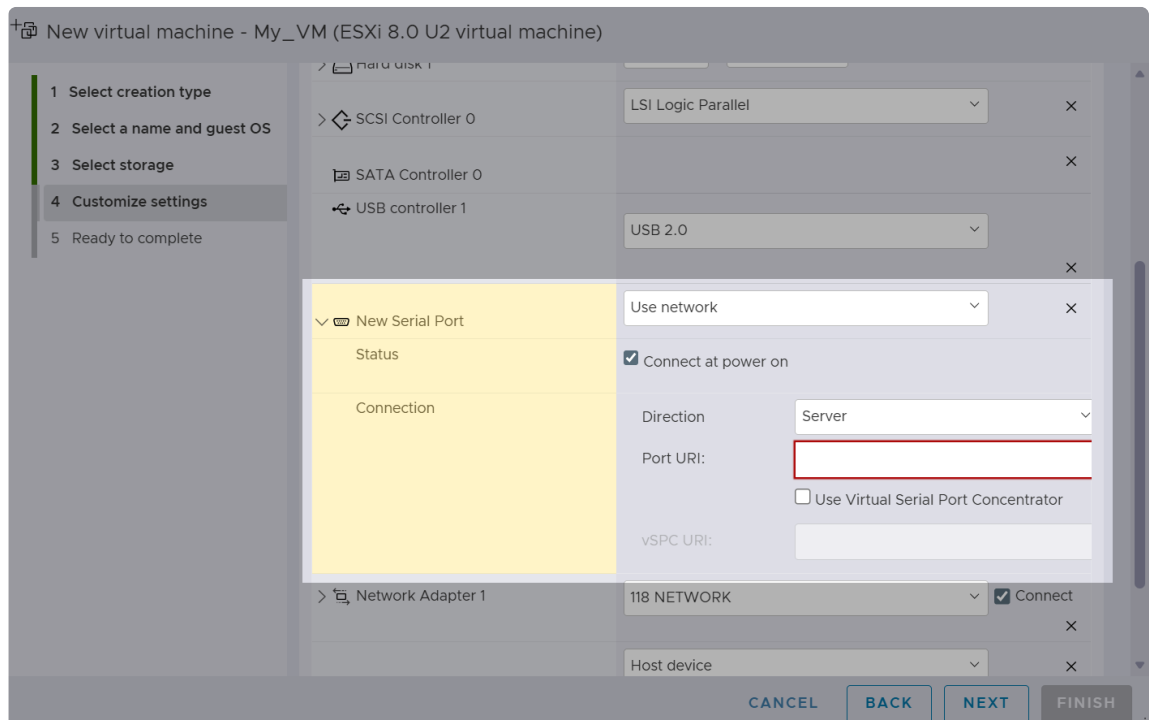
1. Expand the **CPU** section by clicking on it to customize the distribution of cores between virtual sockets.



Choose **Use network** from the drop-down menu and specify the port in the **Port URI** field in the following format: *protocol://:port*. For example:

```
tcp://:8045
```

Make sure that **Server** is selected in the **Direction** drop-down menu.



⚠ Attention

For the connection via serial port to work, you need to configure the ESXi firewall as described in [Configuring VMware ESXi Firewall](#).

Click **Next**.

7. **Ready to complete:** In the right pane, you will see the parameters and values that will be used in your virtual machine configuration. Make sure to review them and check that they meet the [recommended ESXi virtual machine settings for your VSI OpenVMS version](#). If necessary, click the **Back** button and edit the values.

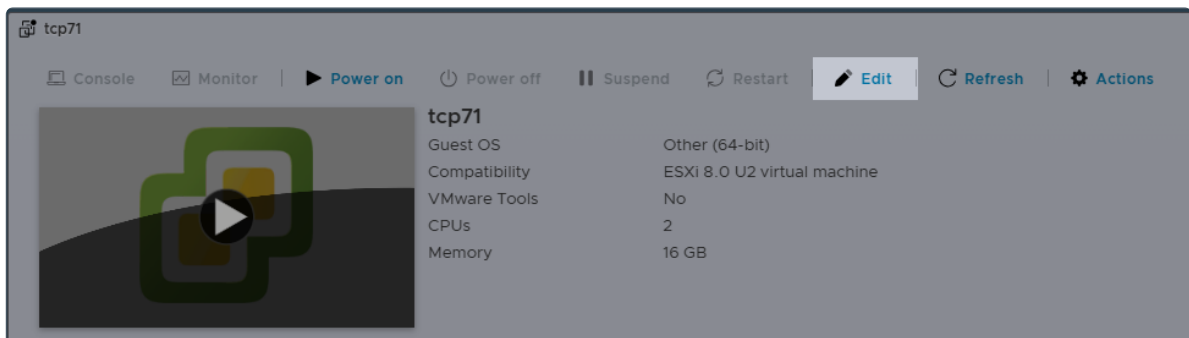
8. Click **Finish**.

3.2.1 Additional Configuration

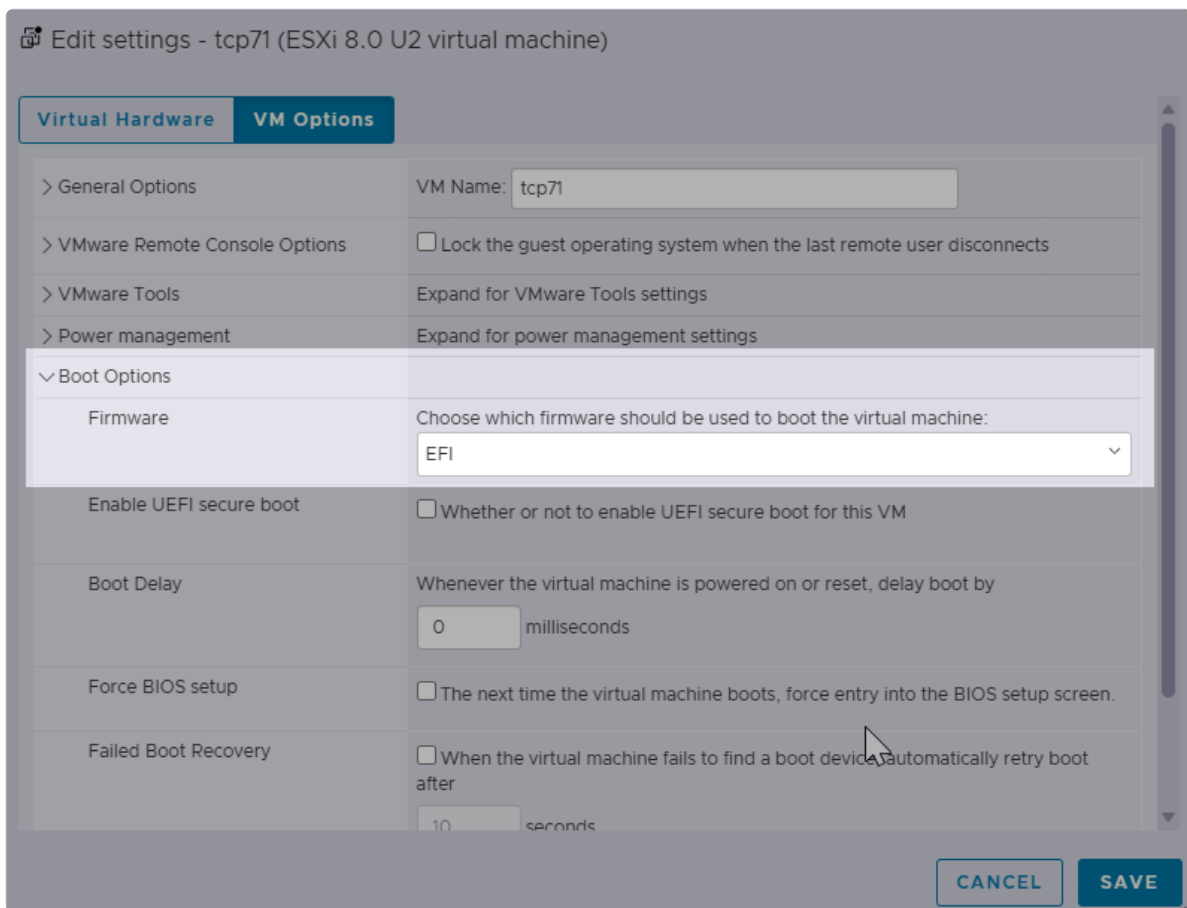
3.2.1.1 Mandatory Steps

You must perform the following additional configuration steps after you have created a virtual machine.

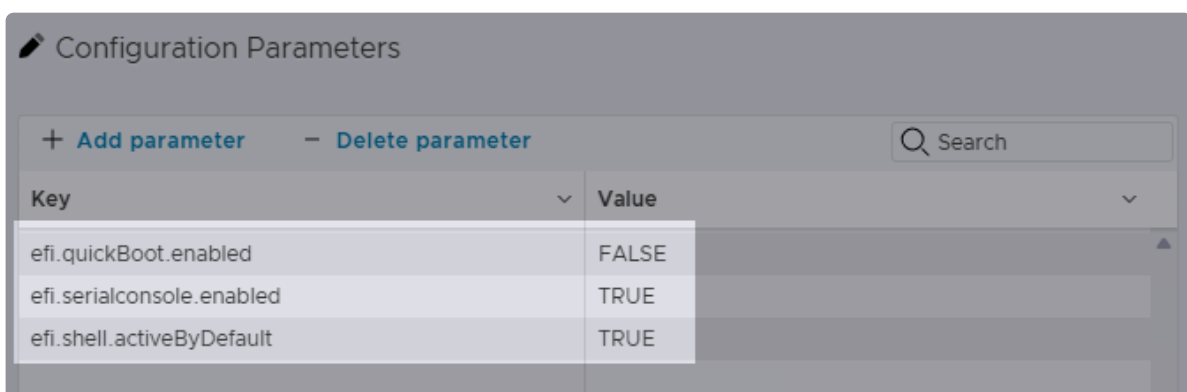
1. In the left pane of the **ESXi Host Client**, click on the virtual machine that you have just created. Then click **Edit** in the main window. A new pop-up window will open.



2. Click the **VM Options** button at the top of the window, then select the **Boot Options** category to see the firmware options. Choose **EFI** from the drop-down list.



3. Expand the **Advanced** section, click the **Edit Configuration** button in the right pane. The **Configuration Parameters** window will open.
4. Use the **Add parameter** button to add the following parameters:
 - efi.quickBoot.enabled = FALSE
 - efi.serialconsole.enabled = TRUE
 - efi.shell.activeByDefault = TRUE



5. Click **OK**.
6. Click **Save** in the **Edit settings** window.

3.2.1.2 Optional Steps

The parameters specified below are not required but are generally recommended by VSI to ensure your virtual machine works properly.

1. In the left pane of the **ESXi Host Client**, click on the virtual machine that you have just created. Then click **Edit** in the main window. A new pop-up window will open.
2. Click the **VM Options** button, expand the **VMware Remote Console Options** category, and uncheck the boxes as shown below:

Edit settings - tcp71 (ESXi 8.0 U2 virtual machine)

Virtual Hardware **VM Options**

> General Options VM Name: tcp71

▼ VMware Remote Console Options

Guest OS lock	☐ Lock the guest operating system when the last remote user disconnects
Maximum number of sessions	☐ Limit the number of simultaneous connections to this virtual machine 40

> VMware Tools Expand for VMware Tools settings

> Power management Expand for power management settings

> Boot Options Expand for boot options

> Advanced Expand for advanced settings

> Fiber Channel NPIV Expand for fiber channel NPIV

CANCEL **SAVE**

3. Click **Save**.

4. Booting VSI OpenVMS on VMware ESXi

Different booting options are available depending on your version of VSI OpenVMS.

V9.2-3 and earlier

At the `BOOTMGR>` prompt, execute **BOOT *device-name***, where *device-name* is the name of the virtual CD/DVD device to which your VSI OpenVMS installation ISO is assigned.

For more information, see the [VSI OpenVMS x86-64 Boot Manager User Guide](#).

E9.2-4

- At the `BOOTMGR>` prompt, execute **BOOT *device-name***, where *device-name* is the name of the virtual CD/DVD device to which your VSI OpenVMS installation ISO is assigned.

For more information, see the [VSI OpenVMS x86-64 Boot Manager User Guide](#).

- Starting with VSI OpenVMS E9.2-4, you can boot OpenVMS with Secure Boot enabled. However, you must either boot the system once with Secure Boot disabled or follow the procedure for importing the required certificate manually.

Refer to the [Secure Boot](#) section for more details.

5. Connecting to the OpenVMS Console

You can choose to connect to your OpenVMS operator terminal via the Guest Console, a serial port, or a named pipe.

⚠ Important

Make sure that the port used by your VM can go through the ESXi firewall. If you are having trouble at this stage, refer to the [Configuring Firewall](#) section or contact the ESXi administrator in your company.

via Guest Console

1. From your browser, connect to the **ESXi Host Client**.
2. In the left pane, click **Virtual Machines** and then, on the right, click the name of the virtual machine where you want to boot OpenVMS. You will see the selected virtual machine configuration details page.
3. Click **Power on** at the top of the page. Alternatively, click the “play” button (▶) on the VM browser console preview window to start your virtual machine. The VSI OpenVMS Boot Manager window should appear.

If the Boot Manager window did not open in a pop-up window, try clicking the browser console VM preview window (🖥) or click the **Console** button above and choose the option that suits your needs:



4. At the `BOOTMGR>` prompt, execute the following command:

```
BOOTMGR> OPA0
```

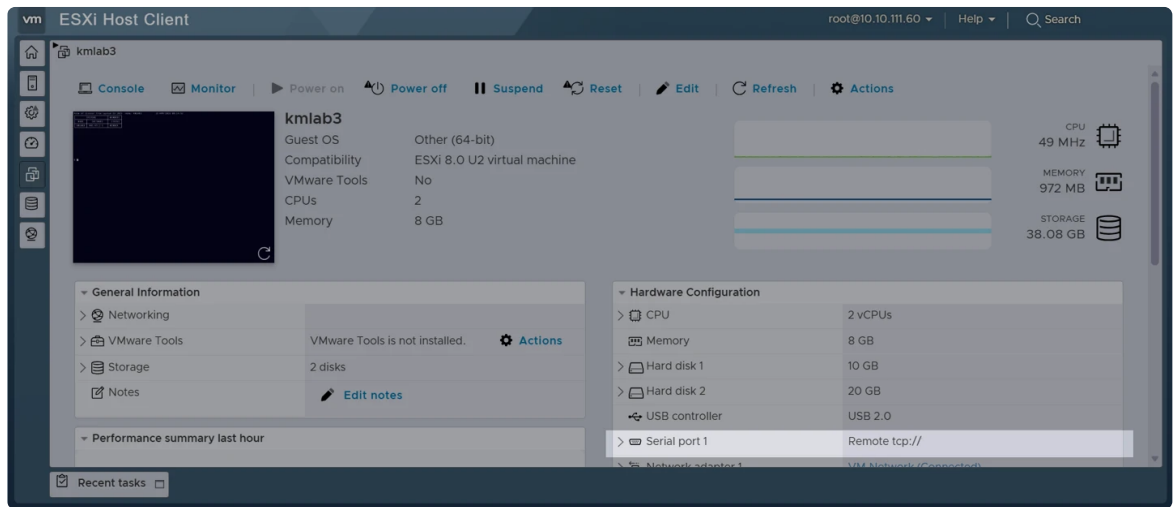
For more information about the Guest Console, refer to the [VSI OpenVMS x86-64 V9.2-3 Installation Guide](#) and the [VSI OpenVMS x86-64 Boot Manager User Guide](#).

📝 Note

When the connection via the Guest Console is active, it is impossible to connect to the running OpenVMS system using a serial port.

via Serial Port

1. Open your terminal emulator (e.g. PuTTY) and specify the IP address and port of your virtual machine that can be looked up in the ESXi Host Client as shown below:



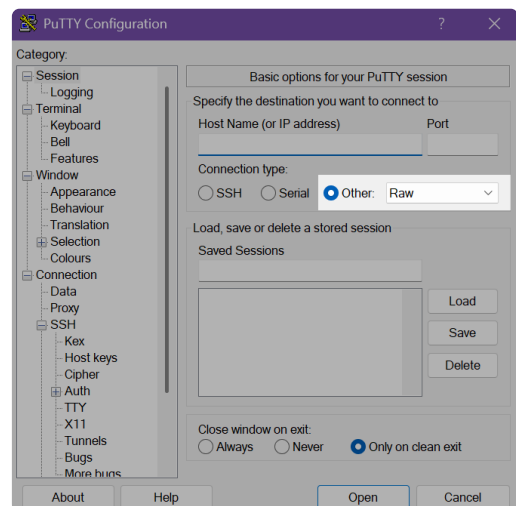
Note

The following steps contain examples of how to configure the PuTTY terminal emulator.

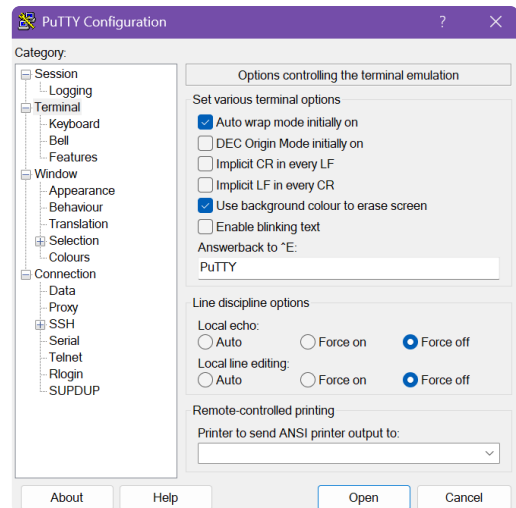
While VSI tests with PuTTY, other terminal utilities can also be used, but may have different restrictions and incompatibilities.

2. Edit your terminal emulator settings as specified below:

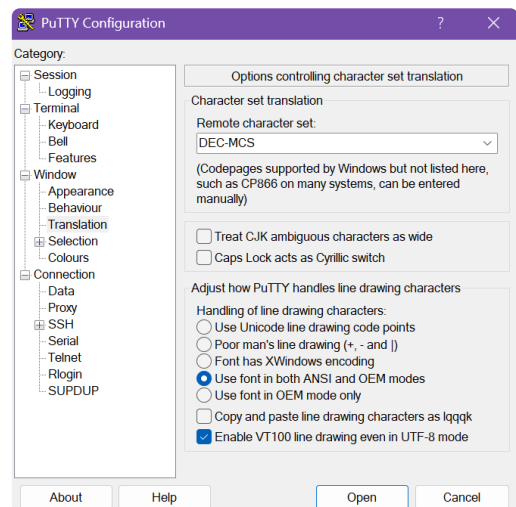
- **Connection type:** Raw



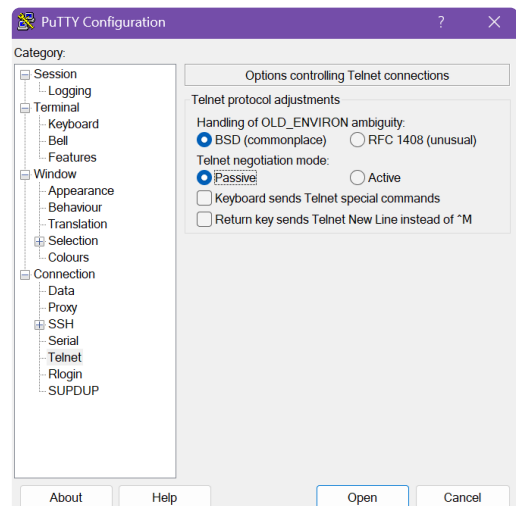
- **Implicit CR in every LF:** Unchecked
- **Implicit LF in every CR:** Unchecked
- **Local echo:** Force off
- **Local line editing:** Force off



- **Remote character set:** DEC-MCS
- **Enable VT100 line drawing even in UTF-8 mode:** Checked

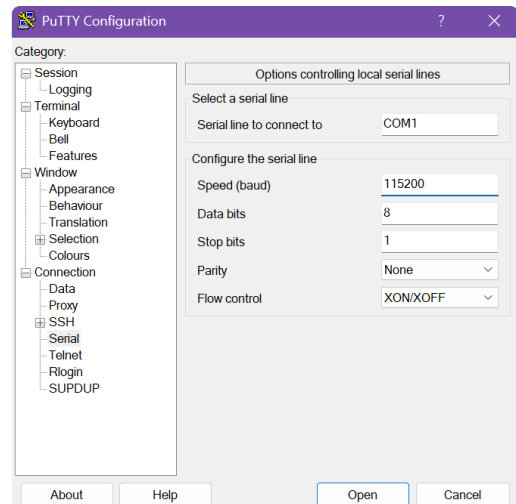


- **Telnet negotiation mode:** Passive
- **Return Key Sends Telnet New Line instead of ^M:** Unchecked

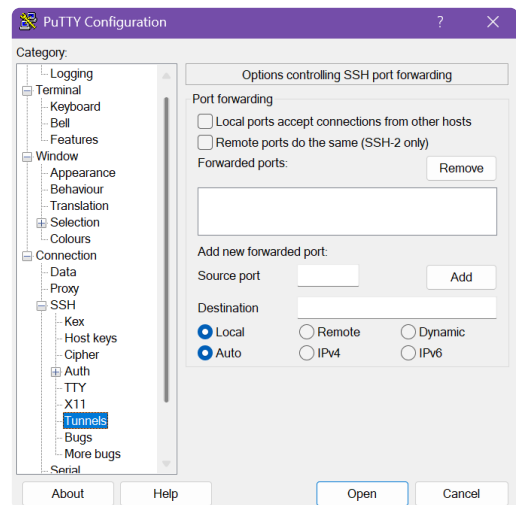


If connecting via a named pipe:

- **Speed:** 115200
- **Data Bits:** 8
- **Stop Bits:** 1
- **Parity:** None
- **Flow Control:** XON/XOFF



*If connecting remotely via SSH through your VPN, make sure that the **SSH Port Forwarding** is set up in your terminal emulator.*



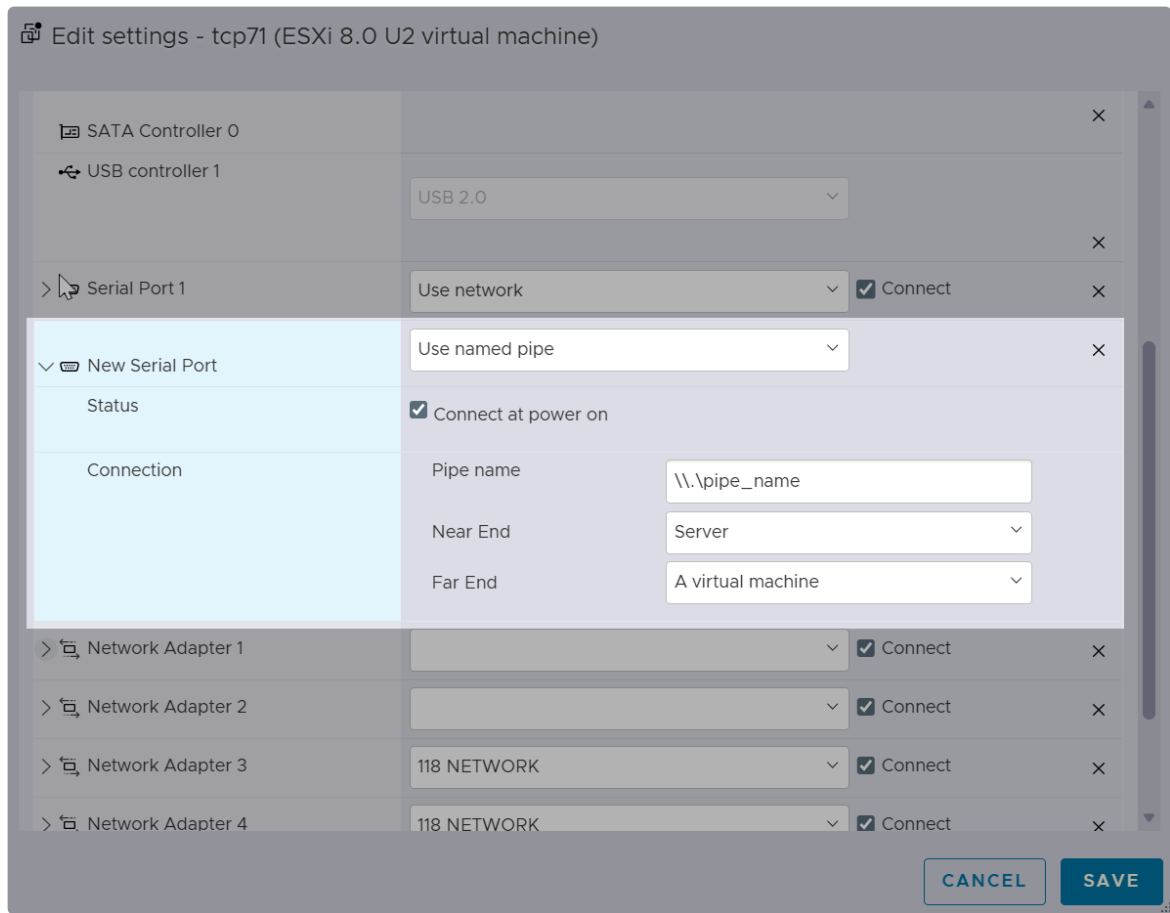
via Named Pipe

A virtual serial port connected to a named pipe allows access to the OpenVMS console over the network without any physical serial hardware. This is useful when multiple administrators need console access from different systems, or when ESXi is running on hardware without usable serial ports.

A named pipe forms a virtual connection between two virtual serial ports on virtual machines running on the same ESXi host. One of these virtual machines is your OpenVMS system, the other is any other system (e.g. Windows or Linux), from which you will connect to your OpenVMS system.

1. Power off the OpenVMS virtual machine.
2. In the left pane of the **ESXi Host Client**, click on the virtual machine that will be configured as a server and is a non-OpenVMS system. Then click **Edit** in the main window. A new pop-up window will open.
3. Add a new serial port by clicking the **Add other device** tab at the top of the window and selecting **Serial port**. You will see the **New Serial Port** category appear among other categories.
 - a. Choose **Use named pipe** from the drop-down menu.
 - b. Specify the pipe name in the following format: `\\.\pipe_name`
 - c. Select **Server** as **Near End**.

d. Select **A virtual machine** as **Far End**.



e. Click **Save**.

4. In the left pane of the **ESXi Host Client**, click on the virtual machine that will be configured as a client and is an OpenVMS system. Then click **Edit** in the main window. A new pop-up window will open.
5. Add a new serial port by clicking the **Add other device** tab at the top of the window and selecting **Serial port**. You will see the **New Serial Port** category appear among other categories.
 - a. Choose **Use named pipe** from the drop-down menu.
 - b. Specify the same pipe name as for the server side in the following format: `\\.\pipe_name`
 - c. Select **Client** as **Near End**.
 - d. Select **A virtual machine** as **Far End**.

Edit settings - tcp71 (ESXi 8.0 U2 virtual machine)

SATA Controller 0			
USB controller 1	USB 2.0		
Serial Port 1	Use network	☒ Connect	
New Serial Port	Use named pipe		
Status	☒ Connect at power on		
Connection	Pipe name	\\.\pipe_name	
	Near End	Client	
	Far End	A virtual machine	
Network Adapter 1		☒ Connect	
Network Adapter 2		☒ Connect	
Network Adapter 3	118 NETWORK	☒ Connect	
Network Adapter 4	118 NETWORK	☒ Connect	

CANCEL **SAVE**

e. Click **Save**.

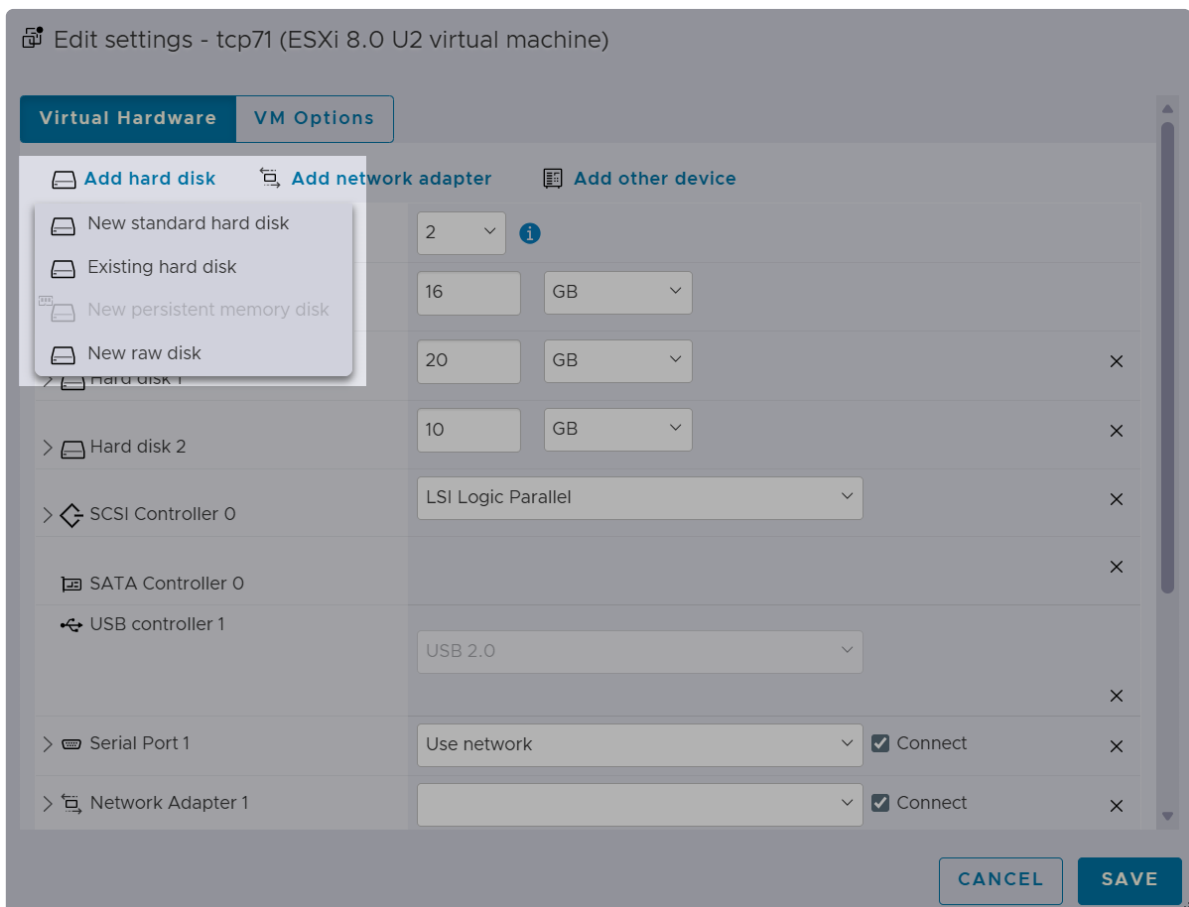
- Access the console on the OpenVMS system by first logging in to the server system and then using the terminal emulator to establish a connection to the OpenVMS system via the serial port as described earlier in [Connecting to the OpenVMS Console](#).

Using the named pipe functionality, map COM1/OPA0: on the OpenVMS system to a pipe on the server system on which a terminal emulator is installed.

6. Administering a VMware ESXi Virtual Machine

6.1 Adding Disks to Your ESXi VM

1. Open your virtual machine configuration page by clicking **Virtual Machines** and selecting your VM from the list.
2. On your virtual machine configuration page, click **Edit**. In the **Edit Settings** window, click **Add Hard Disk** and select **New standard hard disk** or **Existing hard disk**.



- If you have selected **New standard hard disk**, a **New Hard Disk** category will appear in the list settings.
 - a. Expand the category and make sure that **Disk Provisioning** is set to **Thick-provisioned, lazily zeroed**.
 - b. Specify the amount of storage space to allocate to your new hard disk and proceed to [Step 3](#).

✖ Restriction

Volumes larger than 1.98 TB are not supported on VSI OpenVMS.

- If you have selected **Existing hard disk**, a pop-up window will open where you can select a hard disk that you wish to use with your VM.
 - a. Locate a hard disk that is not used by any other virtual machine.
 - b. Click **Save** and proceed to [Step 3](#).
- 3. Assign the appropriate controller to the disk using the drop-down menu in the **Controller location** field. Match the controller type to the OpenVMS recommendations for your release and your environment needs.
- 4. Click **Save**.

 Tip

ESXi supports exclusively VMDK disks. To learn how to convert a different-format disk into .vmdk, refer to the [Converting Hypervisor Images](#) article.

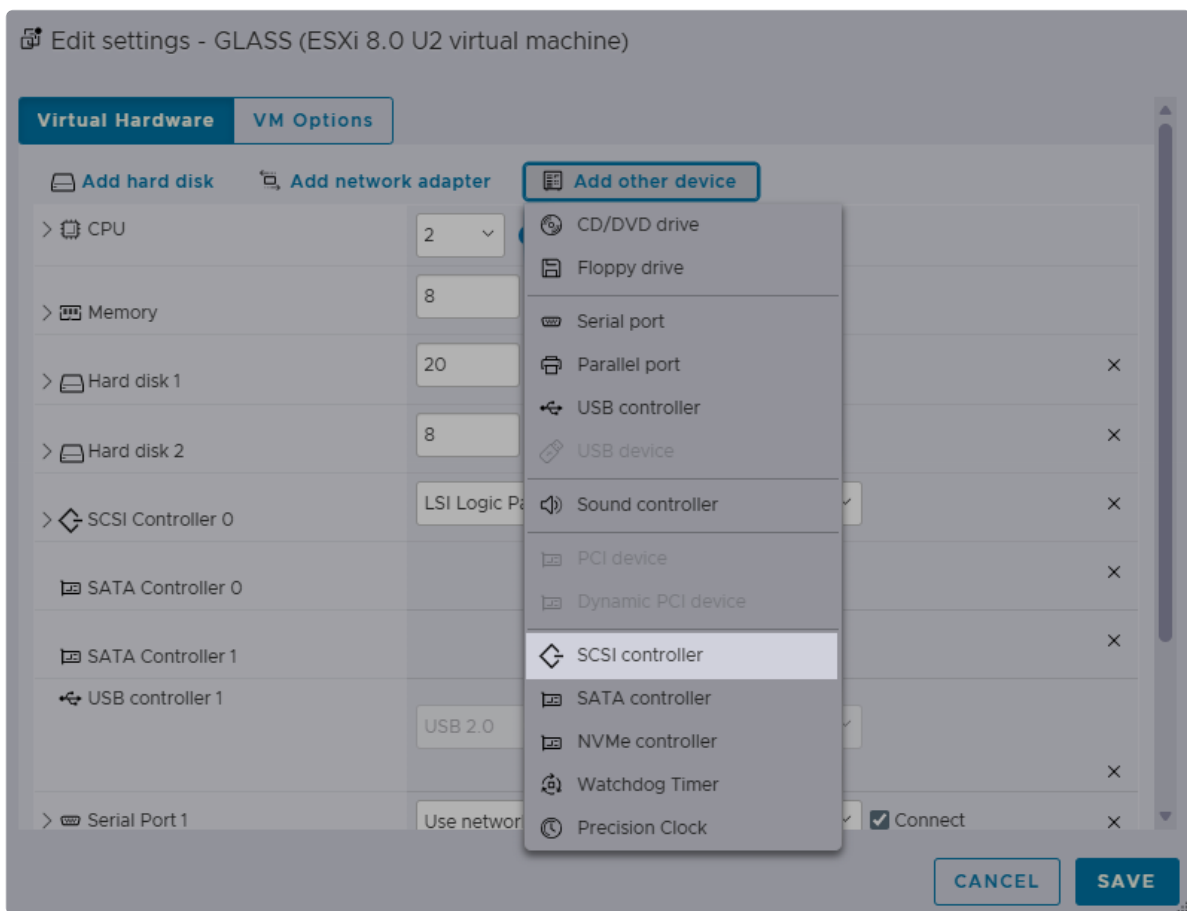
6.2 Adding a VMware Paravirtual SCSI Controller

VMware Paravirtual SCSI (PVSCSI) controller requires a native OpenVMS driver. It provides functionality on VMware similar to the Virtio-SCSI storage controller on KVM systems.

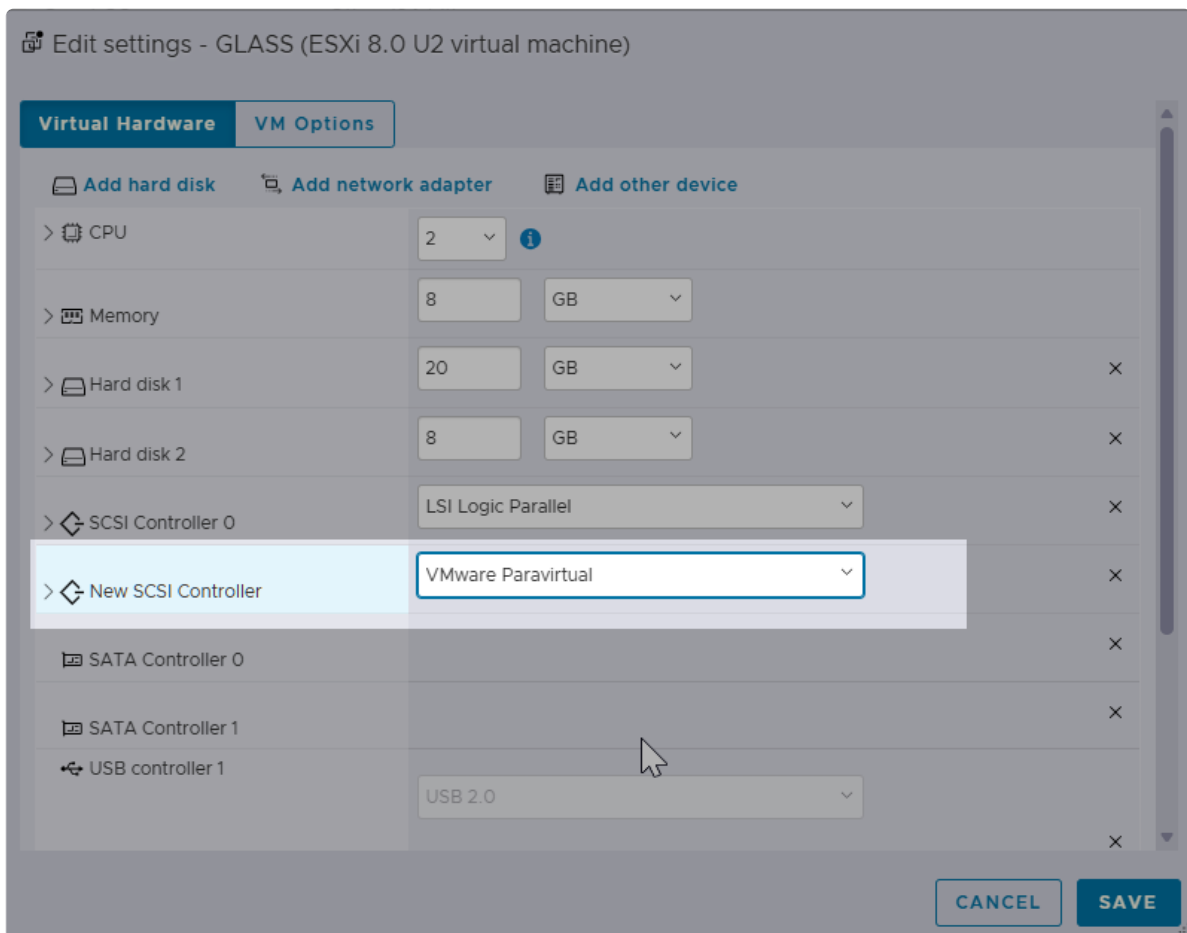
Starting with VSI OpenVMS E9.2-4, you can assign a VMware paravirtual SCSI controller after adding it in the hardware settings of your ESXi virtual machine.

This can be done while creating a virtual machine at the **Customize settings** stage or afterwards, in the **Edit Settings** window.

1. Click the **Add other device** button and choose **SCSI Controller**. A **New SCSI Controller** will appear in the list of categories.



2. From the drop-down menu next to the **New SCSI Controller** section, select **VMware Paravirtual**.



What is now displayed as **New SCSI Controller** will be named **SCSI Controller *n*** in your ESXi VM configuration, where *n* is the next available controller number. If your system already has two controllers configured (for example, SCSI Controller 0 and LSI Logic Parallel Controller 1), the next one you create will be SCSI Controller 2.

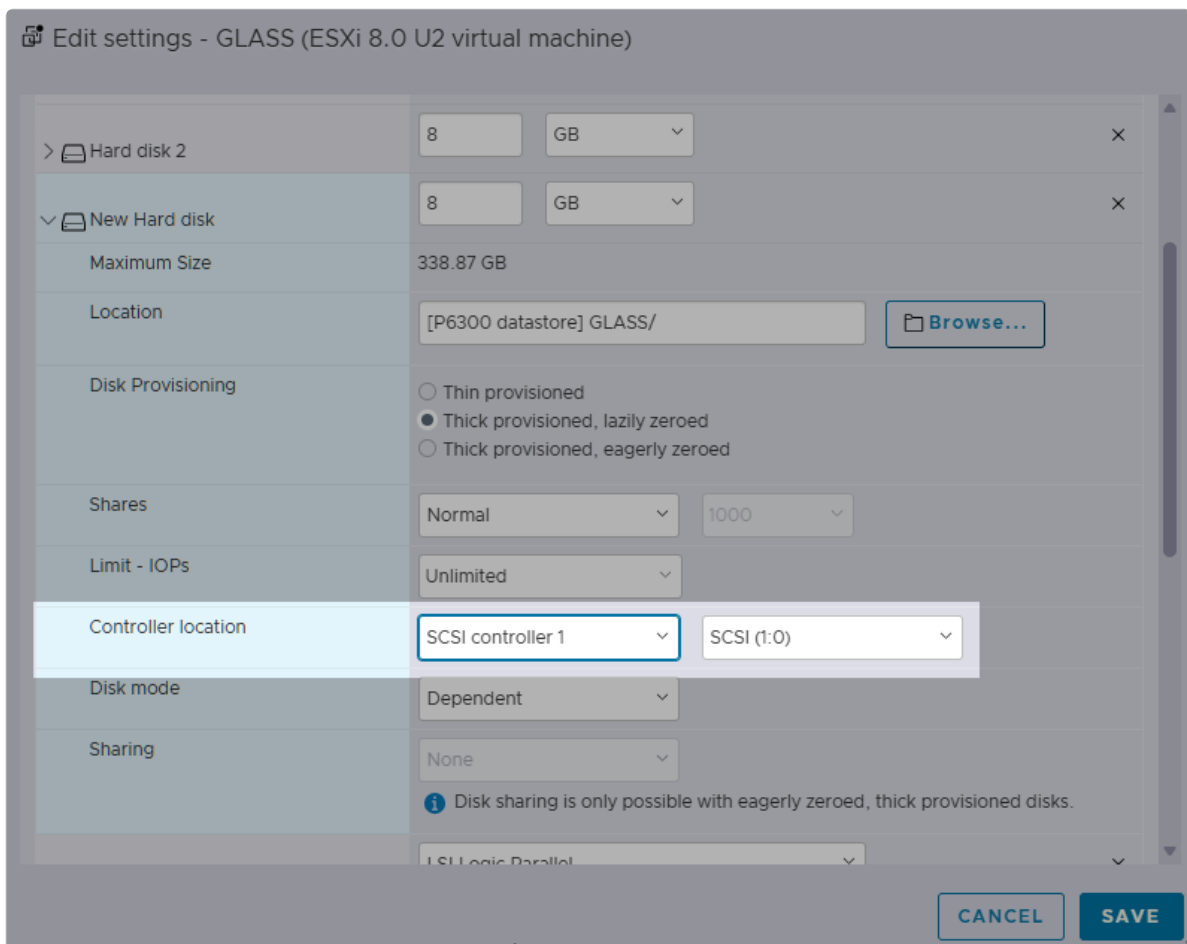
 Note

You can add a maximum of four SCSI controllers regardless of their type and up to 15 SCSI disks per controller.

