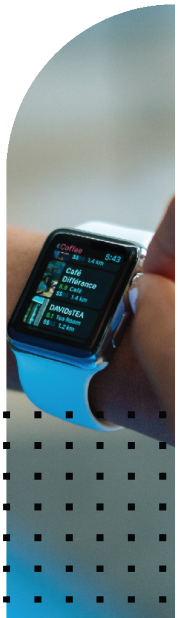
Hyper V Deployment Guide

FortiDeceptor 5.3.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 6, 2024
FortiDeceptor 5.3.0 Hyper V Deployment Guide
00-530-806195-20240306

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-03-15	Initial release.
2024-03-06	Updated Configure the hardware settings on page 13.
2024-09-06	Added Minimum system requirements on page 6.

About FortiDeceptor VM on Microsoft Hyper-V

FortiDeceptor VM is a 64-bit virtual appliance version of FortiDeceptor. It is deployed in a virtual machine environment. Once the virtual appliance is deployed and set up, you can manage FortiDeceptor VM via its GUI in a web browser on your management computer.

This document provides information about deploying a FortiDeceptor VM in Microsoft Hyper-V environments.

This includes how to configure the virtual hardware settings of the virtual appliance. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For that information, see the *FortiDeceptor Administration Guide* in the Fortinet Document Library.

Licensing

Fortinet offers the FortiDeceptor in a stackable license model. This model allows you to expand your VM solution as your environment expands. For information on purchasing a FortiDeceptor license, contact your Fortinet Authorized Reseller, or visit https://www.fortinet.com/how_to_buy/.

For more information, see the FortiDeceptor product data sheet available on the Fortinet web site, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiDeceptor.pdf.

After placing an order for FortiDeceptor, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiDeceptor with Customer Service & Support at https://support.fortinet.com.

Upon registration, you can download the license file. You will need this file to activate your FortiDeceptor. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded and validated, the CLI and GUI will be fully functional.

Minimum system requirements

The following are the minimum system requirements for deploying decoys with FortiDeceptor for Hyper-V:

Technical Specification	Details
Virtual CPUs (min / max)	4/ Unlimited
Virtual Network Interfaces	2-6
Virtual Memory (min / max)	8GB / Unlimited
Virtual Storage (min / max)	HDD 500GB/ 16TB

A minimum of 8GB of memory and two CPUs are required for the VM. Fortinet recommends that the number of CPU cores be four more than the number of Deception VMs, and 3GB of RAM per Deception VM.

Deploying FortiDeceptor VM on Microsoft Hyper-V

To deploy FortiDeceptor VM on Microsoft Hyper-V:

1. Prepare the FortiDeceptor image for Hyper-V on page 7
2. Configure the Virtual Machine on page 9
3. Configure the hardware settings on page 13

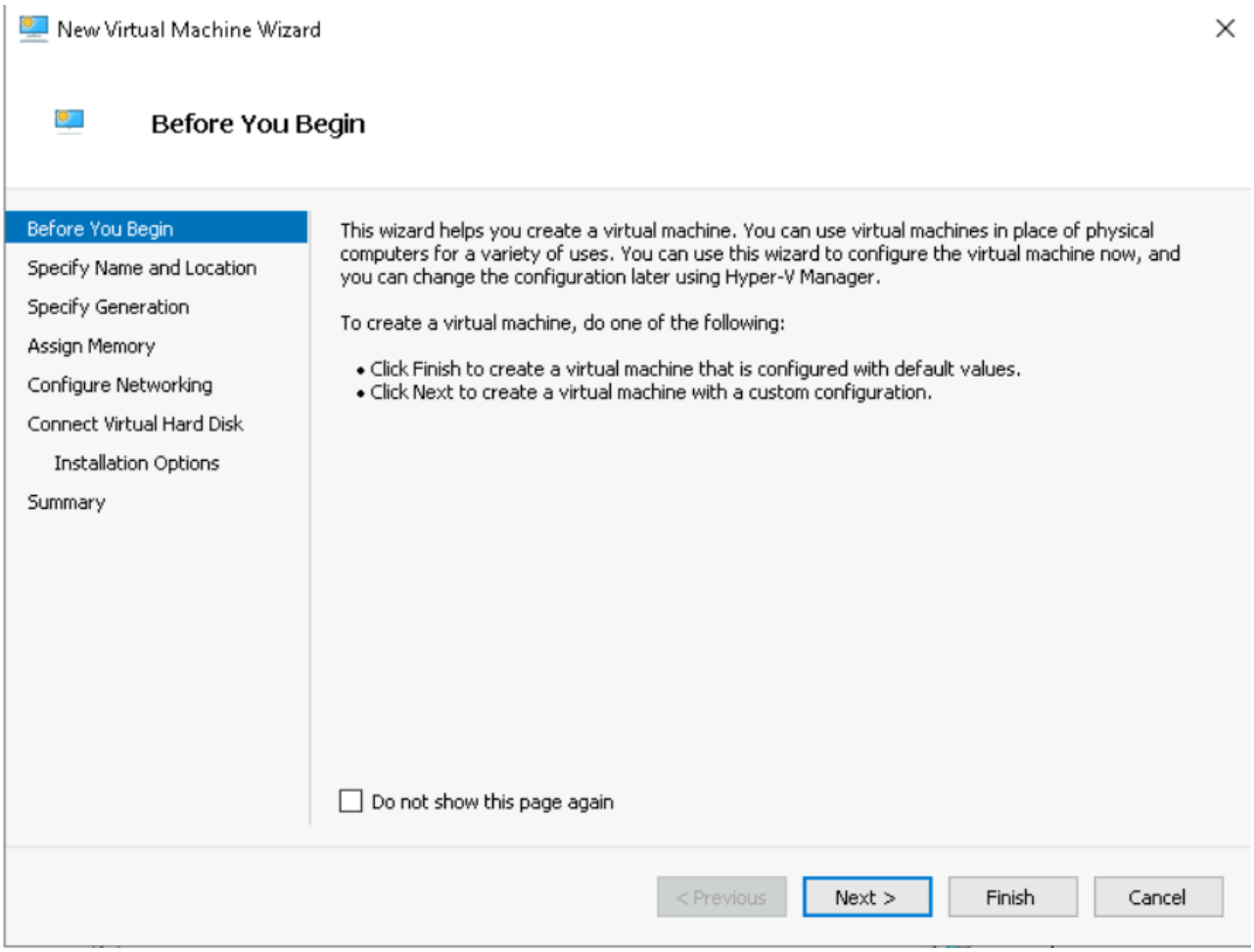
Prepare the FortiDeceptor image for Hyper-V

Download the image archive file for the Hyper-V platform and unzip it to get image file *.out.hyperv.zip*. After the image is downloaded, connect to the Hyper-V server to create the Virtual Machine.

To download the FortiDeceptor image:

1. Log in to FortiCloud.
2. In the banner, click *Support* > *Downloads* > *Firmware Download*. The *Download/Firmware Images* page opens.
3. From the *Select Product* dropdown, select *FortiDeceptor*.
4. Click the *Download* tab.
5. In the *Image File Path* section, click the image folder until you reach the image page.
6. Select *FDC_VM-v400-build0204-FORTINET.out.hyperv.zip*.
7. Go to *Start* > *Windows Administrative* > *Tools* > *Hyper-V Manager* to launch the Hyper-V Manager on your Microsoft server.
8. In the *Actions* pane, click *Connect to Server* to connect to the Hyper-V server.
9. Right-click the server and click *New* > *Virtual Machine*. The *New Virtual Machine Wizard* opens.

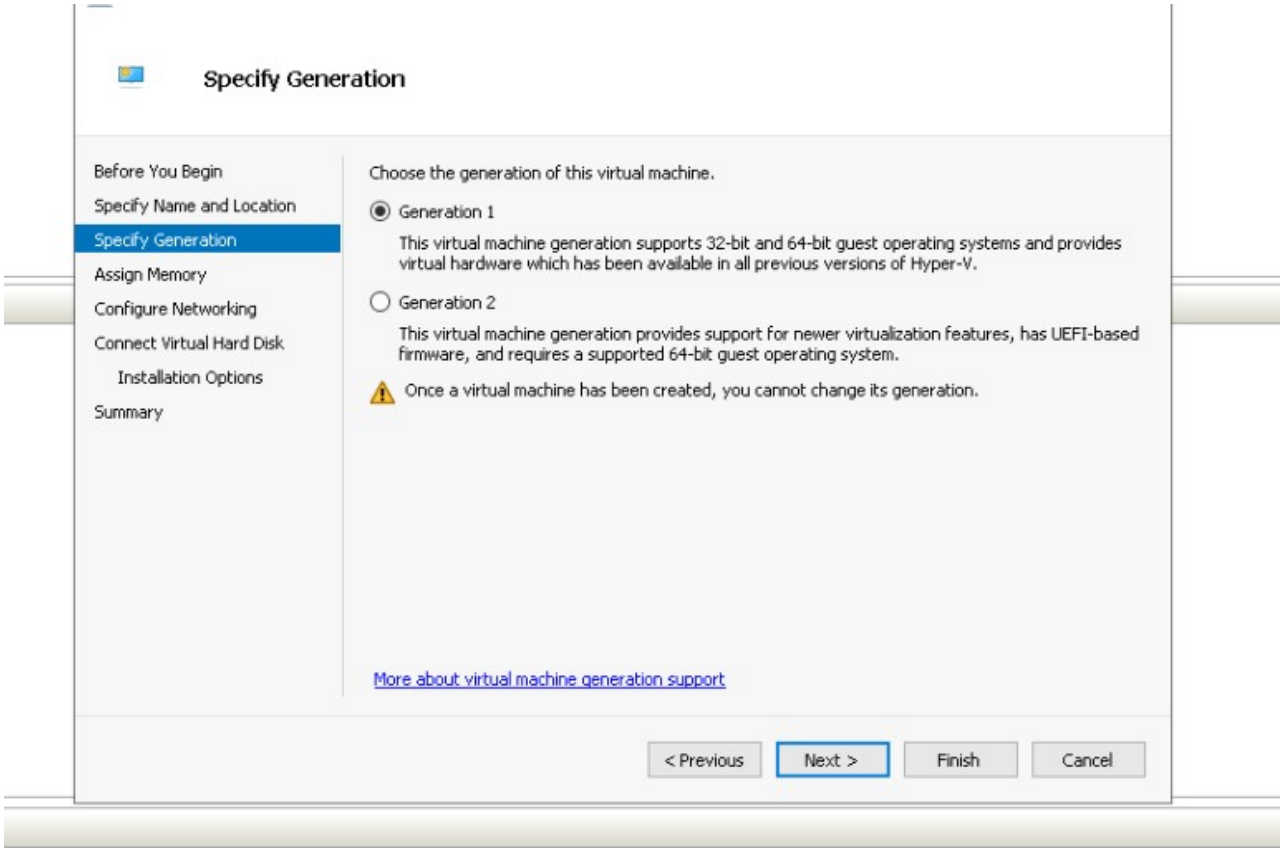
   Alternatively, in the *Actions* menu, you can click *New* > *Virtual Machine* to launch the wizard.