3. Expand the existing **Hard Disk** section.

Optionally, if you wish to create another disk, click **Add hard disk** and choose **New standard hard disk**. A **New Hard Disk** will appear in the list of categories.

4. In the **Hard disk** section where you wish to assign your SCSI controller, scroll down to the **Controller location** setting and choose the newly added SCSI Controller (see [Step 2](#)).



5. Click **Save**. The VMware Paravirtual SCSI controller is now assigned to the selected device.

6.2.1 Verification on OpenVMS

Boot OpenVMS and execute the appropriate command to see the devices used by the system. PVSCSI disks appear as standard OpenVMS storage devices and follow the naming convention specified below.

- To list the disk devices, issue **SHOW DEVICES DK**.
- To list the controller devices, issue **SHOW DEVICES PK**.

For example:

```
$ SHOW DEVICES DK
```

Device Name	Device Status	Error Count	Volume Label	Free Blocks	Trans Count	Mnt Cnt
X86\$DKC0:	Online	0				
X86\$DKC1:	Online	0				
X86\$DKC2:	Online	wrtlck 0				

```
$ SHOW DEVICES PK
```

Device Name	Device Status	Error Count
PKB0:	Online	0

PKC0:	Online	0
PKD0:	Online	0

Note that, for example, 0 in PKB0: corresponds to the number of the SCSI controller.

For information on OpenVMS device naming conventions, refer to the [Device Name article](#).

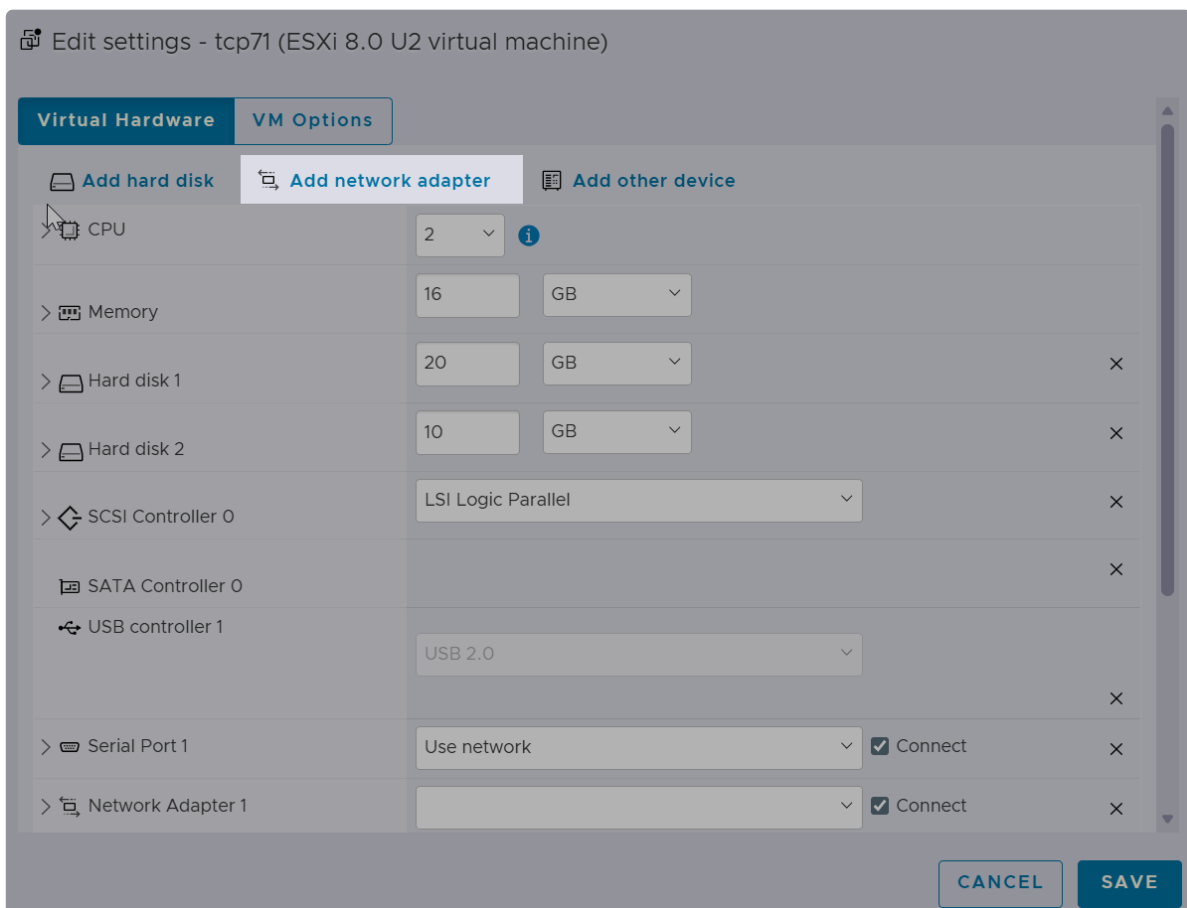
6.3 Adding Network Adapters to your ESXi VM

⚠ Attention

Some network configuration changes may require TCP/IP, LAN Failover, or VLAN definitions reconfiguration. It is recommended to record the VM NIC configuration before adding, removing, or changing NICs. See [Next Steps](#) for more information.

Perform the following steps to add new virtual Network Interface Cards (vNICs) to your virtual machine:

1. Open your virtual machine configuration page by clicking on your VM in the left pane of the **ESXi Host Client** window or by clicking **Virtual Machines** and selecting your VM from the list.
2. On your virtual machine configuration page, click **Edit**. In the **Edit Settings** window, click **Add Network Adapter**.

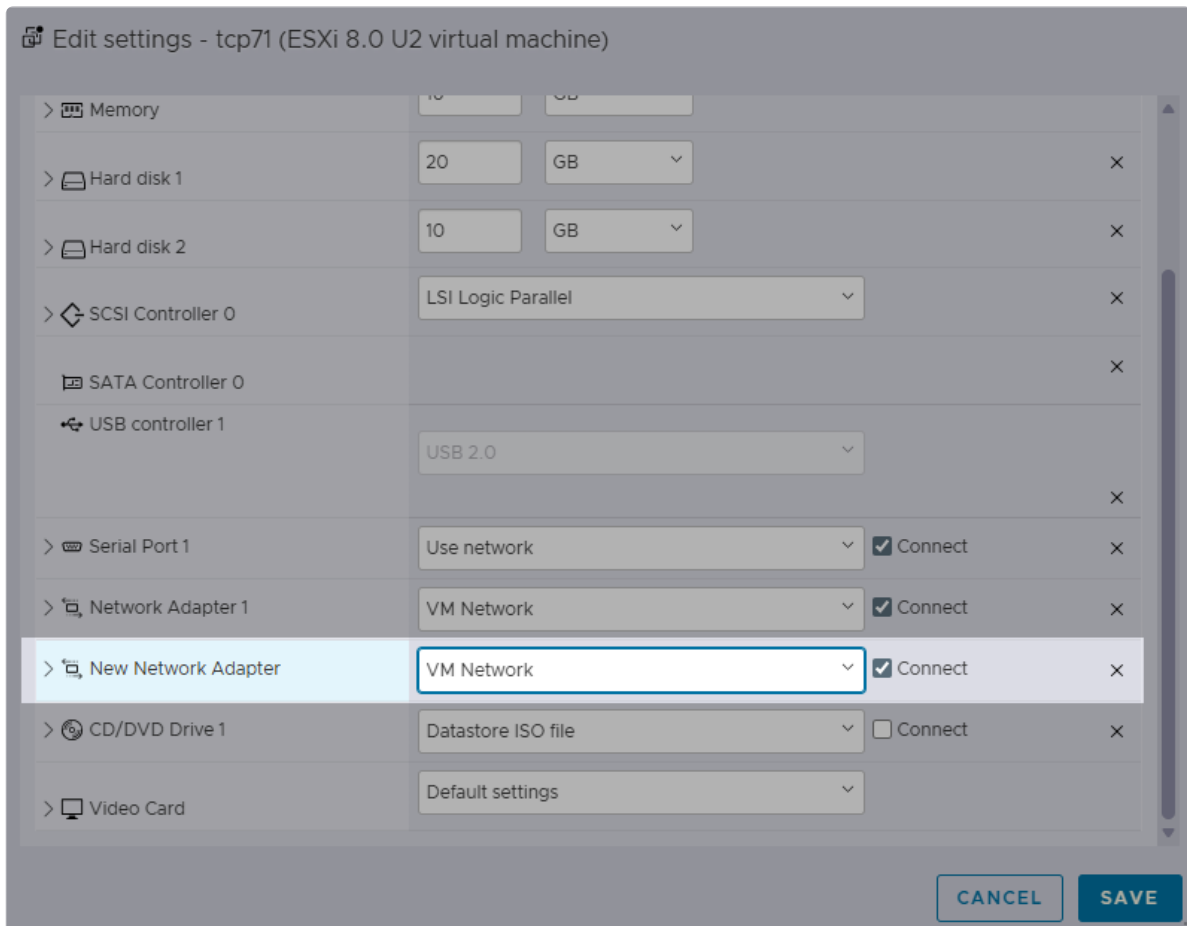


Use separate network adapters to isolate management, DECnet, and application traffic when required by your network design.

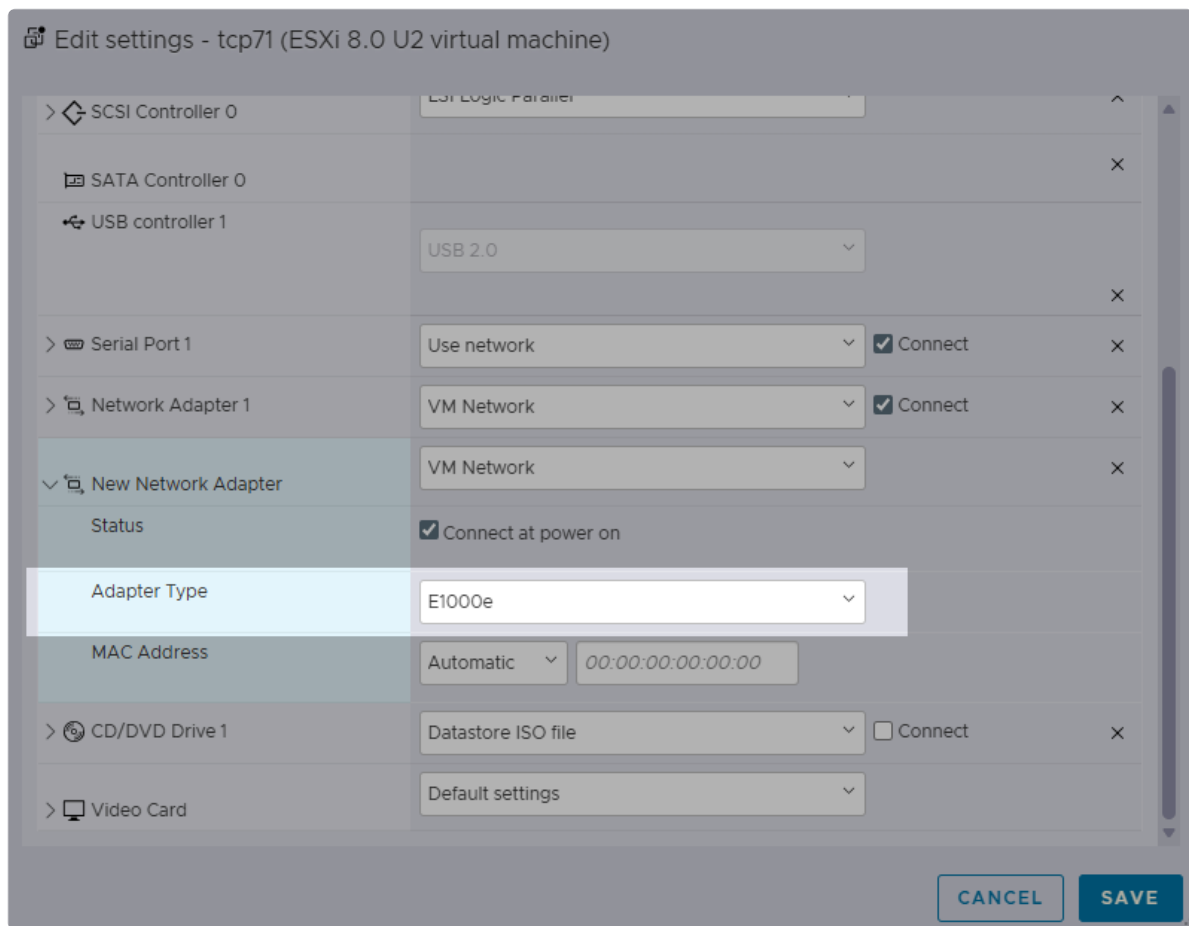
⚠ Attention

The use of DECnet or LAN Failover requires specific settings to be enabled or disabled. Refer to the [Blocked Network Traffic](#) section for more details.

3. A **New Network Adapter** section will be added to the list of settings. Choose **VM Network** from the drop-down list.



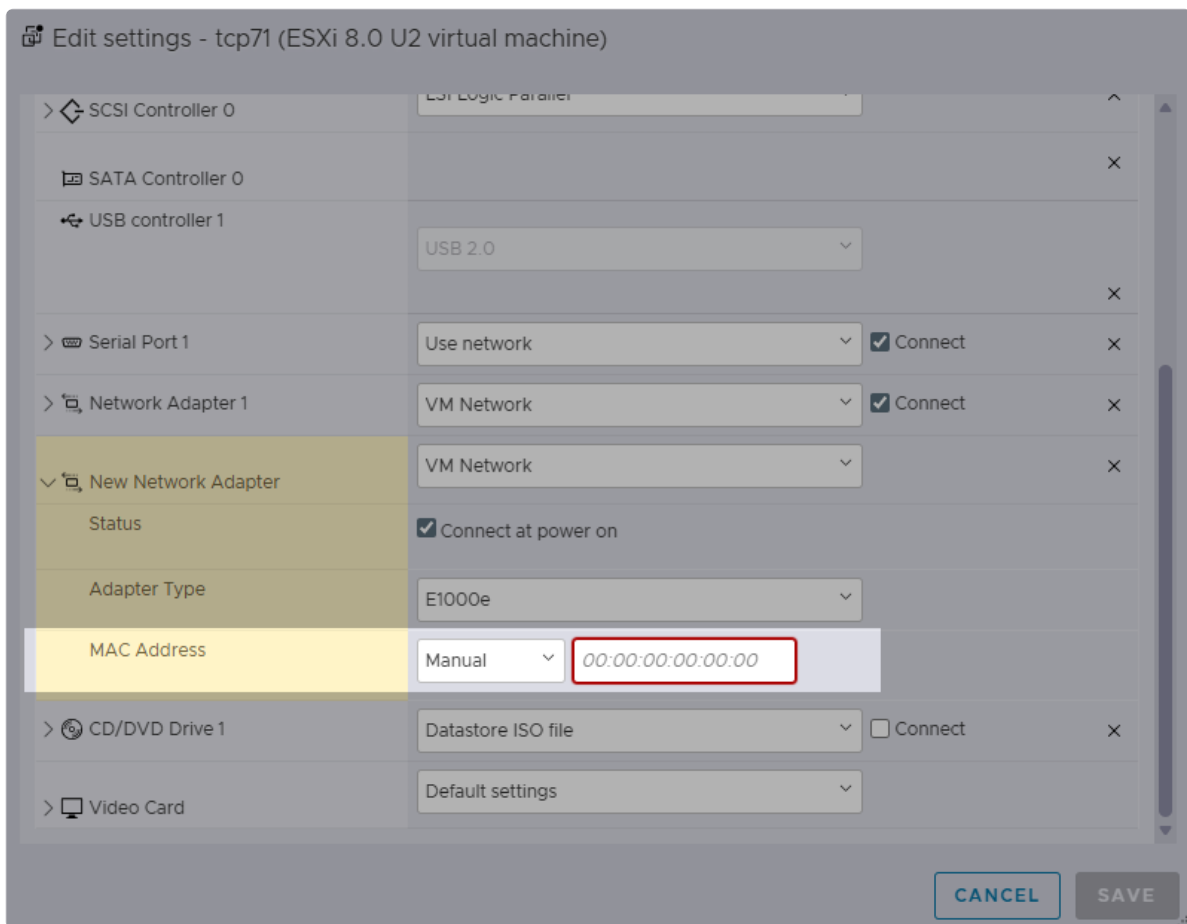
4. Expand the **New Network Adapter** section by clicking the arrow on the left. Choose one of the supported network controllers as **Adapter Type**. Find the current information about the supported hardware on the [Supported Platforms](#) page.



✖ **Restriction**

The **VMXNET 2** adapter type is not supported.

5. **Optional:** It is also possible to specify a custom MAC address after selecting **Manual** in the drop-down list.



6. Reboot the system for the changes to take effect.

⚠ Important

Changing the adapter type from VMXNET 3 to E1000 or E1000e requires deleting the existing network adapter and then adding a new one of the desired type.

6.3.1 Next Steps

After the network configuration change, you may need to reconfigure TCP/IP, LAN Failover, or VLAN definitions.

1. Boot OpenVMS and issue **MCR LANCP SHOW CONFIGURATION** (or **SHOW CONFIGURATION/USERS**), comparing the adapter types and MAC addresses against the VM NIC configuration.
2. Adjust your applications (TCP/IP, LAN Failover, VLAN definitions) to use the correct network adapters.

For information on how to do so, refer to the [System Manager's Manual Volume 2: Tuning, Monitoring, and Complex Systems](#).

7. VMware ESXi VM Advanced Configuration

7.1 Secure Boot

7.1.1 Secure Boot Overview

Starting with VSI OpenVMS E9.2-4, the Secure Boot feature is supported via the First Stage Bootloader.

The OpenVMS Boot Manager is signed with an OpenVMS-specific certificate and is validated by the First Stage Bootloader before it is loaded. To establish trust between the First Stage Bootloader and OpenVMS, the OpenVMS signing certificate must be added to the First Stage Bootloader's Machine Owner Key (MOK) database as described in [Adding OpenVMS Certificate to the Machine Owner Key Database](#).

Once the certificate is registered and the Secure Boot option is enabled, OpenVMS can boot successfully while maintaining the Secure Boot chain of trust.

Use the following command to see whether Secure Boot is enabled on your system:

```
$ WRITE SYS$OUTPUT F$GETSYI("SECURE_BOOT")
```

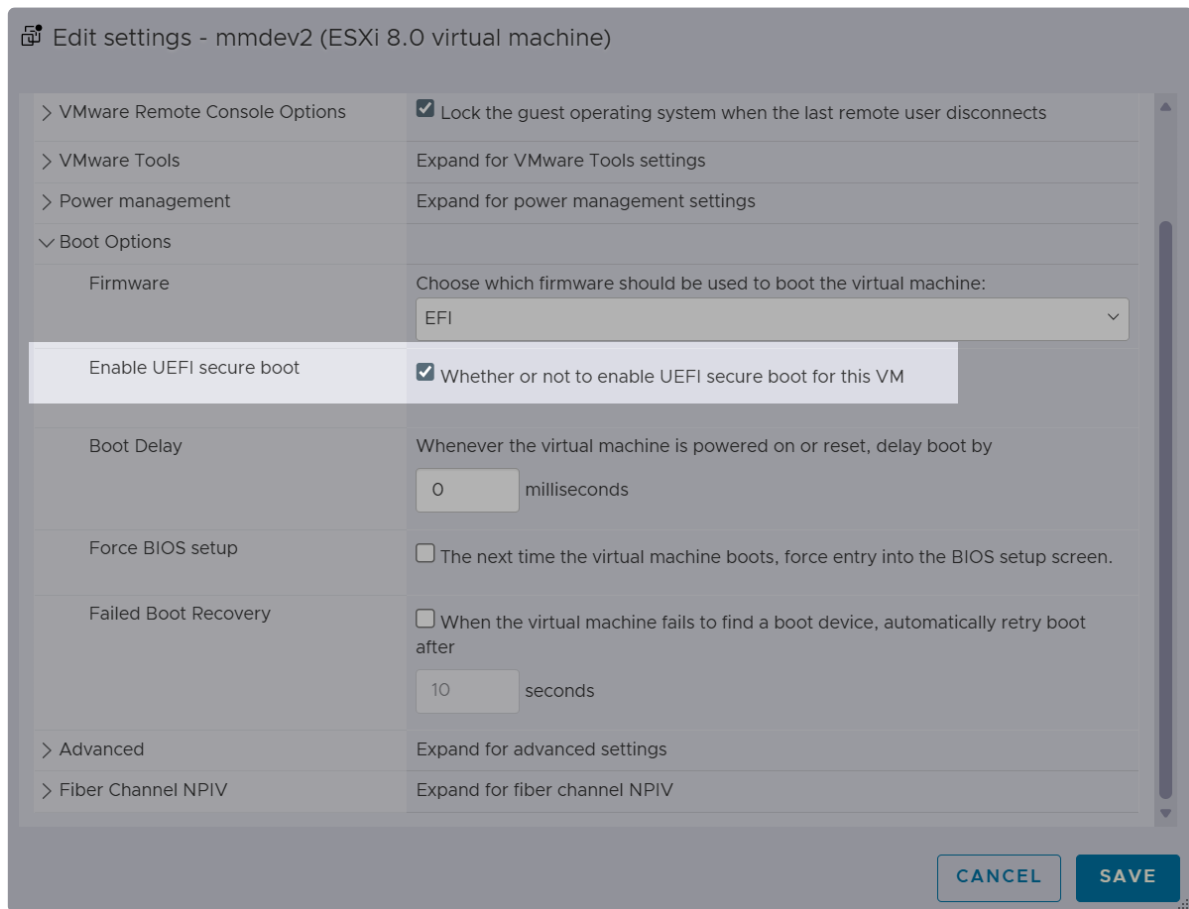
Output	Description
0	Disabled
1	Enabled

For more information, see [VSI OpenVMS Guide to System Security](#).

7.1.2 Secure Boot Option on ESXi Virtual Machine

On ESXi, the Secure Boot option can be enabled or disabled in the **ESXi Host Client**.

1. Open your virtual machine configuration page by clicking **Virtual Machines** and selecting your VM from the list.
2. On your virtual machine configuration page, click **Edit**. In the **Edit Settings** window, click **VM Options**.
3. Expand the **Boot Options** category and select the checkbox for the **Enable UEFI secure boot** parameter to enable Secure Boot.



To disable the Secure Boot option, leave the checkbox empty.

4. Click **Save**.

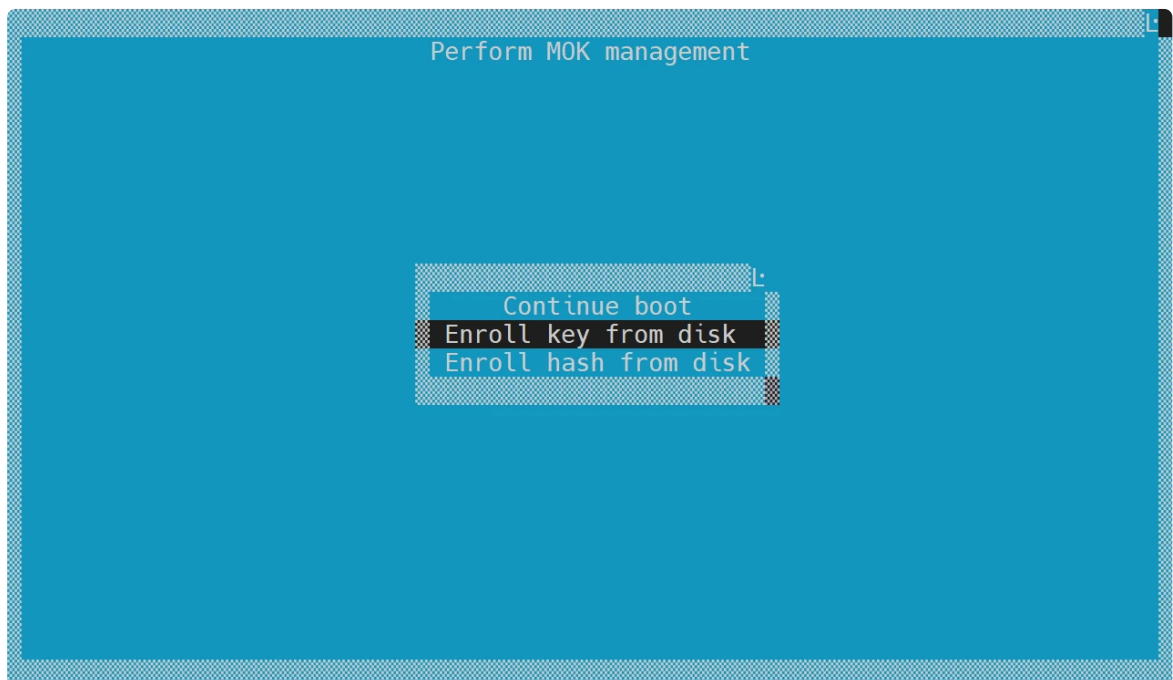
7.1.3 Adding OpenVMS Certificate to the Machine Owner Key Database

In order to boot VSI OpenVMS with Secure Boot enabled, you must register the OpenVMS key in the Machine Owner Key (MOK) database.

There are two methods to do so: manual and automatic. For automatic registration, ensure that OpenVMS has been booted at least once before enabling Secure Boot.

Manual registration

1. Enable Secure Boot as described in the [Secure Boot Option](#) section and start your virtual machine.
2. The UEFI key management utility will load. You will see a countdown at the bottom of the screen. Press before it runs out and the system starts booting.
3. Use the arrow keys to select **Enroll key from disk** and press .



4. Locate the **VMS_CERTIF.DER** file at the following path: ***your-disk*/EFI/VMS/VMS_CERTIF.DER**.



5. Select **Continue**.
6. At the **Enroll the key(s)?** prompt, select **Yes**.
7. Select **Reboot**.
8. Now you will be able to boot to the OpenVMS Boot Manager with Secure Boot.

Automatic registration

The OpenVMS Boot Manager automatically registers the certificate when the First Stage Bootloader is present.

1. Boot OpenVMS with Secure Boot disabled so that the certificate is registered automatically.
2. Shut down OpenVMS.
3. Enable Secure Boot in the UEFI as described in the [Secure Boot Option](#) section.
4. You will now be able to boot to the VSI Boot Manager with Secure Boot enabled.

7.2 Configuring VMware ESXi Firewall

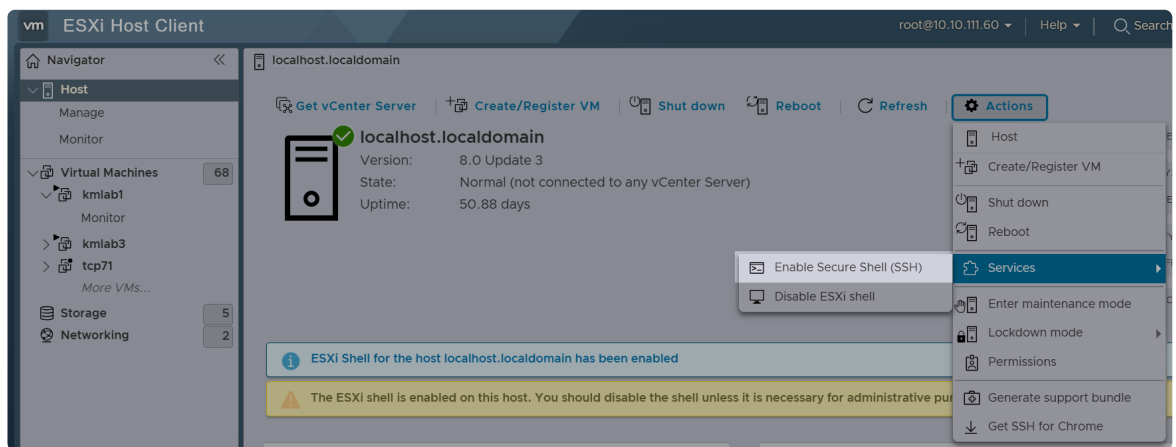
Configure the ESXi firewall to be able to connect to your OpenVMS VM via a serial port or SSH.

To do so, you will need to connect to the ESXi host command-line interface.

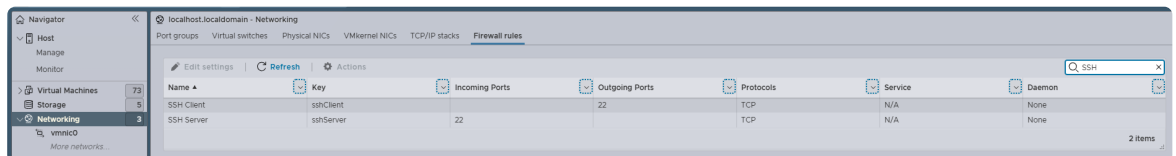
7.2.1 Connecting to the ESXi Command-Line Interface

via SSH

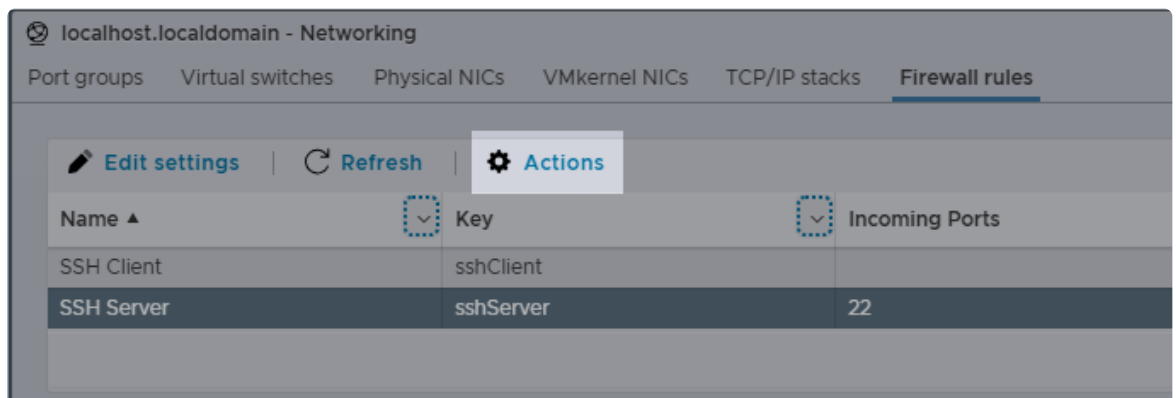
1. In the left pane of the **ESXi Host Client** window, click on your virtual machine, then click **Actions > Services > Enable Secure Shell (SSH)** in the main window.



2. In the left pane of the **ESXi Host Client** window, click **Networking**. Then click the **Firewall rules** tab in the right pane.



3. In the ruleset list, select **SSH Server** (or **TSM-SSH**, depending on the ESXi version) and click the **Actions** button. Select **Enable**.

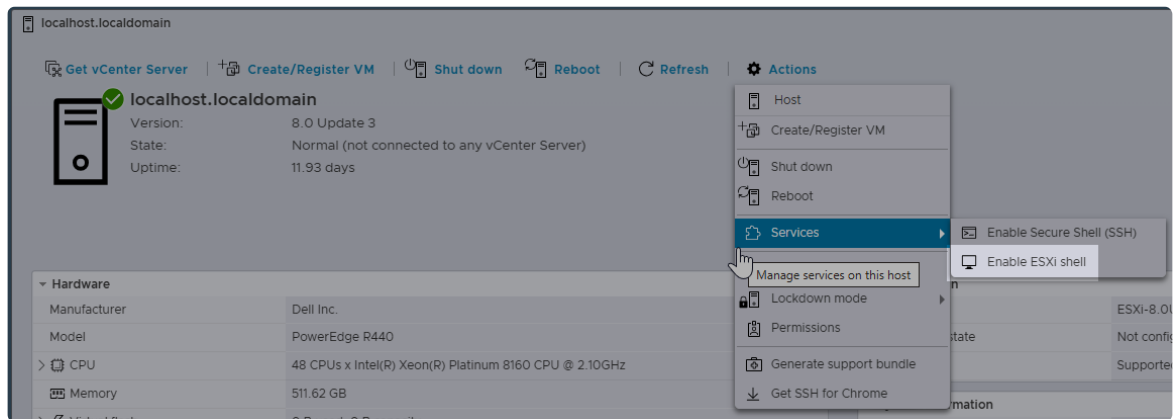


4. You will now be able to connect to the ESXi host CLI using the following command:

```
ssh root-user@esxi-host-ip-address
```

via ESXi Shell

1. In the left pane of the **ESXi Host Client** window, click on your virtual machine, then click **Actions > Services > Enable ESXi Shell** in the main window.



2. You will now be able to connect to the ESXi host CLI via a direct SSH connection.

7.2.2 Editing Configuration Files

First, you will need to edit the XML file to allow connection via the desired ports. Then apply the changes and make sure they are persistent after reboot.

1. You can view the existing XML files containing the firewall rules under `/etc/vmware/firewall/`.
2. Use the syntax from the existing files to create your own rules in `/etc/rc.local.d/local.sh` using the following command:

```
vi /etc/rc.local.d/local.sh
```

For basics on how to use the Vi editor, refer to the [Introduction to the Vi editor](#) article.

3. Enclose your custom firewall rules into the following lines:

```
/bin/cat > /etc/vmware/firewall/custom-rules-filename.xml << EOF
.
.
.
your-custom-rules
.
.
.
EOF
```

The rules should look similar to the following:

```

<ConfigRoot>
  <service>
    <id>ruleset-name</id>
    <rule id='0000'>
      <direction>inbound</direction>
      <protocol>tcp</protocol>
      <porttype>dst</porttype>
      <port>
        <begin>5140</begin>
        <end>5146</end>
      </port>
    </rule>
    <rule id='0001'>
      <direction>inbound</direction>
      <protocol>udp</protocol>
      <porttype>src</porttype>
      <port>2055</port>
    </rule>
    <enabled>true</enabled>
    <required>false</required>
  </service>
</ConfigRoot>

```

Tip

- Allowed direction values: inbound or outbound.
- Allowed protocol values: tcp or udp.
- Allowed porttype values: destination (dst) or source (src).
- Port values can be specified as a range using the <begin> and <end> elements or as a single value.

4. Add the following command at the end of the `/etc/rc.local.d/local.sh` file:

```
/sbin/esxcli network firewall refresh
```

5. Run the startup script for the changes to take effect:

```
/bin/sh /etc/rc.local.d/local.sh
```

6. Confirm that the custom firewall rules have been enabled:

```
esxcli network firewall ruleset list | grep ruleset-name
```

You should see `true` in the Enabled column next to your custom ruleset name.

In the **ESXi Host Client**, you should see your new rule in the list of rules in **Networking > Firewall rules**.

neo.eng.vmssoftware.com - Networking

Port groupsVirtual switchesPhysical NICsVMkernel NICsTCP/IP stacksFirewall rules

Edit settingsRefreshActions

Search

Name	Key	Incoming Ports	Outgoing Ports	Protocols	Service	Daemon
lofiltervp	lofiltervp	9080		TCP	N/A	None
lwarp-pm	lwarp-pm	3935	3935	UDP	N/A	None
MyFW.SerialPorts	MyFW.SerialPorts	2032, 2033, 2034, 2035, 2...		TCP	N/A	None
NFC	NFC	902	902	TCP	N/A	None
NFC Client	nfcClient			TCP	N/A	None

58 items

7.3 Allowing MAC Address Changes

By default, the ESXi host denies requests to change the MAC address of a virtual machine to the one different from the initial MAC address. However, for DECnet using Phase-IV addressing and for LAN Failover to work, you must allow virtual machine MAC address changes.

To do so, perform the following steps:

1. In the browser, open the **ESXi Host Client**, power off your virtual machine, and click **Networking** in the left pane.
2. From the list in the main window, select the port group to which your virtual machine is assigned.
3. Click **Edit Settings** and expand the **Security** category.
4. Set **Promiscuous mode**, **MAC Address Changes**, and **Forged Transmits** to **Accept**.

Edit port group - 118 NETWORK

Name	118 NETWORK
VLAN ID	0
Virtual switch	118 NET
Security	
Promiscuous mode	☒ Accept ☐ Reject ☐ Inherit from vSwitch
MAC address changes	☒ Accept ☐ Reject ☐ Inherit from vSwitch
Forged transmits	☒ Accept ☐ Reject ☐ Inherit from vSwitch
> NIC teaming	Click to expand
> Traffic shaping	Click to expand

CANCEL **SAVE**

5. Click **Save**.

7.4 Fibre Channel Passthrough on ESXi Virtual Machine

Starting with the V9.2-3 release, OpenVMS x86-64 supports the VMware VMDirectPath I/O feature, which allows VMware ESXi virtual machines to directly access the physical PCI devices of the host system, bypassing the virtualization layer. The use of this feature allows for direct access to Storage Area Network (SAN).

For more information, see [VMware VMDirectPath I/O Support for Data Disks](#).

✖ Restrictions

- Booting OpenVMS from a Fibre Channel disk is currently not possible.
- The VMware VMDirectPath I/O feature is not compatible with the VMware vMotion feature.
- N_Port ID Virtualization (NPIV) is not supported.

7.4.1 Supported Platforms and Hardware

Host Bus Adapters

Refer to the [Supported Platforms](#) page for the full list of supported HBA (Host Bus Adapter) devices.

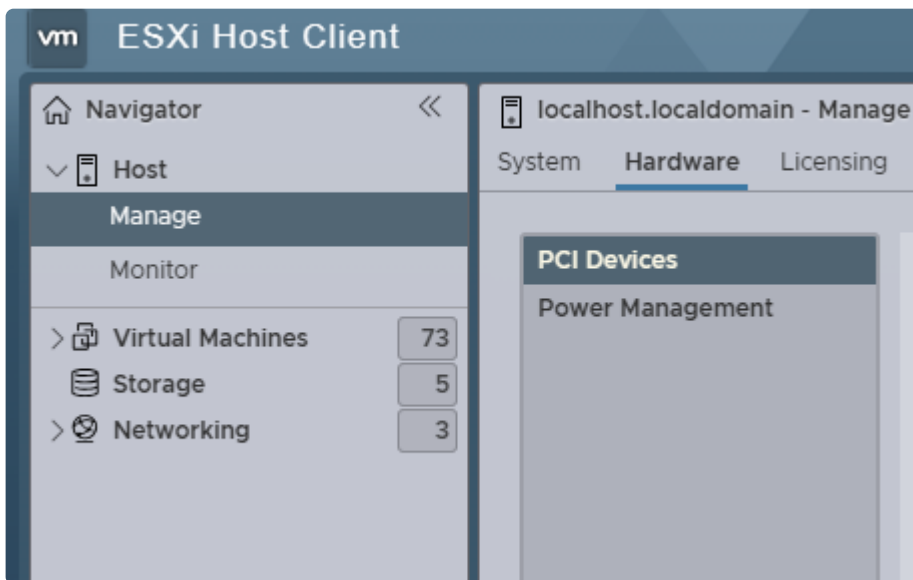
VSI OpenVMS Version

[VSI OpenVMS V9.2-3](#) or higher

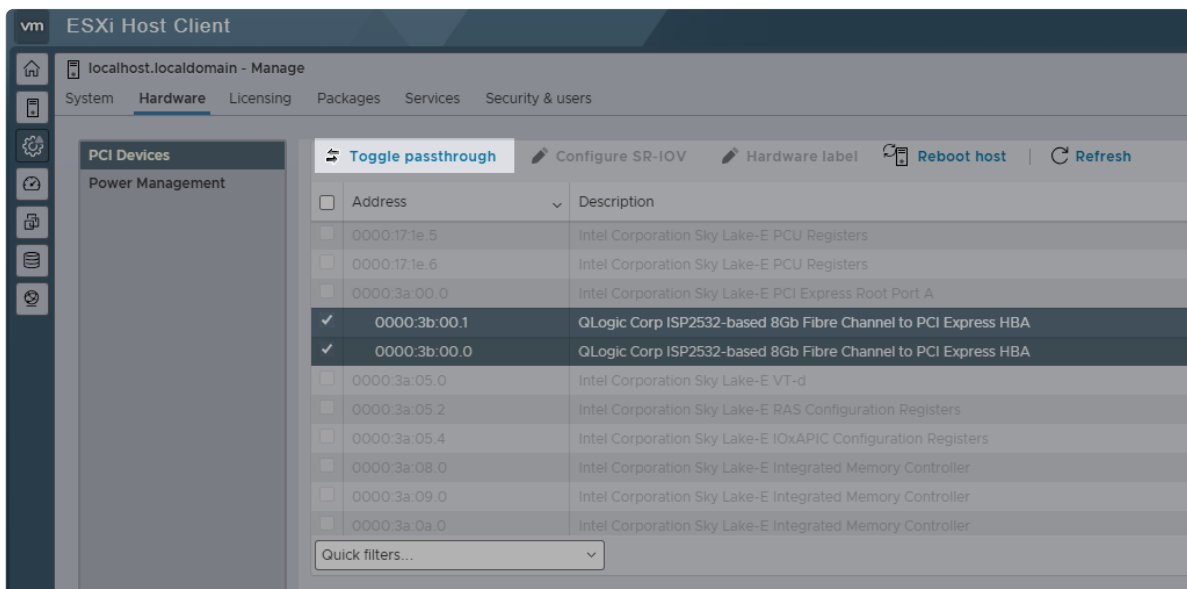
7.4.2 Setting up Fibre Channel Passthrough

To configure your VMware ESXi virtual machine to use physical Fibre Channel disks of the host system, perform the following steps:

1. Make sure that a supported Fibre Channel HBA card is installed into your server and configured on your host system. For information on how to plug in and configure a Fibre Channel HBA, refer to the documentation for your system hardware.
2. Use the browser to log in to the **ESXi Host Client**. In the left pane, expand **Host**, then click **Manage**.
3. In the **Manage** area, switch to the **Hardware** tab, then click **PCI Devices**.