New Virtual Machine Wizard
Before You Begin
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary
This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.
To create a virtual machine, do one of the following:
• Click Finish to create a virtual machine that is configured with default values.
• Click Next to create a virtual machine with a custom configuration.
Do not show this page again
< Previous
Next >
Finish
Cancel

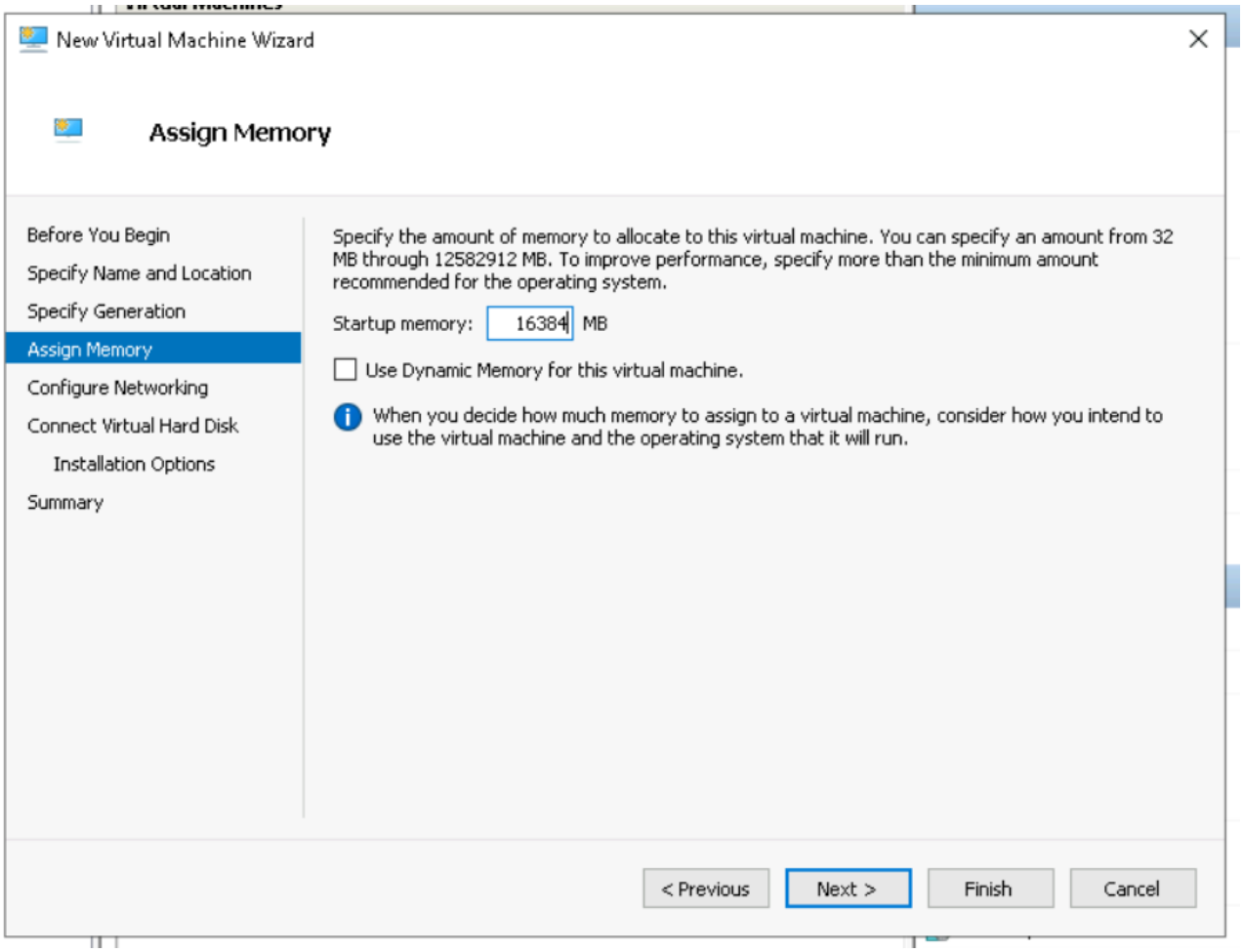
Configure the Virtual Machine

To configure the VM:

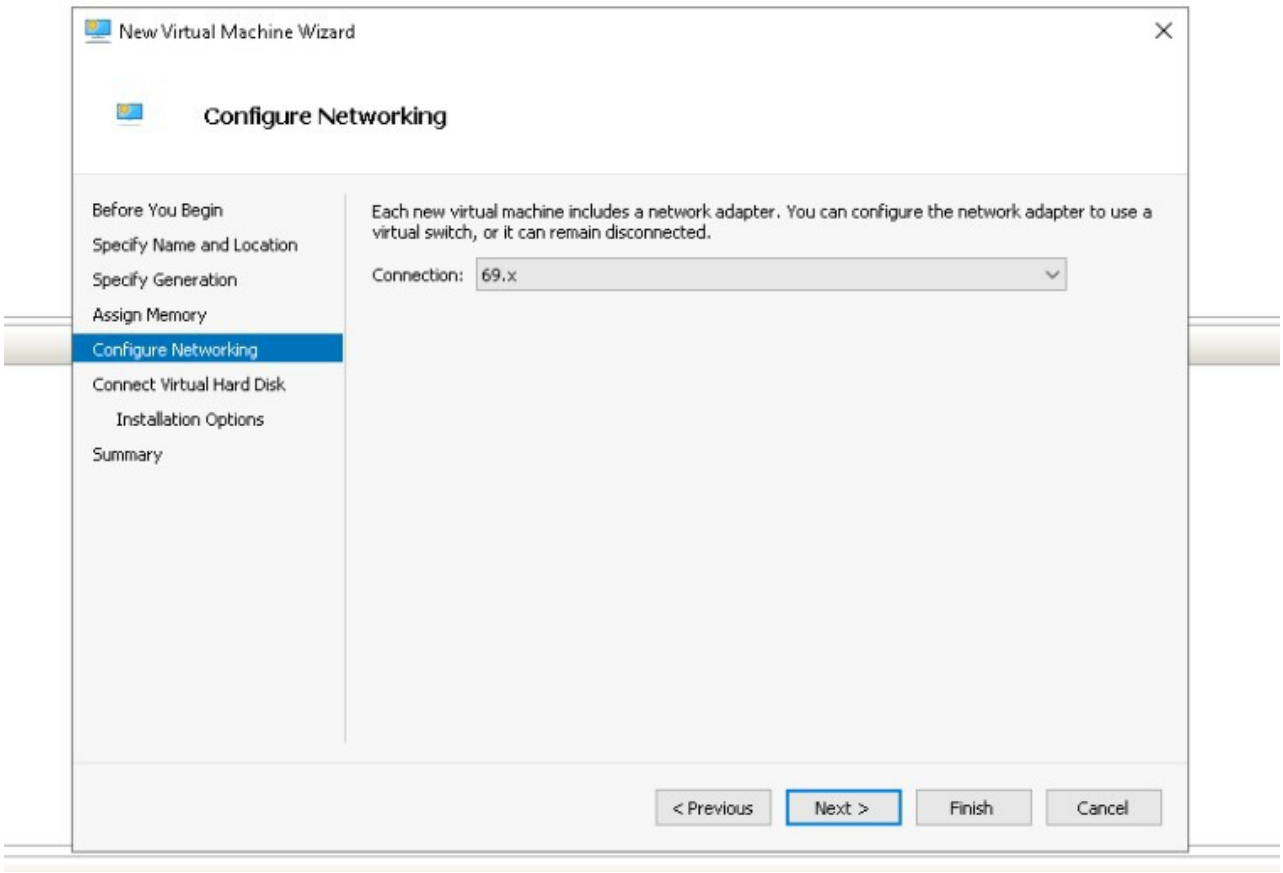
1. Specify a name for your FortiDeceptor and Location (if it is different from the default) for the VM and click *Next*.
2. Select *Generation 1*. This option is mandatory for FortiDeceptor.