4. Select the devices that represent the ports of your Fibre Channel HBA and click **Toggle passthrough**.



5. Reboot your ESXi host system and log back in to the **ESXi Host Client**.
6. Bring up the **Edit Settings** window for your VM by clicking the **Edit** button.
7. In the **Edit Settings** window, click **Add other device**, then **PCI Device**.
8. Click the drop-down list next to your new PCI device and select one of the ports of your Fibre Channel HBA.
9. Create as many PCI devices as there are ports on your Fibre Channel HBA and map each device to a different port.
10. In the left pane of the **Edit Settings** window, click **Memory**, then enable the **Reserve all guest memory (All locked)** option.
11. Save the changes and close the **Edit Settings** window.
12. Power on your VM and boot OpenVMS from the Boot Manager.

13. Once booted and logged in to the system, ensure that OpenVMS has access to the Fibre Channel HBA(s) on your host system by entering the following command:

```
$ SHOW DEVICES /FULL FG
```

You should see an output similar to the following:

```
Device FGA0:, device type device_name, is online, shareable, error
    logging is enabled.
.
.
.
Device FGB0:, device type device_name, is online, shareable, error
    logging is enabled.
.
.
.
```

14. Log in to the management interface of your storage array and map the volumes created there to the HBA that your VM is using. For information on how to create and map Fibre Channel volumes, refer to the documentation provided with your storage device.
15. Identify and configure the volumes that you have mapped by entering the following command:

```
$ MCR SYSMAN IO AUTOCONFIGURE/FULL/LOG
```

You should see an output similar to the following:

```
%SYSMAN-I-OUTPUT, command execution on node MM2442
%IOGEN-I-PREFIX, searching for ICBM with prefix SYS$
%IOGEN-I-ACTIVATE, activating ICBM SYS$ICBM
%IOGEN-I-FIBREPOLL, scanning for devices through FIBRE port FGA0
%IOGEN-I-FIBREPOLL, scanning for devices through FIBRE port FGB0
%IOGEN-I-CONFIGURED, configured device DGA19
%IOGEN-E-NODEVID, no identifier defined for device unit D19
%IOGEN-I-CONFIGURED, configured device DGA19
%IOGEN-E-NODEVID, no identifier defined for device unit D19
```

7.5 VMware vMotion

7.5.1 Overview

The vMotion feature of VMware vSphere makes it possible to migrate a running virtual machine from one VMware ESXi host to another with zero downtime.

Sections below discuss the requirements and provide an outline of the steps that you must take to build a vMotion-capable environment. For a detailed step-by-step demonstration, refer to [this tutorial](#) on the official VSI YouTube channel.

Starting with V9.2-3, VSI OpenVMS x86-64 supports the VMware vMotion technology with the following limitations:

1. Your VMware ESXi cluster must be configured for vMotion. For details, refer to [the official VMware documentation](#).
2. vMotion is not compatible with the VMware VMDirectPath I/O (Fibre Channel passthrough) feature (see [VMware VMDirectPath I/O Support for Data Disks](#)).
3. VSI Guest Console *must* be used to interact with virtual machines.

7.5.2 Requirements

7.5.2.1 CPU Requirements

Depending on the processor that each of the systems in your cluster is equipped with, the cluster may or may not function correctly. Ideally, all of your systems should be equipped with identical processors – this guarantees that vMotion will always work. If some or all your machines are equipped with different processors, consider the following:

- vMotion *should* work between host systems equipped with processors of the same family and generation.
- vMotion *might* work between host systems equipped with processors of different families and/or generations from the same manufacturer.
- vMotion *will not* work between AMD- and Intel-equipped host systems.

7.5.2.2 Network Interface Requirements

All ESXi host systems in your cluster must have the same network connections.

In addition to the network interfaces used for the host and guest systems network connections, each host system *must* have at least one dedicated network interface (preferably, 10 Gbit or faster) for the vMotion traffic. These dedicated network interfaces must be connected to the same dedicated network or VLAN.

7.5.2.3 Storage Requirements

All host systems must have access to a Storage Area Network (SAN) array which presents a volume for use as a VMFS datastore. This can be achieved either through a VMware-supported Fibre Channel adapter, a VMware-supported iSCSI Ethernet adapter, or a regular (preferably dedicated) 10 Gbit or

faster network interface (using VMware's software iSCSI). In the [tutorial](#), we are using an iSCSI shared storage.

7.5.3 Creating a vMotion-Capable Environment and Performing vMotion Outline

The steps below outline the process of building a vMotion-capable environment from scratch. For a detailed step-by-step demonstration, see [this video tutorial](#) on the official VSI YouTube channel or follow the instruction described in *[vMotion: Detailed Configuration and Migration Procedure](#)*.

1. Create the first ESXi host system and set it up with a static IP address rather than a dynamic one managed by DHCP. Using a static IP address guarantees that vMotion will work correctly.
 - a. Set the Management Network on the system the way that fits your environment.
 - b. Create as many more ESXi host systems as you need and set them up the same way.
2. Create an iSCSI datastore and connect one of your ESXi host systems to the shared storage device (in the tutorial, we are using iSCSI).
3. Install vCenter vSphere and provide it with the IP address of the ESXi host from the previous step.
4. In vSphere, connect your ESXi host systems into a cluster.
5. While in vSphere, create a new distributed switch and add your ESXi hosts systems to it. The distributed switch allows the guest VMs to maintain network connection while being moved between hosts.
 - a. Add at least two NICs per host to the switch (as a failsafe mechanism for network failure).
 - b. Assign the existing network adapters of each VM to the switch.
 - c. Make sure that the DPortGroup on the switch contains all ESXi hosts systems and the vSphere virtual machine.
6. On any of the ESXi host systems, create your guest systems and install VSI OpenVMS x86-64 on them.

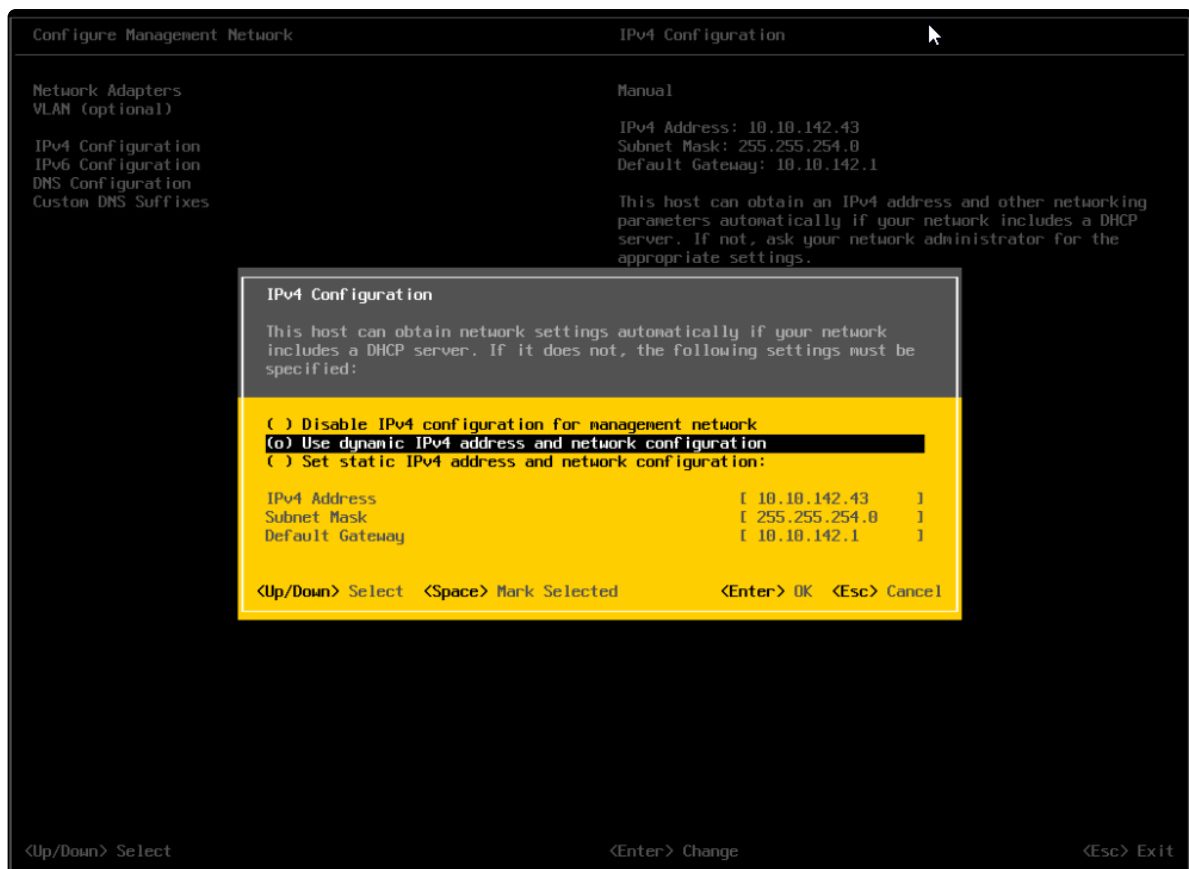
Enable the Guest Console feature on each of your VSI OpenVMS guest systems. For detailed instructions, refer to the *[VSI OpenVMS x86-64 Boot Manager User Guide](#)*.
7. Add the virtual machines running OpenVMS to the VMware ESXi cluster.
8. Now, you are ready to perform vMotion on any of your VSI OpenVMS x86-64 guests. To do that, right-click the guest that you want to move and select **Migrate** from the context menu.

7.5.4 vMotion: Detailed Configuration and Migration Procedure

This page describes the same steps as [VMware vMotion Overview](#) but provides detailed instructions for every installation and configuration stage.

7.5.4.1 Step 1: Set a Static IP on the ESXi Hosts

1. At the physical (or virtual) console of the host, wait for the Direct Console User Interface (DCUI) yellow/gray screen, then press **F2** and log in as root.
2. Select **Configure Management Network**.
3. Select **IPv4 Configuration**, change the setting to **Static**, and enter the IP address, subnet mask, and default gateway.



4. Select **DNS Configuration** if needed and enter DNS server addresses/hostname.
5. Press **Esc**, then confirm with **Y** to apply the changes and restart the management network.

Repeat the **DCUI > Configure Management Network** steps above on every additional ESXi host, giving each its own static IP address, but keeping NIC layout and network configuration identical across hosts.

7.5.4.2 Step 2: Create iSCSI Shared Storage

1. In the **ESXi Host Client**, click **Storage > Adapters > Software iSCSI**. A new window will open.
2. Set **iSCSI enabled** to **Enabled**.

3. In the **Network port bindings** section, click **Add port binding** and select a VMkernel interface. Click **Select** to save the changes.
4. In the **Dynamic targets** section, specify the IP address of your iSCSI storage.

Configure iSCSI - vmhba64

iSCSI enabled: ☐ Disabled ☒ Enabled

> Name and alias: iqn.1998-01.com.vmware:esxi1.camicom.local:153270950:64 (iscsi_vmk)

> CHAP authentication: Do not use CHAP

> Mutual CHAP authentication: Do not use CHAP

> Advanced settings: Click to expand

Network port bindings: **Add port binding** Remove port binding

VMkernel NIC Port group IPv4 address

No port bindings

Static targets: **Add static target** Remove static target Edit settings Search

Target Address Port

No static targets

Dynamic targets: **Add dynamic target** Remove dynamic target Edit settings Search

Address Port

No dynamic targets

CANCEL SAVE CONFIGURATION

5. Click **Save Configuration**.
6. Click the **Refresh** button, then click **Devices**. You will see your newly added iSCSI storage.

vm ESXi Host Client root@esxi1.local.camicom.com Help

esxi1.camicom.local - Storage

Datstores Adapters **Devices** Persistent Memory

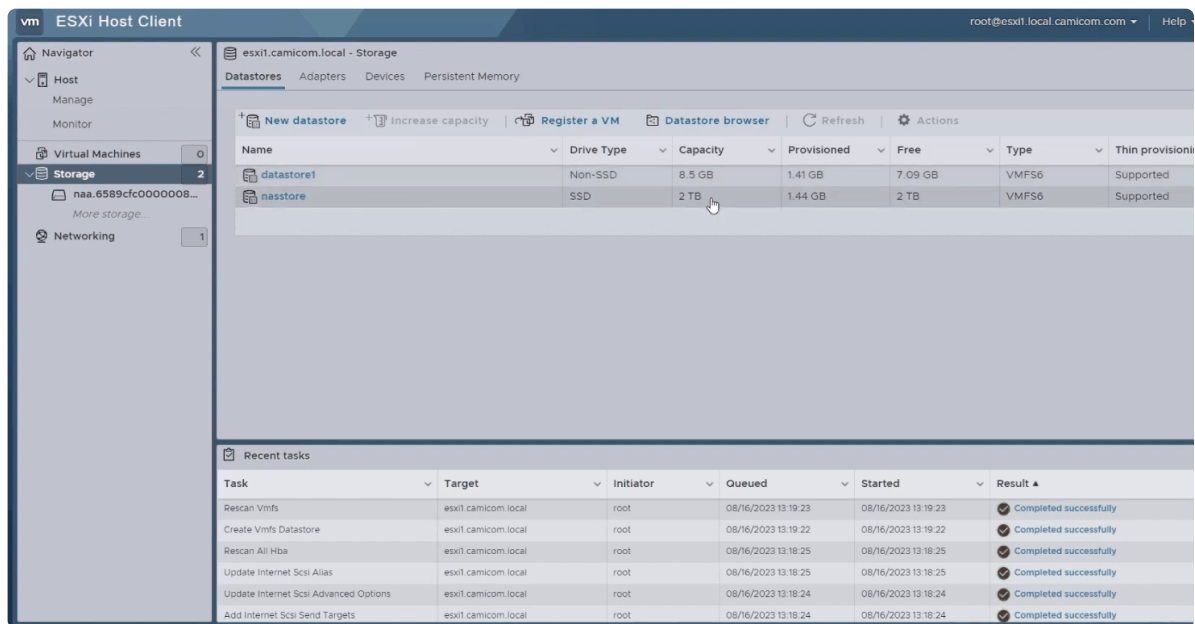
+ New datastore + Increase capacity Rescan Refresh Actions

Name	Status	Type	Capacity	Queue Depth	Vend
TrueNAS iSCSI Disk (naa.6589cf00000083f042b1d9f61d703c)	Normal, Degraded	Disk (SSD)	2 TB	128	TrueNAS
Local HP Disk (naa.600508b1001cd10ff61567980a318a5b)	Normal	Disk	136.7 GB	1009	HP

Recent tasks

Task	Target	Initiator	Queued	Started	Result
Update Internet Scsi Alias	esxi1.camicom.local	root	08/16/2023 13:14:21	08/16/2023 13:14:21	Completed successfully
Update Internet Scsi Advanced Options	esxi1.camicom.local	root	08/16/2023 13:14:21	08/16/2023 13:14:21	Completed successfully
Add Internet Scsi Send Targets	esxi1.camicom.local	root	08/16/2023 13:14:21	08/16/2023 13:14:21	Completed successfully
Bind Vnic	esxi1.camicom.local	root	08/16/2023 13:14:21	08/16/2023 13:14:21	Completed successfully
Update Software Internet Scsi Enabled	esxi1.camicom.local	root	08/16/2023 13:13:57	08/16/2023 13:13:57	Completed successfully

7. Click on the iSCSI storage name, then click **New datastore**. A **New datastore** wizard will open.
 - a. In the **Datastore name** section, specify the name for your datastore, then click **Next**.
 - b. In the **Select partitioning options** section, use the default values. Click **Next**.
 - c. In the **Ready to complete** section, review the configuration summary and click **Finish**.
8. You should now see the iSCSI storage listed in **Storage > Datastores**.



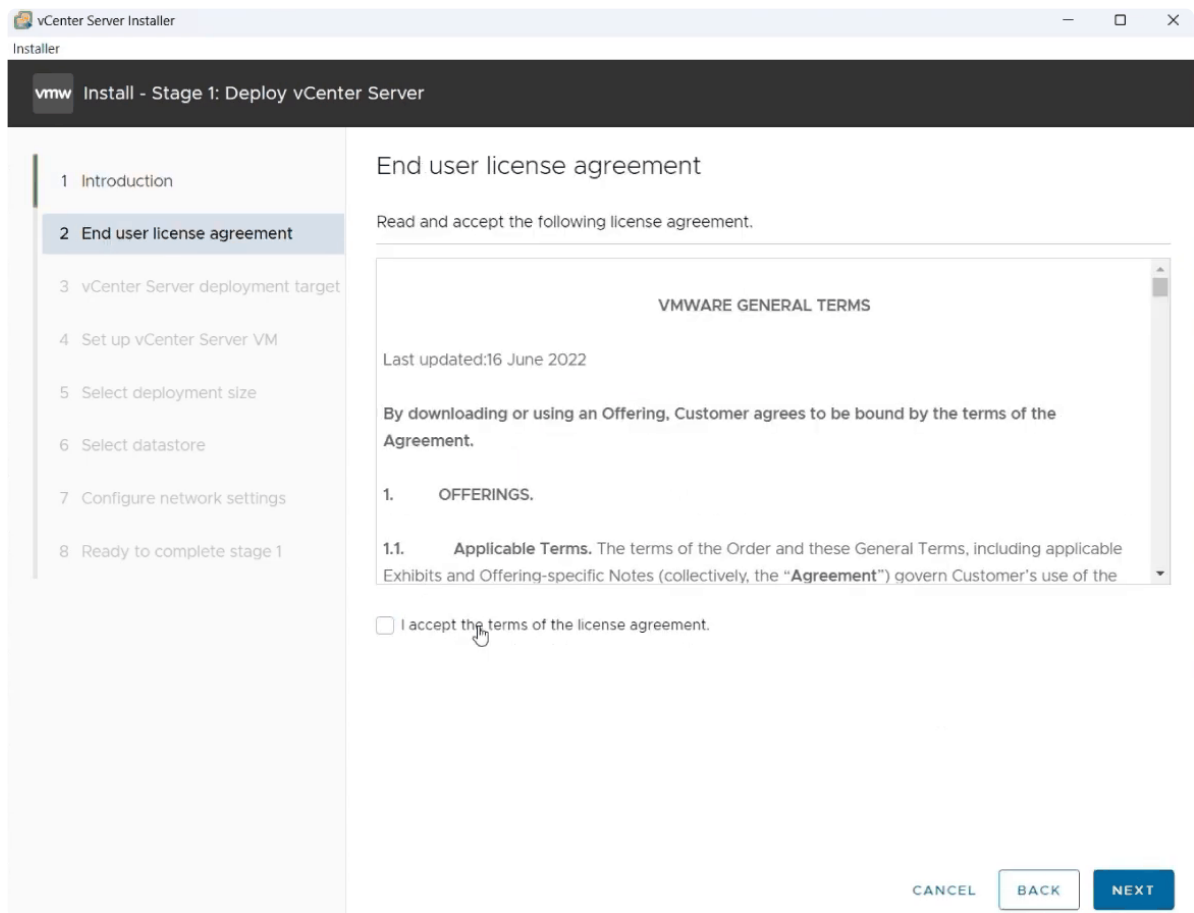
7.5.4.3 Step 3: Install VMware vSphere to Manage the VMware Cluster

Install vSphere using the configuration utility.

The installation is performed in two stages – the setup wizard will guide you through the steps necessary to complete the installation procedure.

INSTALLATION: STAGE 1

1. When the utility starts, select **Install**.
Read the **Introduction** section and click **Next**.
2. Read and accept the terms of the license agreement. Click **Next**.



3. In the **vCenter Server deployment target** section, provide the IP address of your ESXi host, HTTPS port, root user name, and password.

vCenter Server Installer

Installer

vmw Install - Stage 1: Deploy vCenter Server

1 Introduction

2 End user license agreement

3 vCenter Server deployment target

4 Set up vCenter Server VM

5 Select deployment size

6 Select datastore

7 Configure network settings

8 Ready to complete stage 1

vCenter Server deployment target

Specify the vCenter Server deployment target settings. The target is the ESXi host or vCenter Server instance on which the vCenter Server will be deployed.

ESXi host or vCenter Server name

HTTPS port

User name

Password

CANCEL BACK NEXT

Click **Next**.

4. In the **Set up vCenter Server VM** section, specify the name for your vSphere virtual machine and set a password for the root user.

vCenter Server Installer

Installer

vmw Install - Stage 1: Deploy vCenter Server

- 1 Introduction
- 2 End user license agreement
- 3 vCenter Server deployment target
- 4 Set up vCenter Server VM
- 5 Select deployment size
- 6 Select datastore
- 7 Configure network settings
- 8 Ready to complete stage 1

Set up vCenter Server VM

Specify the VM settings for the vCenter Server to be deployed.