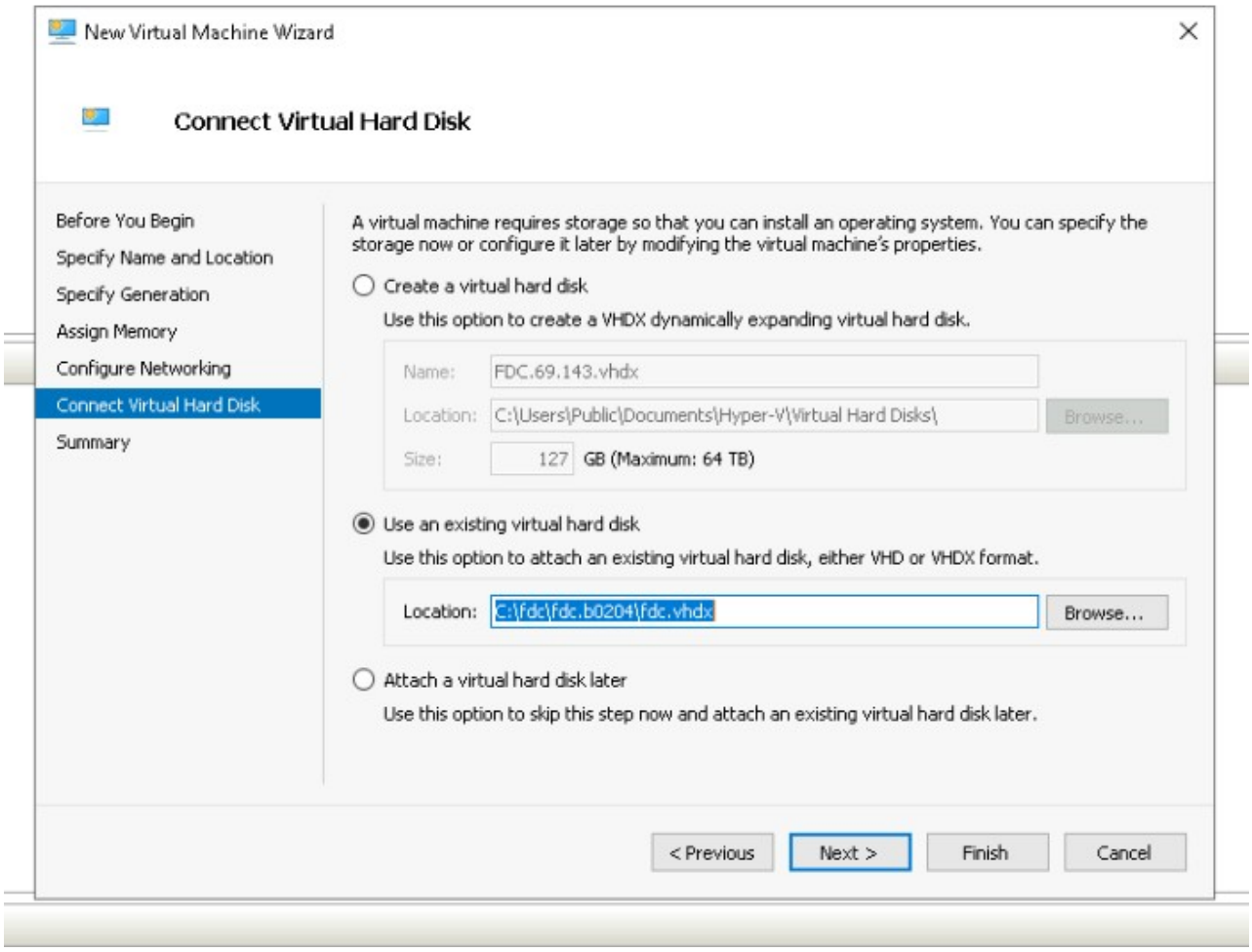
3. In the *Startup memory* field, specify the amount of memory to allocate to this VM and click *Next*.
The recommended memory for the FortiDeceptor VM is 16 GB.


New Virtual Machine Wizard
Assign Memory
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.
Startup memory: 16384 MB
Use Dynamic Memory for this virtual machine.
When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.
< Previous
Next >
Finish
Cancel

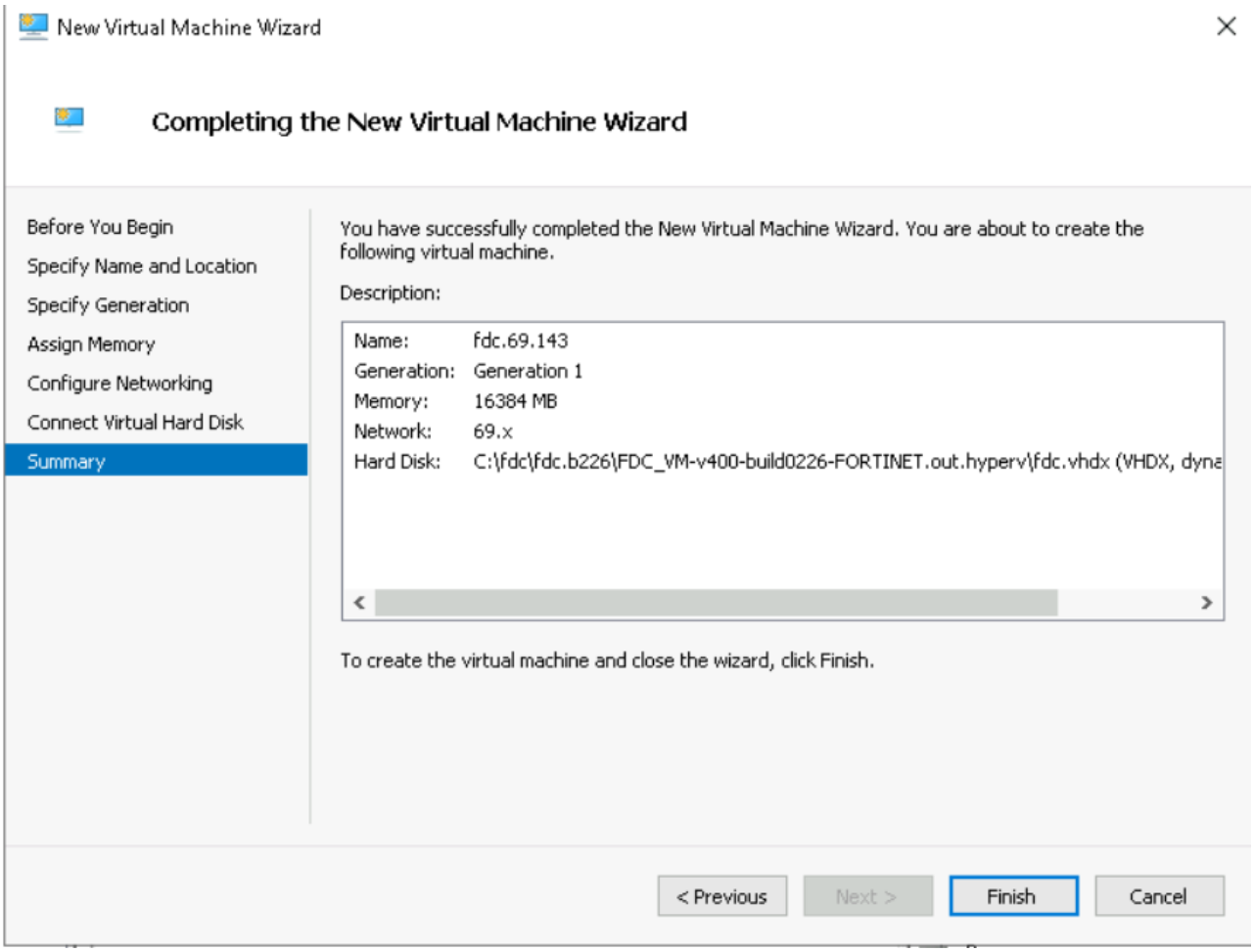
4. From the *Connection* dropdown, configure the network adapter for port1, then click *Next*.



5. Select *Attach a virtual hard disk later* and click *Next*. We will perform this task in a following section.



6. Review the chosen options, then click *Finish*.



Do not start the FortiDeceptor VM until you have completed all the steps in Configure the hardware settings on page 13.