VM name VMware vCenter Server ⓘ

Set root password ⓘ ⓘ
Password does not meet requirements.

Confirm root password

CANCEL BACK NEXT

5. In the **Set deployment size** section, select the values that suit your environment needs.

vCenter Server Installer

Installer

vmw Install - Stage 1: Deploy vCenter Server

- 1 Introduction
- 2 End user license agreement
- 3 vCenter Server deployment target
- 4 Set up vCenter Server VM
- 5 Select deployment size
- 6 Select datastore
- 7 Configure network settings
- 8 Ready to complete stage 1

Select deployment size

Select the deployment size for this vCenter Server.

For more information on deployment sizes, refer to the vSphere 8.0 documentation.

Deployment size Tiny ▾

Storage size Default ⓘ

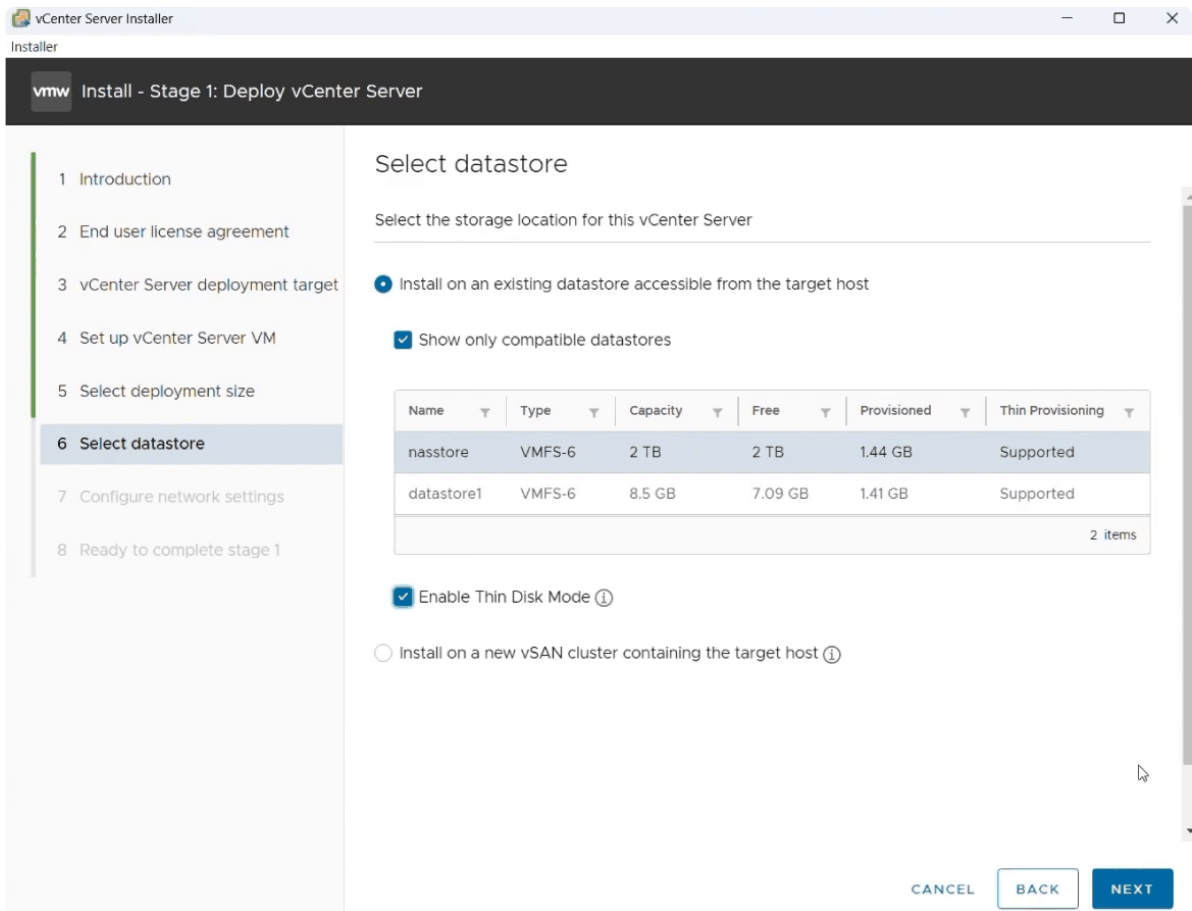
Resources required for different deployment sizes

Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	14	579	10	100
Small	4	21	694	100	1000
Medium	8	30	908	400	4000
Large	16	39	1358	1000	10000
X-Large	24	58	2283	2000	35000

CANCEL BACK NEXT

6. In the **Select datastore** section, select the datastore that you created earlier in [Step 2](#).

Select **Enable Thin Disk Mode** and click **Next**.



vCenter Server Installer

Installer

vmw Install - Stage 1: Deploy vCenter Server

- 1 Introduction
- 2 End user license agreement
- 3 vCenter Server deployment target
- 4 Set up vCenter Server VM
- 5 Select deployment size
- 6 Select datastore**
- 7 Configure network settings
- 8 Ready to complete stage 1

Select datastore

Select the storage location for this vCenter Server

☒ Install on an existing datastore accessible from the target host

☒ Show only compatible datastores

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
nasstore	VMFS-6	2 TB	2 TB	1.44 GB	Supported
datastore1	VMFS-6	8.5 GB	7.09 GB	1.41 GB	Supported

2 items

☒ Enable Thin Disk Mode ⓘ

☐ Install on a new vSAN cluster containing the target host ⓘ

CANCEL BACK NEXT

7. In the **Configure network settings** section, provide networking details for your vSphere Server.

The screenshot shows the vCenter Server Installer window. The title bar reads 'vCenter Server Installer'. Below the title bar, the text 'Installer' is visible. The main window has a dark header bar with the VMware logo and the text 'Install - Stage 1: Deploy vCenter Server'. On the left side, there is a vertical list of steps: 1 Introduction, 2 End user license agreement, 3 vCenter Server deployment target, 4 Set up vCenter Server VM, 5 Select deployment size, 6 Select datastore, 7 Configure network settings (highlighted), and 8 Ready to complete stage 1. The main area is titled 'Configure network settings' and contains the text 'Configure network settings for this vCenter Server'. Below this, there are several configuration fields: Network (set to VM Network), IP version (set to IPv4), IP assignment (set to static), FQDN (set to FQDN (optional)), IP address (empty), Subnet mask or prefix length (empty), Default gateway (empty), DNS servers (set to Comma separated IP address), Common Ports (empty), HTTP (set to 80), and HTTPS (set to 443). At the bottom right, there are three buttons: CANCEL, BACK, and NEXT.

Field	Value
Network	VM Network
IP version	IPv4
IP assignment	static
FQDN	FQDN (optional)
IP address	
Subnet mask or prefix length	
Default gateway	
DNS servers	Comma separated IP address
Common Ports	
HTTP	80
HTTPS	443

8. In the **Ready to complete stage 1** section, review the configuration parameters. Click **Back** to edit the configuration; click **Finish** to complete the configuration.

vCenter Server Installer
Installer

Install - Stage 1: Deploy vCenter Server

1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 **Ready to complete stage 1**

Ready to complete stage 1
Review your settings before starting the vCenter Server deployment.

Deployment Details	
Target ESXi host	esxi1.local.camicom.com
VM name	VMware vCenter Server
Deployment size	Tiny
Storage size	Default

Datastore Details	
Datastore, Disk mode	nasstore, thin

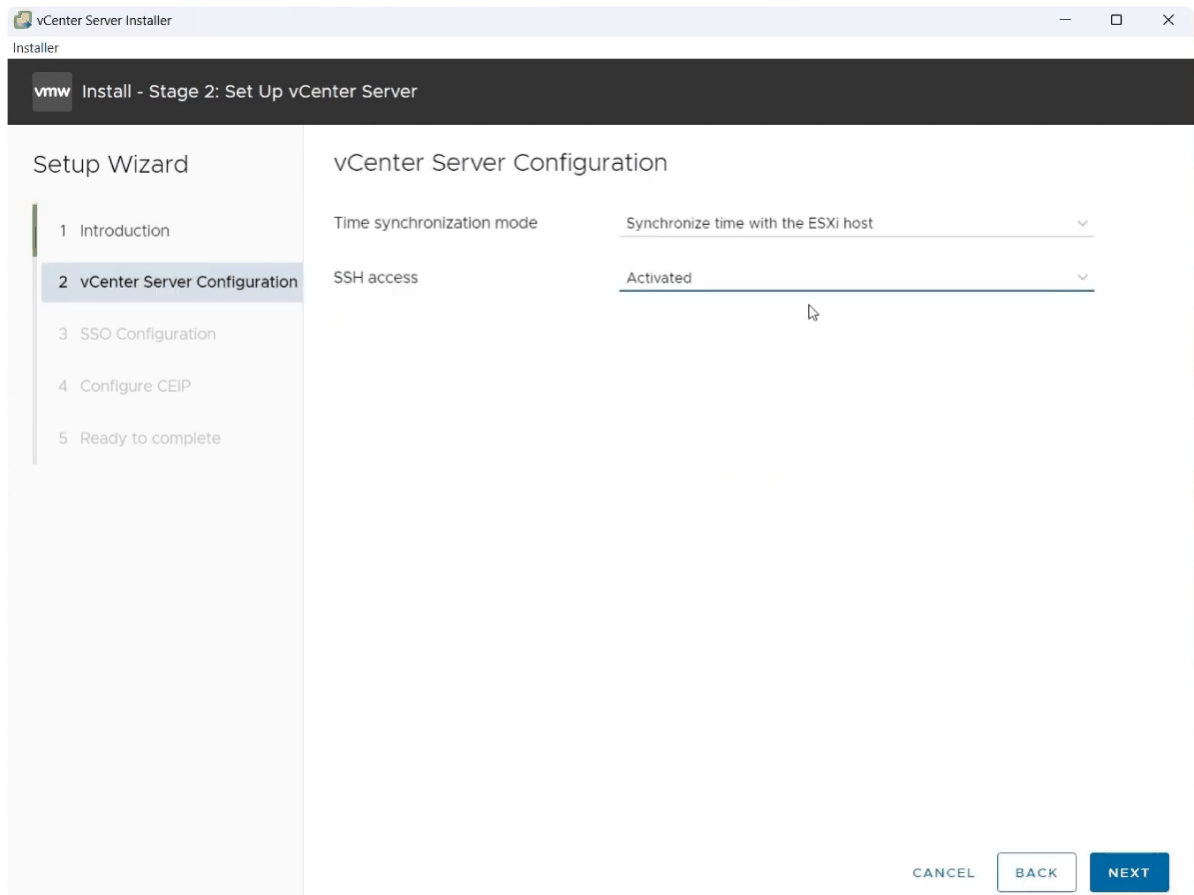
Network Details	
Network	VM Network
IP settings	IPv4, static
IP address	172.16.8.254
Host name	vcenter.local.camicom.com
Subnet mask or prefix length	255.255.0.0
Default gateway	172.16.254.254
DNS servers	172.16.254.254

CANCEL BACK **FINISH**

9. The installation procedure **Stage 1: Deploy vCenter Server** will now create a new virtual machine running on your ESXi host.

INSTALLATION: STAGE 2

1. When you see a message about having successfully deployed the vCenter Server, click **Continue**.
2. In the **Introduction** section, click **Next**.
3. In the **vCenter Server Configuration** section, select the following values:
 - **Time synchronization mode:** Synchronize time with the ESXi host
 - **SSH access:** Activated



Click **Next**.

4. In the **SSO Configuration** section, specify the Single Sign-On (SSO) domain name, username, and password. You will use this username and password to log in to vSphere later.

vCenter Server Installer

Installer

vmw Install - Stage 2: Set Up vCenter Server

Setup Wizard

- 1 Introduction
- 2 vCenter Server Configuration
- 3 SSO Configuration
- 4 Configure CEIP
- 5 Ready to complete

SSO Configuration

☒ Create a new SSO domain

Single Sign-On domain name ? vsphere.local.camicom.com

Single Sign-On username administrator

Single Sign-On password ?

Confirm password ?

Passwords do not match.

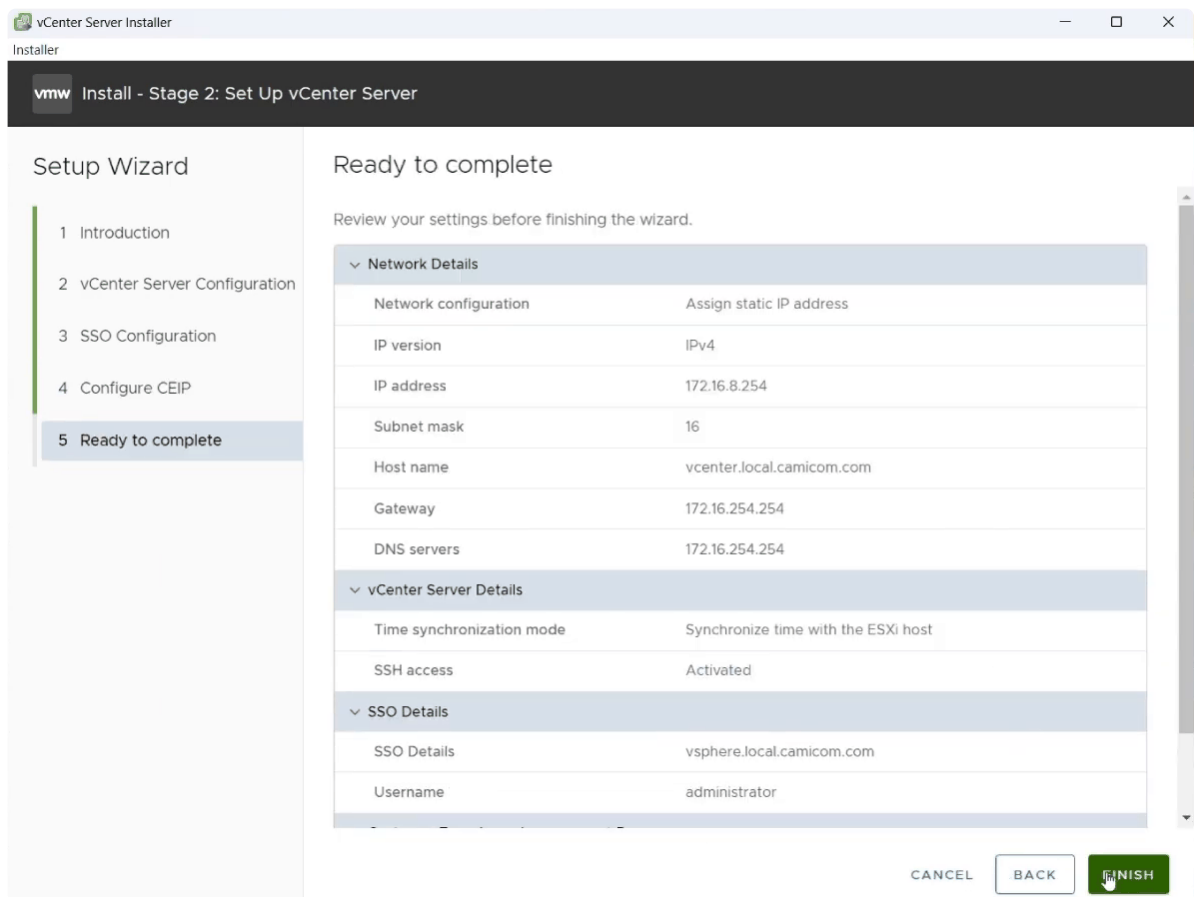
☐ Join an existing SSO domain

vCenter Server

CANCEL BACK NEXT

Click **Next**.

5. In the **Configure CEIP** section, review the information and click **Next**.
6. On the **Ready to complete** section, review the configuration parameters. Click **Back** to edit the configuration; click **Finish** to complete the configuration.



7.5.4.4 Step 4: Create a VMware Cluster and Add Hosts

1. Log in to the **VMware vSphere** client using the username and password you created [earlier](#).
2. Click **Actions > New Datacenter**. Type the name for the Datacenter and click **OK**.
3. In the left pane, click on the created Datacenter, then click **Actions > New Cluster**. The **New Cluster** wizard will open.
4. In the **Basics** section:
 - Enter a name for your cluster.
 - Select the **Manage all hosts in the cluster with a single image** checkbox.
 - Choose **Import image from a new host** from the menu.
 - Select the **Manage configuration at a cluster level** checkbox.

New Cluster

1 Basics
2 Image
3 Configuration
4 Review

Basics

☒ vSphere DRS

☒ vSphere HA

☒ vSAN
☐ Enable vSAN ESA ⓘ

☒ Manage all hosts in the cluster with a single image ⓘ

Choose how to set up the cluster's image

☐ Compose a new image

☐ Import image from an existing host in the vCenter inventory

☒ Import image from a new host

☒ Manage configuration at a cluster level ⓘ

CANCEL NEXT

Click **Next**.

5. In the **Image** section, specify the host IP where you are running the ESXi vCenter Server instance along with the root user credentials. Click **Next**.
6. The **Configuration** section may or may not contain any details, you can safely click **Next**.
7. In the **Review** section, check the cluster configuration. Click **Back** to edit the parameters; click **Finish** to complete the configuration.

ADDING HOSTS

1. In the left pane of the **vSphere Client**, click the cluster icon (🏠). Keep expanding the vCenter instance menu until you see the cluster you have just created. Click on the cluster name, then click the **Actions** button in the right pane and select **Add Hosts**. The **Add hosts** wizard will open.
2. In the **Add hosts** section, specify the IP address for the second ESXi server and the root username and password. Click **Next**.

Add hosts

1 Add hosts
2 Host Summary
3 Import Image
4 Review

Add new and existing hosts to your cluster

New hosts (1) Existing hosts (0 from 0)

☐ Use the same credentials for all hosts

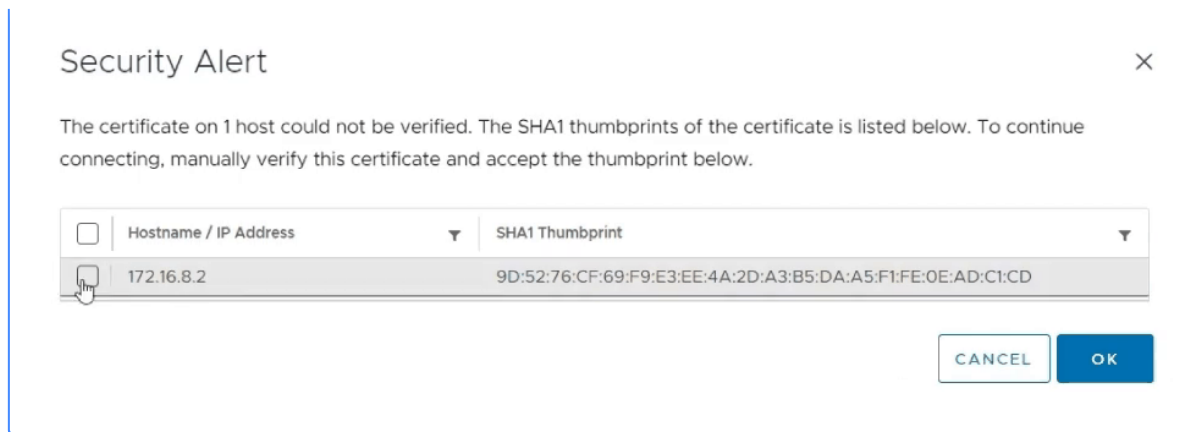
172.17.8 Username Password

ADD HOST

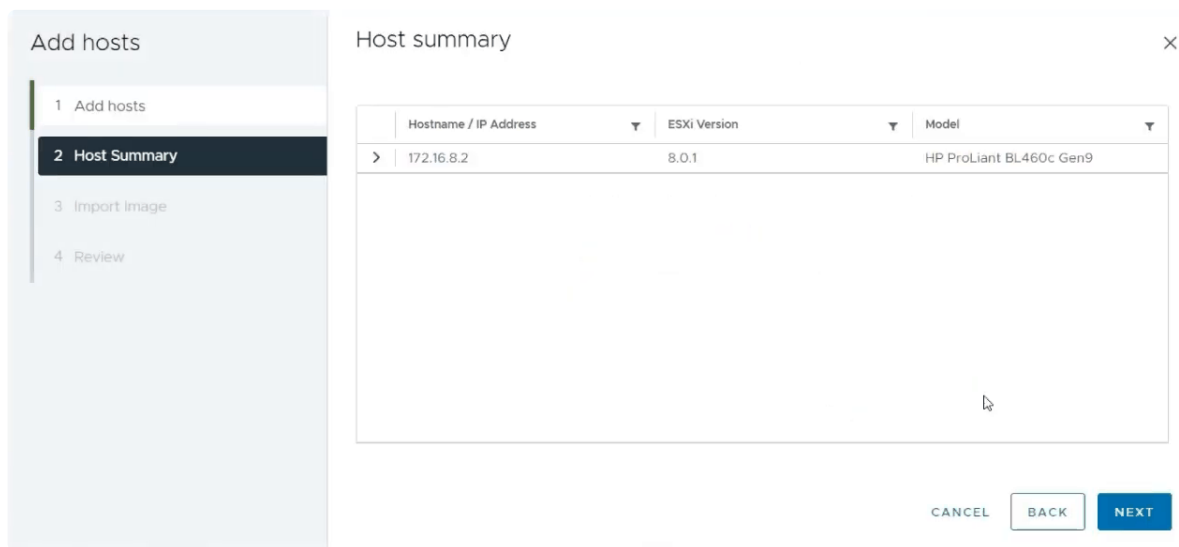
CANCEL NEXT

Note

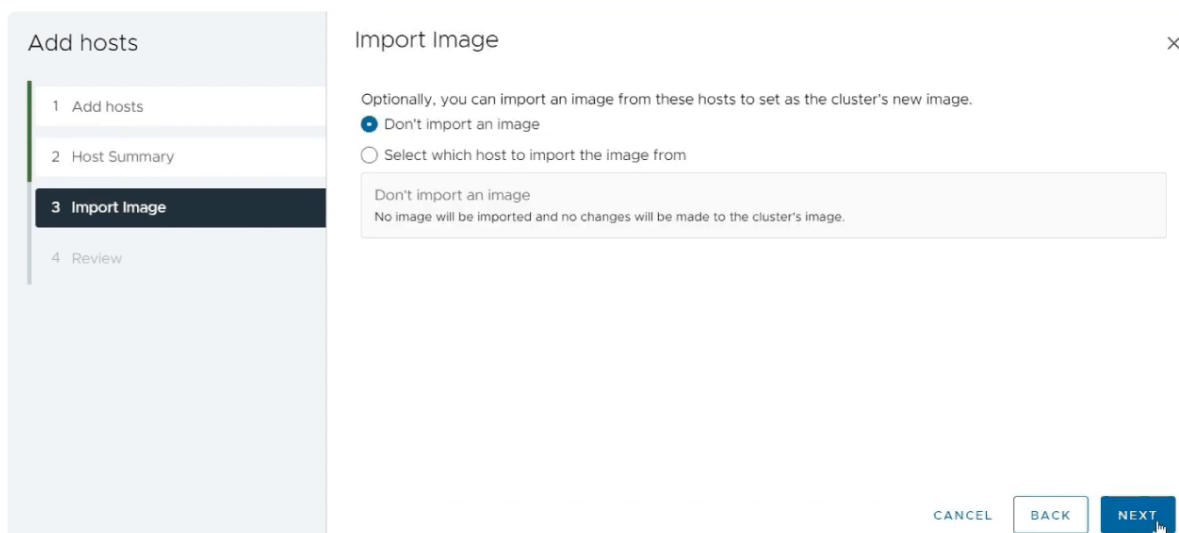
vSphere may show a **Security Alert** about the new host's certificate not being verifiable. Verify the SHA1 thumbprint and click **OK** to accept it and continue.