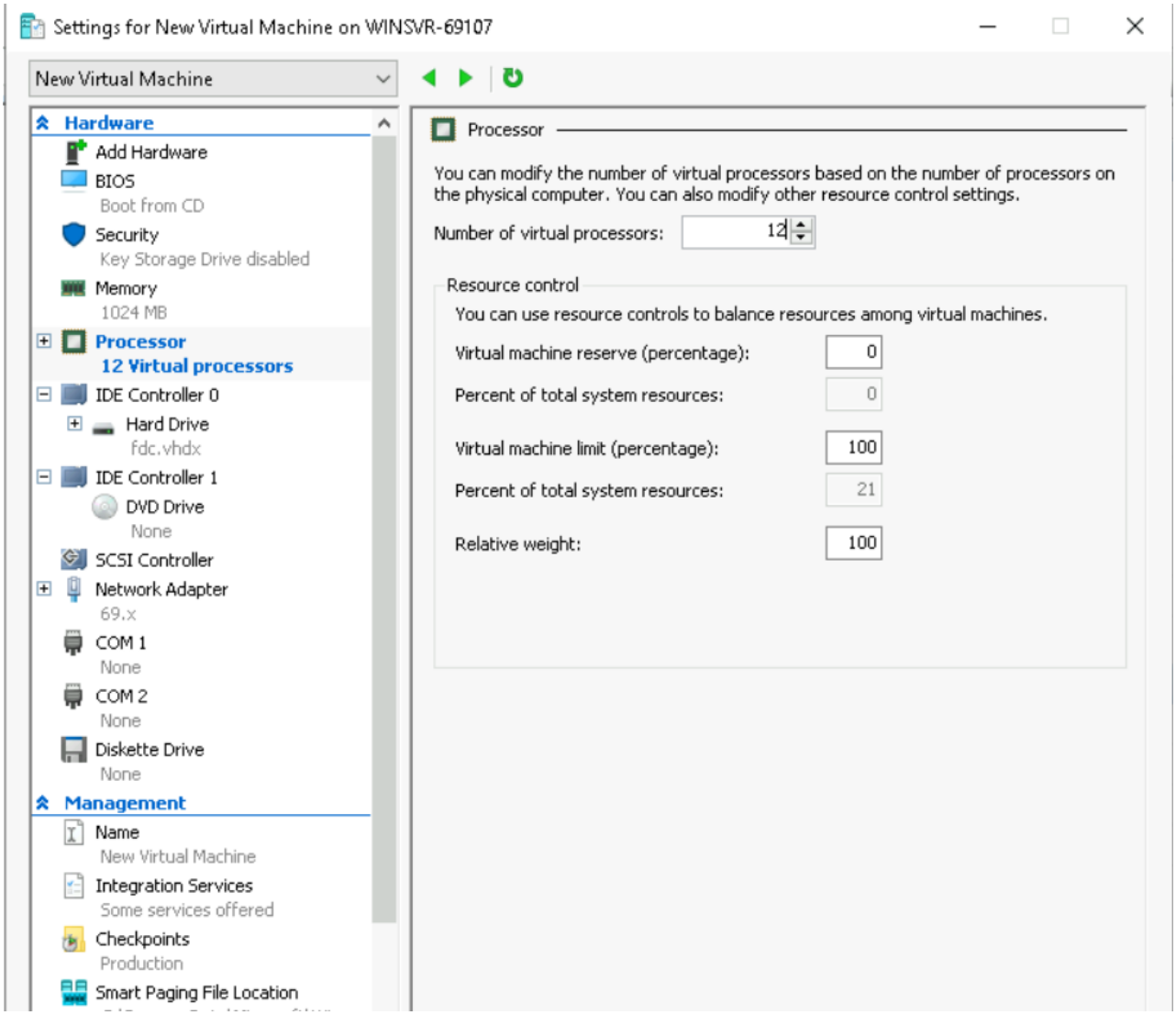
Configure the hardware settings

To configure the hardware settings, set the number of processors and attach the hard drive from the package you downloaded. After you have attached the hard drive, configure the Network Adapter and Deployment Network.

Unlike ESXi, to configure a trunk port on Hyper-V requires using PowerShell commands.

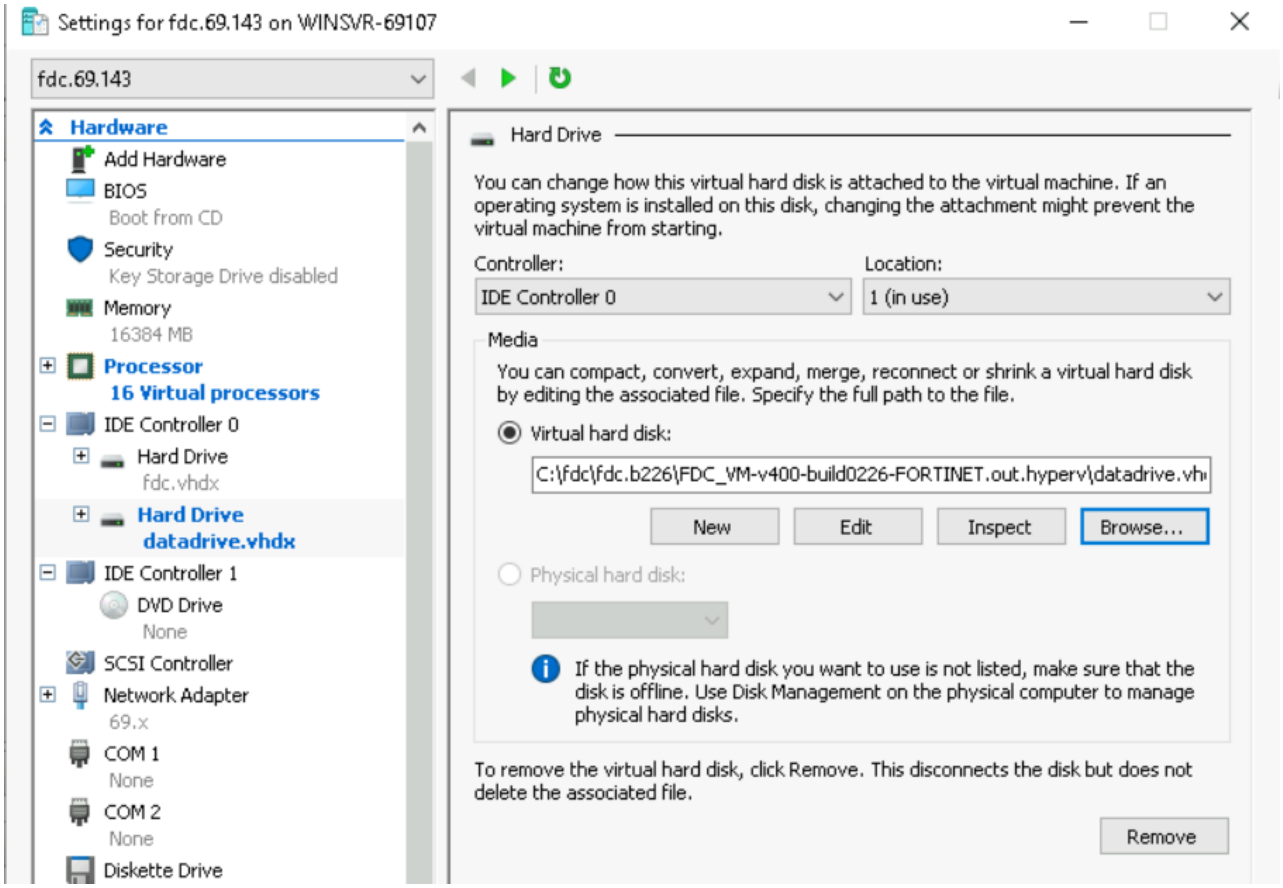
To configure the hardware settings:

1. Right-click the VM you created and click *Settings*.
2. Click *BIOS* and set the BIOS to boot from the IDE as primary by moving it to the top. Click *Apply*.
3. Click *Processor* and set the *Number of virtual processors* to a minimum of 12.