3. In the **Host Summary** section, you will see the details of the host you have just added. Click **Next**.



4. In the **Import Image** section, select **Don't import an image**, then click **Next**.

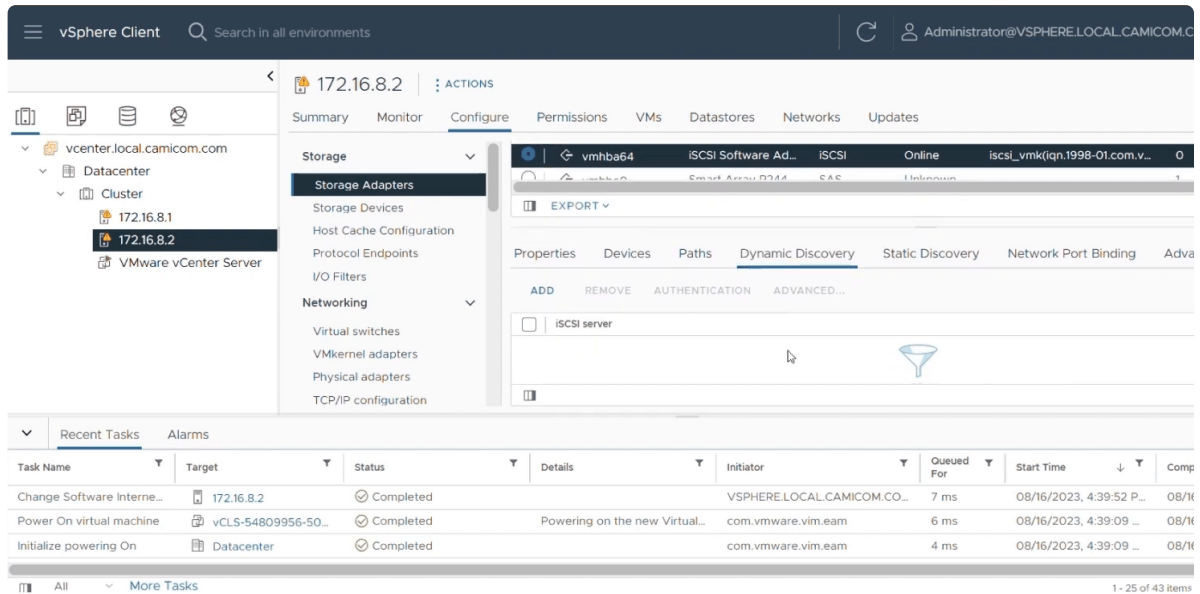


5. In the **Review** section, review the host IP that will be connected to the vCenter Server and moved to the cluster. Click **Finish**.

6. You will see the new host added to the cluster menu in the left pane.

CONNECTING THE HOSTS TO THE ISCSI STORAGE

1. In the left pane of the **vSphere Client**, click on the host you have just added in the [Adding hosts](#) section. Click **Configure > Storage Adapters**.
2. Click **Add Software Adapter** and select **Add iSCSI adapter**.
3. Click on the new iSCSI adapter on the list of adapters, then click **Dynamic Discovery > ADD**.



4. Specify the iSCSI Server IP and port. Make sure that the **Inherit authentication settings from parent** checkbox is selected and click **OK**.
5. Click the **Rescan storage** button and select **Scan for new storage devices** and **Scan for new VMFS volumes**. Click **OK**. The datastore you created in [Step 2](#) should now appear on this host as well.
6. You will now be able to access the iSCSI storage from both ESXi hosts.

7.5.4.5 Step 5: Setting Up Networking

1. In the left pane of the **vSphere Client**, click on the Datacenter. Click the **Actions** button and select **Distributed Switch > New Distributed Switch**. The **New Distributed Switch** wizard will open.
2. In the **Name and location** section, enter the name for the distributed switch. Click **Next**.
3. In the **Select version** section, select your version of VMware ESXi. Click **Next**.
4. In the **Configure settings** section, specify the parameters that correspond to your environment needs or use the default values. Click **Next**.
5. In the **Ready to complete** section, review the new distributed switch settings. Click **Back** to edit the parameters; click **Finish** to complete the configuration.

New Distributed Switch

- 1 Name and location
- 2 Select version
- 3 Configure settings
- 4 Ready to complete

Ready to complete

Review your settings selections before finishing the wizard.

Name	DSwitch
Version	8.0.0
Network Offloads compatibility	None
Number of uplinks	4
Network I/O Control	Enabled
Default port group	DPortGroup

▼ Suggested next actions

- New Distributed Port Group
- Add and Manage Hosts

① These actions will be available in the Actions menu of the new distributed switch.

CANCEL BACK FINISH

6. In the left pane, select the newly created distributed switch. Click the **Actions** button and select **Add and Manage Hosts**. The **Add and Manage Hosts** wizard will open.
 - a. In the **Select task** section, select **Add hosts**. Click **Next**.
 - b. In the **Select hosts** section, click **New hosts**, select both ESXi hosts in the cluster, click **OK**, then click **Next**.
 - c. In the **Manage physical adapters** section, assign two physical NICs per host to the distributed switch. Click **Next**.

DSwitch - Add and Manage Hosts

- 1 Select task
- 2 Select hosts
- 3 Manage physical adapters
- 4 Manage VMkernel adapters
- 5 Migrate VM networking
- 6 Ready to complete

Manage physical adapters

Add or remove physical network adapters to this distributed switch.

Adapters on all hosts Adapters per host

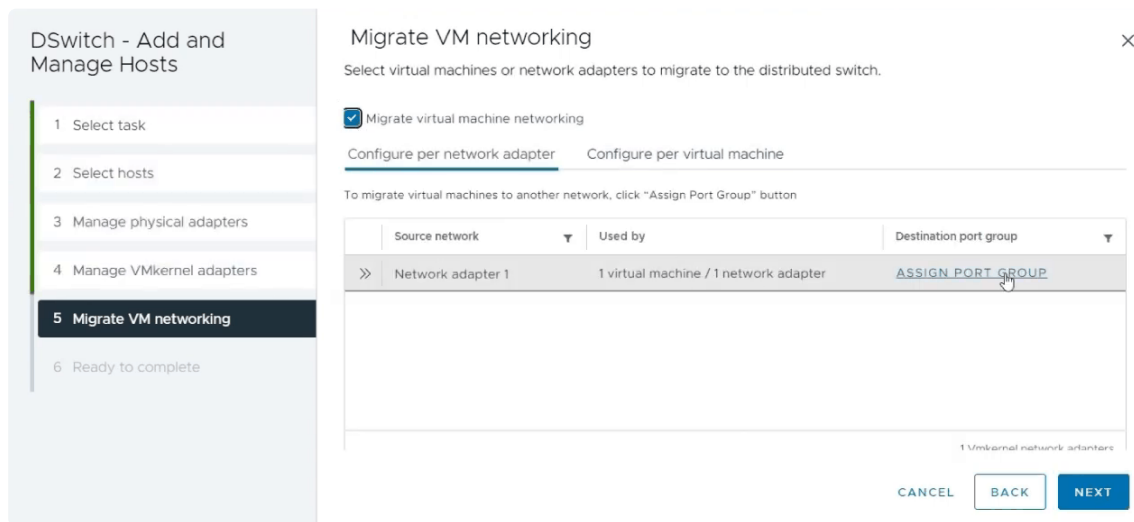
To associate a physical network adapter with an uplink, use "Assign uplink". This assignment would be applied to all the hosts that have the same physical network adapter available.

Physical network adapters	In use by switch	Assign uplink
>> vmnic0	2 hosts / 2 switches	None
>> vmnic1	2 hosts / 0 switches	None
>> vmnic2	2 hosts / 0 switches	None
>> vmnic3	2 hosts / 0 switches	None
>> vmnic4	2 hosts / 0 switches	None
>> vmnic5	2 hosts / 0 switches	None

6 physical network adapters

CANCEL BACK NEXT

- d. In the **Manage VMkernel adapters** section, accept the defaults. Click **Next**.
- e. In the **Migrate VM networking** section, select the network adapters of your existing virtual machines and assign them to the distributed switch, so that these VMs keep their network connection when migrated between hosts. Click **Next**.



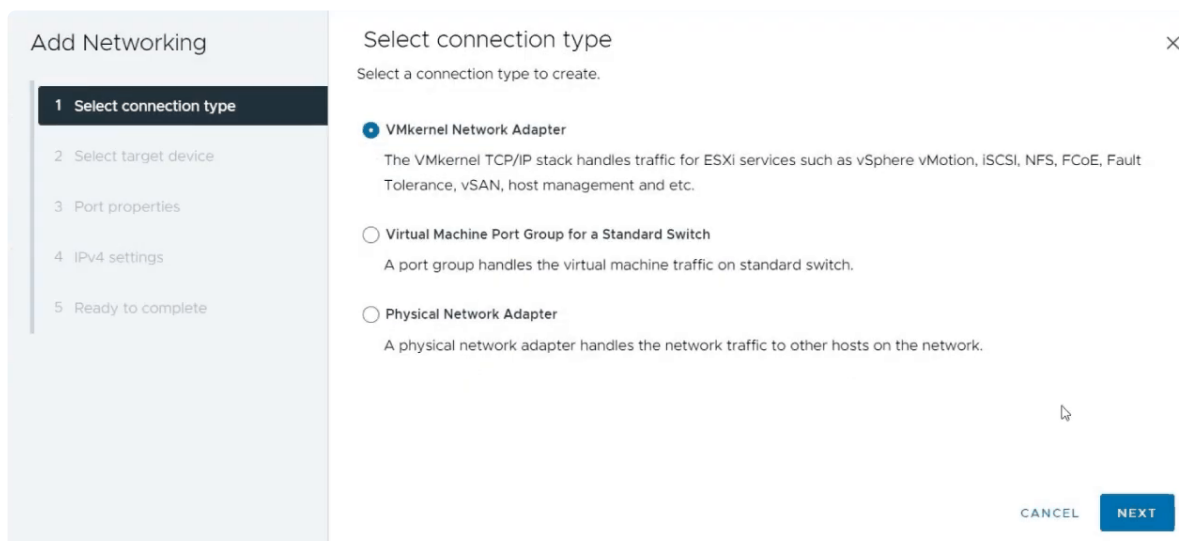
f. In the **Ready to complete** section, review the configuration summary and click **Finish**.

7. In the left pane, select the distributed switch. In the **Hosts** and **VMs** tabs, confirm that both ESXi hosts and the vCenter Server virtual machine are now connected to it. A virtual machine connected to this distributed switch will keep its network connection when it is vMotioned between hosts.

CREATING A DEDICATED NETWORK FOR VMOTION TRAFFIC

vMotion traffic requires its own network connection, recommended to be a dedicated 10 Gbit (or faster) link, separate from the network(s) used for host management and guest traffic. Repeat the steps below on **each** ESXi host.

1. In the left pane of the **vSphere Client**, click on one of the ESXi hosts. On the right, click the **Actions** button and select **Add Networking**. The **Add Networking** wizard will open.
2. In the **Select connection type** section, select **VMkernel Network Adapter**. Click **Next**.



3. In the **Select target device** section, select **New standard switch** and click **Next**.
4. In the **Create a standard switch** section, add two physical network adapters to it: mark one as **Active** and the other as **Standby**. This gives the vMotion network a failover path if the active adapter fails. Click **Next**.

5. In the **Port properties** section:

- In the **Network label** field, enter a network name, e.g. VMotion.
- For **TCP/IP stack**, select **vMotion** – this stack is optimized specifically for vMotion traffic.
- Select the **vMotion** service checkbox.

Click **Next**.

6. In the **IPv4 settings** section, enter a static IP address and subnet mask for this host on a dedicated vMotion subnet. This subnet must be completely separate from your management and guest networks. Click **Next**.

Add Networking

- Select connection type
- Select target device
- Create a Standard Switch
- Port properties
- IPv4 settings**
- Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically
☒ Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway ☐ Override default gateway for this adapter

CANCEL BACK NEXT

7. In the **Ready to complete** section, review the configuration summary and click **Finish**.

Repeat this procedure on the remaining ESXi host, assigning it a static IP address on the same vMotion subnet.

Once done, click **Configure** > **Virtual switches** on each host to confirm you now have three virtual switches:

- The distributed switch, used for virtual machine network traffic.
- **vSwitch0**, used for the management network and iSCSI traffic.
- **vSwitch1**, used for vMotion traffic.

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Comp
Update network configur...	172.16.8.2	Completed		VSPHERE.LOCAL.CAMICOM.CO...	11 ms	08/16/2023, 4:47:05 ...	08/16
Update network configur...	172.16.8.1	Completed		VSPHERE.LOCAL.CAMICOM.CO...	11 ms	08/16/2023, 4:45:55 ...	08/16
Reconfigure virtual mach...	VMware vCenter Se...	Completed	Reconfiguring Virtual Machi...	VSPHERE.LOCAL.CAMICOM.CO...	5 ms	08/16/2023, 4:42:33 P...	08/16

7.5.4.6 Step 6 (optional): Verify That vMotion Works

Before installing the OpenVMS guest, verify that vMotion is functioning correctly by migrating the vCenter Server virtual machine between the two ESXi hosts.

1. In the left pane of the **vSphere Client**, right-click the vCenter Server virtual machine and select **Migrate**. The **Migrate** wizard will open.

2. In the **Select the migration type** section, select **Change compute resource only**. Click **Next**.

Migrate | VMware vCenter Server

1 Select a migration type

2 Select a compute resource

3 Select networks

4 Select vMotion priority

5 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

VM origin ⓘ

- ☒ **Change compute resource only**
Migrate the virtual machines to another host or cluster.
- ☐ **Change storage only**
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- ☐ **Change both compute resource and storage**
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- ☐ **Cross vCenter Server export**
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL NEXT

3. In the **Select a compute resource** section, select the other ESXi host in the cluster. Click **Next**.

Migrate | VMware vCenter Server

1 Select a migration type

2 Select a compute resource

3 Select networks

4 Select vMotion priority

5 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

VM origin ⓘ

Hosts Clusters Resource Pools vApps

Quick Filter Enter value

	Name	State	Status	Cluster
☐	172.16.8.1	Connected	Warning	Cluster
☒	172.16.8.2	Connected	Warning	Cluster

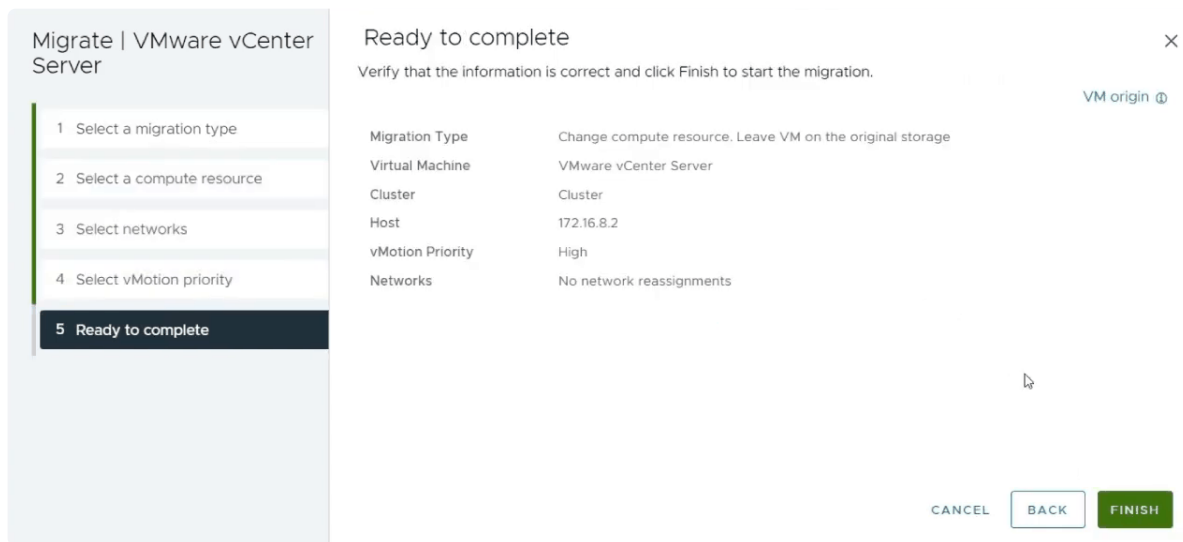
2 Items

Compatibility

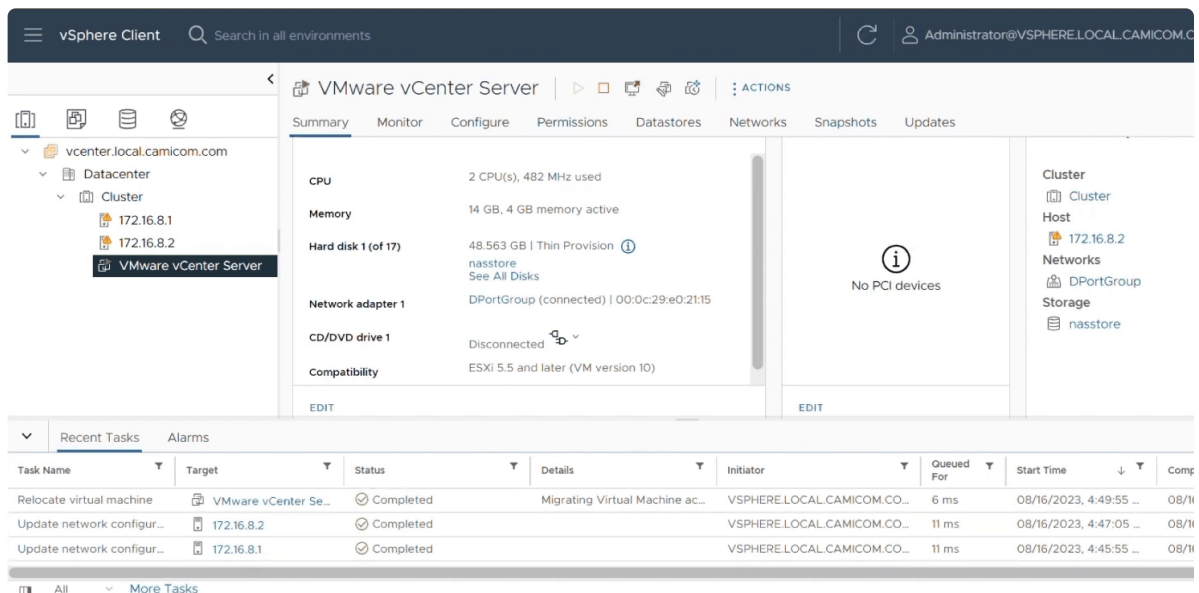
CANCEL BACK NEXT

4. In the **Select vMotion priority** section, select **Schedule vMotion with high priority (recommended)**. Click **Next**.

5. In the **Ready to complete** section, review the configuration summary and click **Finish**.



6. Click on the VMware vCenter Server virtual machine and check its IP address in the **Summary** tab. Once the migration completes, the IP address updates to reflect the host to which the virtual machine has moved, confirming that vMotion works correctly on this cluster.