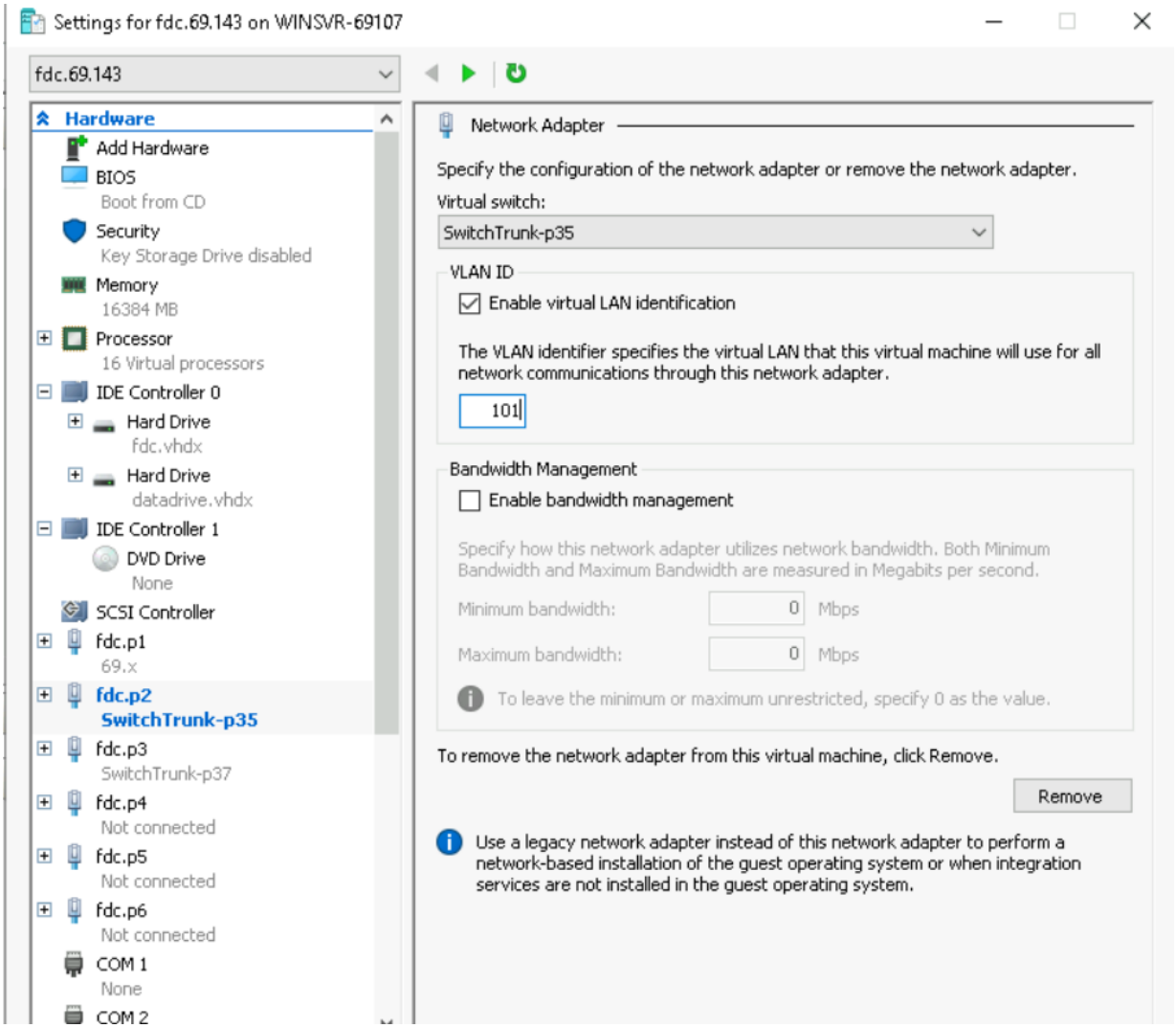


4. Click *IDE Controller 0* and add *Hard Drive*.
5. Select *Virtual Hard Disk*, then click *Browse* to attach the first hard drive from the download package *fdc.vhdx*.

Repeat this step for the second hard drive, '*datadrive.vhdx*'.



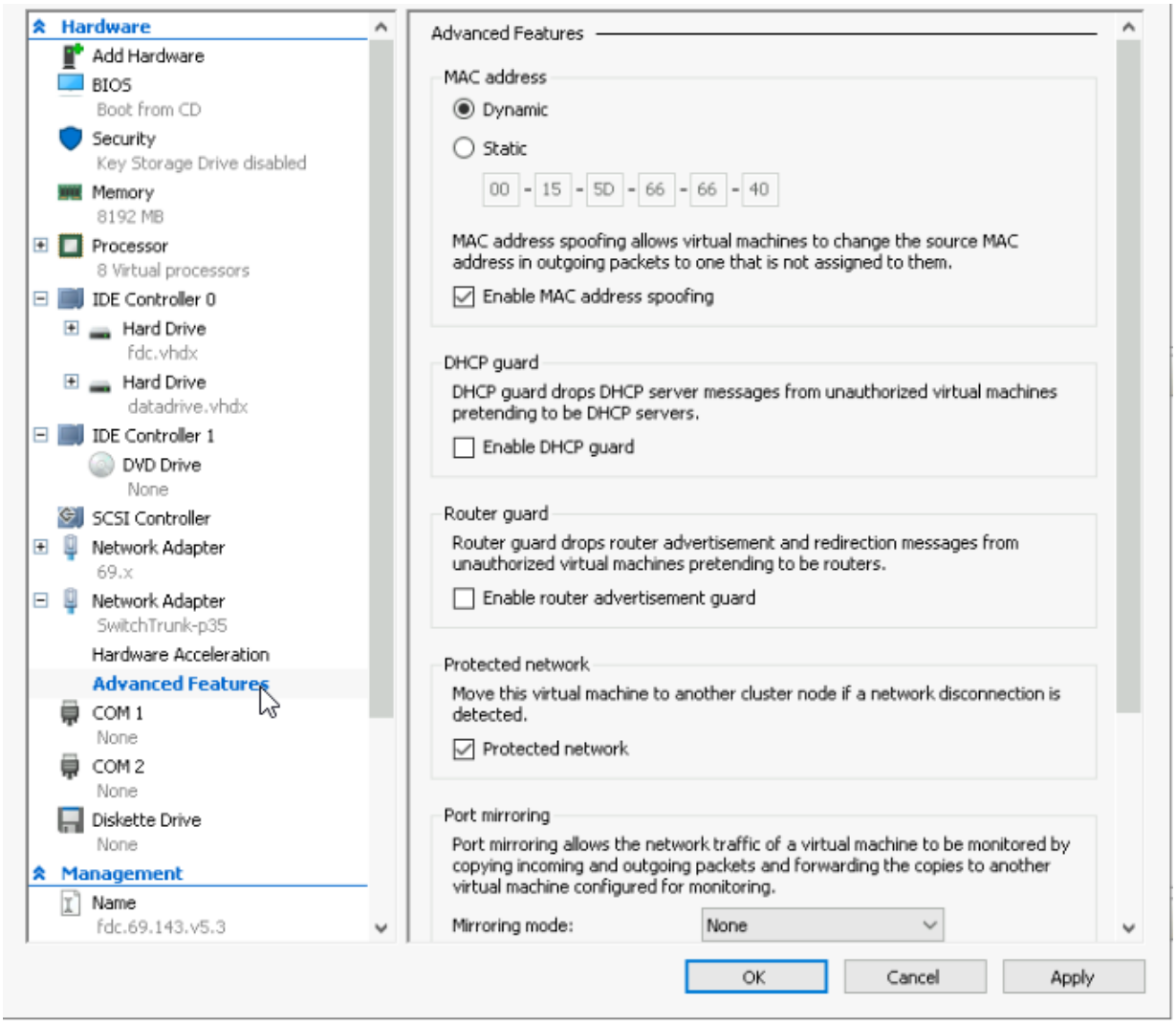
6. FortiDeceptor requires at least two Network Adapters and a maximum of six.
   a. Go to *Add Hardware* > *Network Adapter* > *Add* to attach the Network Adapters.