7.5.4.7 Step 7: Create the OpenVMS x86-64 Virtual Machine

1. In the left pane of the **vSphere Client**, select the first ESXi host. Click **Actions > New Virtual Machine**. The **New Virtual Machine** wizard will open.
2. In the **Select a creation type** section, select **Create a new virtual machine**. Click **Next**.

New Virtual Machine

- Select a creation type**
- Select a name and folder
- Select a compute resource
- Select storage
- Select compatibility
- Select a guest OS
- Customize hardware
- Ready to complete

Select a creation type

How would you like to create a virtual machine?

- Create a new virtual machine**
- Deploy from template
- Clone an existing virtual machine
- Clone virtual machine to template
- Convert template to virtual machine
- Clone template to template

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

CANCEL NEXT

- In the **Select a name and folder** section, enter a name for the virtual machine. Click **Next**.
- In the **Select a compute resource** section, select the ESXi host on which the virtual machine should initially run (you will move it to the other host later, using vMotion). Click **Next**.

New Virtual Machine

- Select a creation type
- Select a name and folder
- Select a compute resource**
- Select storage
- Select compatibility
- Select a guest OS
- Customize hardware
- Ready to complete

Select a compute resource

Select the destination compute resource for this operation

- Datacenter
 - Cluster
 - 172.16.8.1**
 - 172.16.8.2

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

- In the **Select storage** section, select the iSCSI datastore you created in [Step 2](#). Click **Next**.

New Virtual Machine

- Select a creation type
- Select a name and folder
- Select a compute resource
- Select storage**
- Select compatibility
- Select a guest OS
- Customize hardware
- Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

VM Storage Policy Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Cluster
☐	datastor...	--	8.5 GB	1.41 GB	7.09 GB	VMFS 6	
☒	nasstore	--	2 TB	750.14 GB	1.8 TB	VMFS 6	

Items per page 10 2 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

6. In the **Select compatibility** section, select **ESXi 8.0 and later** (or the compatibility level matching your ESXi version). Click **Next**.

7. In the **Select a guest OS** section, set **Guest OS Family** to **Other** and **Guest OS Version** to **Other 64-bit**. Click **Next**.

8. In the **Customize hardware** section:

- Set **CPU** to 2.
- Set **Memory** to 6 GB.
- Set the hard disk size to 30 GB and make sure it is placed on the iSCSI datastore.
- Click **Add New Device > SATA Controller**, then reassign the hard disk to the new SATA controller.
- Remove the default SCSI controller, since it is not needed.
- Under **Network Adapter**, connect the adapter to the distributed switch created in [Step 5](#). Expand the adapter's settings and set a custom MAC address matching the DECnet address you plan to configure for this node once OpenVMS is installed.

- Under **CD/DVD Drive**, select **Datastore ISO File** and browse to the VSI OpenVMS x86-64 installation ISO image previously uploaded to the iSCSI datastore. Make sure **Connect At Power On** is selected and that the drive is attached to the SATA controller.
- Expand **VM Options** and set **Firmware** to **EFI** (instead of **BIOS**).
- Expand the **Advanced** section and set **EFI Quick Boot** to **Disabled**.

The screenshot shows the 'New Virtual Machine' wizard with the 'Customize hardware' step selected. The left sidebar lists steps 1 through 8, with '7 Customize hardware' highlighted. The main area shows hardware configuration options:

Component	Value	Unit	Actions
Memory *	8	GB	
> New Hard disk *	40	GB	
> New SCSI controller	LSI Logic Parallel		
> New Network	VM Network	Connected	
> New CD/DVD Drive	Client Device	Connect At Power On	
> Video card	Specify custom settings		
> New SATA Controller *	New SATA Controller		
> Security Devices	Not Configured		
> Other	Additional Hardware		

Compatibility: ESXi 7.0 and later (VM version 17)

Buttons: CANCEL, BACK, NEXT

Click **Next**.

9. In the **Ready to complete** section, review the configuration summary and click **Finish**.

The screenshot shows the 'New Virtual Machine' wizard with the 'Ready to complete' step selected. The left sidebar lists steps 1 through 8, with '8 Ready to complete' highlighted. The main area shows a configuration summary:

Property	Value
Virtual machine name	vms89
Folder	Datacenter
Host	172.16.8.1
Datastore	nasstore
Compatibility	ESXi 7.0 and later (VM version 17)
Guest OS name	Other (64-bit)
Virtualization Based Security	Disabled
CPU	4
Memory	8 GB
NICs	1
NIC 1 network	DPortGroup (DSwitch)
NIC 1 type	E1000E

Click Finish to start creation.

Buttons: CANCEL, BACK, FINISH

7.5.4.8 Step 8: Install VSI OpenVMS x86-64 and Join the Cluster

1. Power on the newly created virtual machine and launch its console.
2. At the **Boot Manager** screen, type **OPA0** to enable the Guest Console.

```
VSI OpenVMS Boot Manager: V9.2-* Build 160
```

```
ENABLED: Symmetric Multi-Processing
ENABLED: Crash Dump Processing
```

```

ENABLED: Legacy Serial Port Console for remote COM 1
ENABLED: Using Environment ROM

Checking Required Processor Features: PASSED
Identifying devices. This may take a while. COMPLETED

VIRTUAL MACHINE GUEST:
KVM (tm) No Mouse support; Use Command or Arrow Keys

BOOT MANAGER DEVICE: DKA0
DEFAULT BOOT COMMAND: BOOT DKD1 0x00 0x00000001

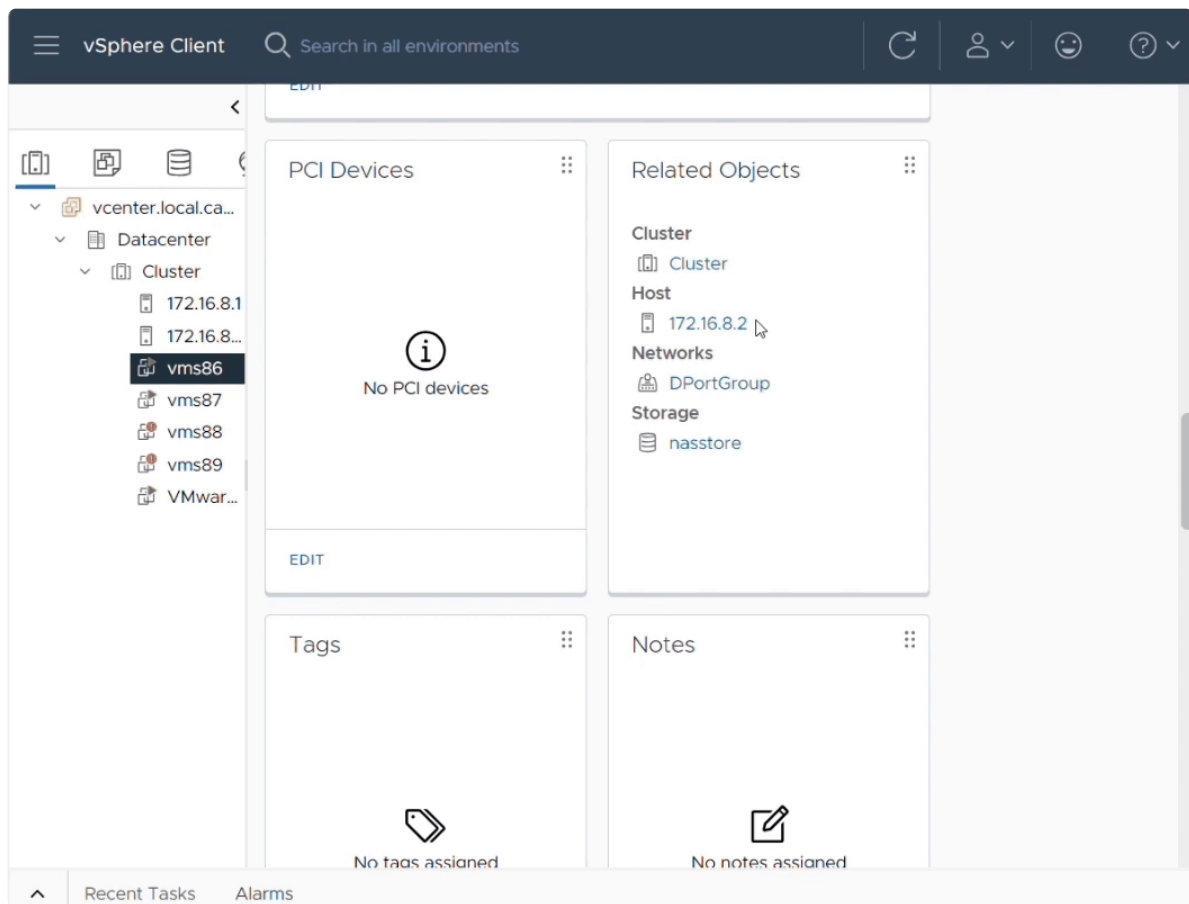
BOOTMGR> OPA0

```

3. Boot from DKA100 (or a different emulated DVD drive) to start the OpenVMS installation.
4. From the installation menu, select option 1) and proceed through the standard OpenVMS installation. For detailed instructions, refer to the [VSI OpenVMS x86-64 E9.2-4 Installation Guide](#).
5. After the installation completes and the system reboots, configure TCP/IP networking and DECnet on the new node. For details on how to do so, refer to the [VSI OpenVMS x86-64 E9.2-4 Installation Guide](#).
6. Add this system as a member of your existing OpenVMS cluster. For details on how to do so, refer to the [Guidelines for OpenVMS Cluster Configurations](#) chapter in the *System Manager's Manual Volume 2: Tuning, Monitoring, and Complex Systems*.
7. Enable the Guest Console feature on this OpenVMS guest, if it was not already enabled during installation. For detailed instructions, refer to the [VSI OpenVMS x86-64 Boot Manager User Guide](#).

7.5.4.9 Step 9: Perform vMotion on the OpenVMS Guest

1. In the left pane of the **vSphere Client**, right-click the OpenVMS virtual machine you have just installed and select **Migrate**. The **Migrate** wizard will open.
2. In the **Select the migration type** section, select **Change compute resource only**. Click **Next**.
3. In the **Select a compute resource** section, select the ESXi host in the cluster to which you wish to migrate your OpenVMS instance. Click **Next**.
4. In the **Select vMotion priority** section, select **Schedule vMotion with high priority (recommended)**. Click **Next**.
5. In the **Ready to complete** section, review the configuration summary and click **Finish**.
6. Click on the virtual machine and check its IP address in the **Summary** tab. It should be updated to reflect the ESXi host to which the virtual machine has been migrated.



8. Troubleshooting

8.1 Troubleshooting a VMware ESXi Virtual Machine Configuration

8.1.1 Access Denied Error

When trying to connect to your ESXi VM using a terminal emulator and entering correct credentials, you may get an `Access denied` message.

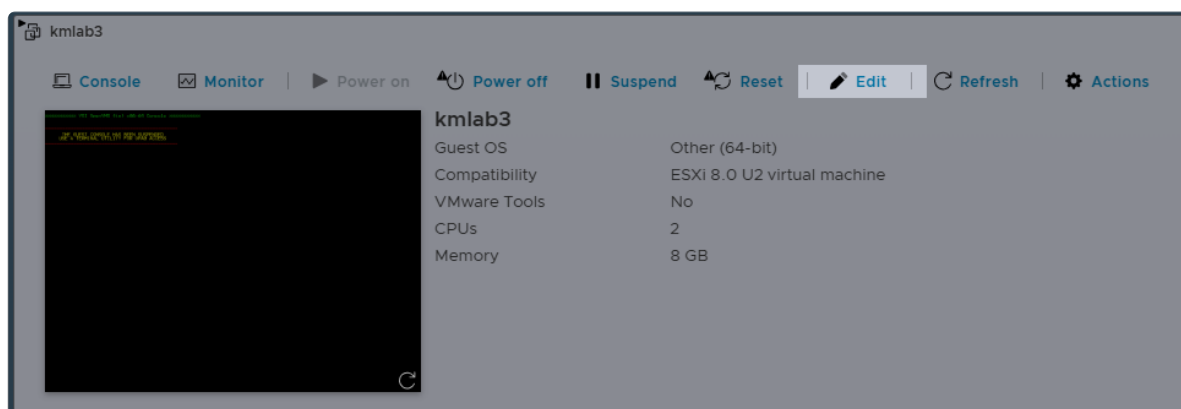
To resolve this issue, perform the following steps:

1. Make sure your terminal emulator settings are configured as described in [Connecting to the OpenVMS Console](#).
2. Press `Ctrl` + `U` before entering your password and type in your password again.

8.1.2 OPA0: Session Is Hung

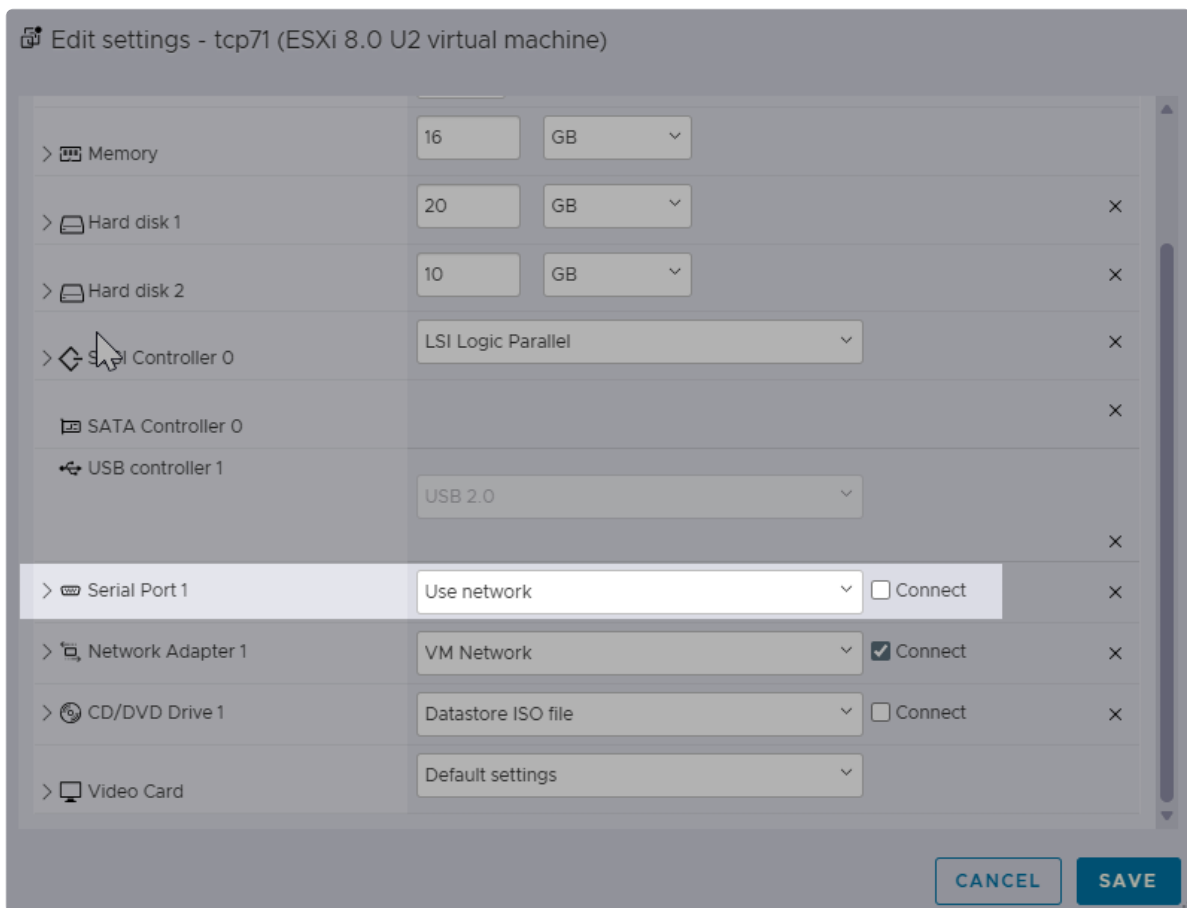
If your OPA0: session appears to be hung, you can perform the following steps to reset the session:

1. In the **ESXi Host Client**, click on the virtual machine, then click the **Edit** button on the virtual machine details page.



A pop-up window will open.

2. In the **Edit Settings** window, uncheck the **Connect** box as shown below:



3. Click **Save**.
4. Open the **Edit Settings** window again by clicking **Edit**. Check the **Connect** box in the **Serial Port** section.
5. Click **Save**. Your OPA0: session has now been reset.

8.1.3 Blocked Network Traffic

If DECnet is installed or LAN Failover is in use, you may find that network traffic is being blocked. This affects all network traffic, including TCP/IP.

By default, DECnet and LAN Failover will change the MAC addresses on their network interfaces to addresses starting with "AA-00-04-00", followed by the encoded DECnet address or the remainder of the MAC address if LAN Failover is in use. By default, most hypervisors block traffic after this MAC address change as a safety measure.

To resolve this issue, you can use one of the following methods:

- Configure the hypervisor to allow MAC address changes. For instructions on how to do this, refer to the [MAC Address Changes](#) section.
- Configure the virtual machine with the MAC address that corresponds to the DECnet address.

 Note

This workaround will not work with LAN Failover enabled as the LAN Failover MAC address is applied to any member of the LAN Failover set.

The method to calculate the MAC address is described in the "Configuring a Cluster Alias" section of the *VSI DECnet-Plus for OpenVMS Installation and Configuration Manual*.

For instructions on how to change the MAC address on the virtual network interface, refer to *Adding Network Adapters to your ESXi VM*.

- Configure DECnet to not change the MAC address on the interface.

If you are running DECnet-Plus and do not need to use addressing compatible with DECnet Phase IV, you can disable Phase IV addressing by editing
SYSS\$MANAGER:NET\$ROUTING_STARTUP.NCL.

For example, you would change the following command:

```
SET NODE 0 ROUTING CIRCUIT SVA-1 ENABLE PHASEIV ADDRESS = TRUE
```

to the command below in order to disable Phase IV addressing on the circuit:

```
SET NODE 0 ROUTING CIRCUIT SVA-1 ENABLE PHASEIV ADDRESS = FALSE
```

- Do not run DECnet. If you do not need to use any DECnet protocols, disable DECnet from starting up. Alternatively, choose not to install it when going through the installation procedure or delete it from your system afterwards.

8.2 Known Issues and Limitations

This section describes known issues and limitations when running VSI OpenVMS x86-64 V9.2-3 or higher as a guest operating system on VMware ESXi virtual machines.

8.2.1 Changing Settings of a Running Virtual Machine May Cause a Hang

Even if the hypervisor appears to allow it, do not change the configuration of a VSI OpenVMS virtual machine while it is running, as this may cause it to hang. Before editing any VM settings, make sure to power off the virtual machine.

8.2.2 Time of Day May Not Be Maintained Correctly in Virtual Machine Environments

VSI OpenVMS x86-64 V9.2-3 and earlier may not maintain the time of day correctly in virtual machine environments after certain events, such as booting or suspending a virtual machine and other similar events (depending on the virtual machine host).

To keep the time of day accurate in such cases, use the **SET TIME** command. If this does not resolve the problem, enter the following command from the SYSTEM account:

```
$ @SYS$MANAGER:UTC$SET_TIME.COM
```

Starting with the E9.2-4 release of VSI OpenVMS x86-64, the use of VM Tools services resolves this issue. Refer to the [Synchronizing Time Between an OpenVMS Virtual Machine and a Host System](#) section for details.

8.2.3 Possible Issues with VMware Virtual Machines

- Enabling EFI mode before finishing the virtual machine creation will require recreating it from scratch to avoid errors when adding SCSI controllers.
- Virtual machines created in VMware ESXi hypervisors may not operate as intended until you manually set the parameters listed in [Additional Configuration Steps](#).

Depending on your specific configuration, there may be cases where you may *not* need to set one or more of those parameters.

8.3 Finetuning and Best Practices

8.3.1 vCPU and Scheduling

- Start with two vCPUs for small OpenVMS instances; only add more if you see sustained CPU demand.
- Avoid over-provisioning vCPUs. Too many vCPUs can increase scheduling latency and make interactive sessions feel slower.
- For latency-sensitive workloads (terminal responsiveness, DECnet routing, etc.), prefer fewer, busy vCPUs rather than many mostly idle ones.

8.3.2 Memory

- Allocate enough RAM to keep OpenVMS from heavy paging; monitor pagefile usage inside OpenVMS.
- Avoid aggressive memory overcommit on the ESXi host for OpenVMS production VMs.
- Keep memory reservations for critical OpenVMS systems if the host is heavily loaded, so they are not ballooned or swapped by ESXi.

8.3.3 Storage

- Use a paravirtual SCSI controller type that is supported starting with VSI OpenVMS x86-64 Version E9.2-4.
- Place system disks for OpenVMS on storage with low latency and good IOPS, such as NVMe SSD.
- [PCI passthrough for Fibre Channel](#) provides the fastest performance for shared cluster data disks.

8.3.4 Network

- Use a single vNIC for simple test systems; add separate vNICs for management, DECnet, and application traffic if you need isolation.
- Assign vNICs to separate physical NICs for higher performance.
- Ensure the vSwitch and port group settings match the VLAN and MTU of your physical network.

8.3.5 Console and Serial Behavior

Document the exact console connection method (pipe name, port, host), so operations staff can reach it during outages.

For more information on performance tuning, see [VMware documentation](#).