   b. Click *Advanced Features* and click *Enable MAC address spoofing*.

FortiDeceptor runs inside of Hyper-V and the FortiDeceptor decoy runs inside FortiDeceptor. This structure is called *Nested Virtualization*.

Enabling MAC address spoofing is required to allow the decoy's MAC address to connect to the Hyper-V network. Despite the name *MAC Spoofing*, this is a legitimate and required setting for any type of hypervisor in a Nested Virtualization.



c. Click *Apply* then click *OK*.

7. In the *Management* section, click *Smart Paging File Location* and use the *Browse* button to select the management folder on the Hyper-V server.
8. Open a *PowerShell* window on the Hyper-V server and execute the following CLI command:
   `Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true`
9. Start up the FortiDeceptor console from the *Virtual Machines* window. The default login is *admin* with no password.
10. Open the console of the FortiDeceptor and configure the port1 IP and Default gateway as per the *FortiDeceptor Administration Guide*.
11. (Optional) For Deployment Networks using a trunk port, you will need to configure the network adapter manually.
    a. Add the VM Network Adapter using PowerShell. You can rename the existing adapter.
    `Rename-VMNetworkAdapter -VMName <VMName> -Name "Network Adapter" -Newname <new name>`
    `Add-VMNetworkAdapter -VMName <VMName> -Name <port name>`

```
PS C:\Users\Administrator> Rename-VMNetworkAdapter -VMName fdc.69.143 -Name "Network Adapter" -NewName fdc.p1
PS C:\Users\Administrator> Get-VMNetworkAdapter -VMName fdc.69.143

Name   IsManagementOs VMName     SwitchName MacAddress   Status IPAddresses
----   -------------- ------     ---------- ----------   ------ -----------
fdc.p1 False          fdc.69.143 69.x       000000000000        {}
```

```
PS C:\Users\Administrator> Get-vmswitch

Name            SwitchType NetAdapterInterfaceDescription
----            ---------- ------------------------------
SwitchTrunk-p37 External   Intel(R) I350 Gigabit Network Connection #4
69.x            External   Intel(R) I350 Gigabit Network Connection #3
SwitchTrunk-p35 External   Intel(R) I350 Gigabit Network Connection #2


PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-VMNetworkAdapter -VMName fdc.69.143

Name   IsManagementOs VMName     SwitchName MacAddress   Status IPAddresses
----   -------------- ------     ---------- ----------   ------ -----------
fdc.p1 False          fdc.69.143 69.x       000000000000        {}


PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p2 -SwitchName SwitchTrunk-p35
PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p3 -SwitchName SwitchTrunk-p37
PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p4
PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p5
PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p6
PS C:\Users\Administrator>
```

b. Set the network adpater using VLAN Trunk Mode using the following command:

```
Set-VMNetworkAdaptervlan -VMName <VMName> -VMNetworkAdapterName <AdaptorName> -Trunk
    -AllowedVlanIdList "4-4090" -NativeVlanId 0
```

```
PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p2 -SwitchName SwitchTrunk-p35
PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p3 -SwitchName SwitchTrunk-p37
PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p4
PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p5
PS C:\Users\Administrator> add-vmnetworkadapter -VMName fdc.69.143 -name fdc.p6
PS C:\Users\Administrator> Set-VMNetworkAdaptervlan -VMName fdc.69.143 -VMNetworkAdapterName fdc.p3 -Trunk -AllowedVlanI
dList "4-4090" -NativeVlanId 0
PS C:\Users\Administrator> Get-VMNetworkAdapter -VMName fdc.69.143

Name   IsManagementOs VMName     SwitchName      MacAddress   Status IPAddresses
----   -------------- ------     ----------      ----------   ------ -----------
fdc.p1 False          fdc.69.143 69.x            000000000000        {}
fdc.p2 False          fdc.69.143 SwitchTrunk-p35 000000000000        {}
fdc.p3 False          fdc.69.143 SwitchTrunk-p37 000000000000        {}
fdc.p4 False          fdc.69.143                 000000000000        {}
fdc.p5 False          fdc.69.143                 000000000000        {}
fdc.p6 False          fdc.69.143                 000000000000        {}


PS C:\Users\Administrator>
```

www.fortinet.com