



FortiManager - VMware ESXi Cookbook

Version 6.4

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



November 18th, 2022

FortiManager 6.4 VMware ESXi Cookbook

02-640-620526-20221118

TABLE OF CONTENTS

Change log	4
About FortiManager on VMware ESXi	5
Licensing	5
Trial license	5
Add-on license	6
Preparing for deployment	7
Minimum system requirements	7
Deployment package for VMware ESXi	8
Downloading a deployment package	9
Compatibility for VM hardware versions	9
Deployment	10
Deploying FortiManager on VMware vSphere	10
Deploying the OVF file	11
Configuring hardware settings	15
Powering on the VM	16
Configuring initial settings	17
Enabling GUI access	17
Connecting to the GUI and enabling a trial license	17
Upgrading to an add-on license	18
Configuring your FortiManager	18
Security Fabric connector integration with VMware vCenter	19
vMotion in a VMware environment	24

Change log

Date	Change description
2020-04-09	Initial release.
2020-06-22	Added Security Fabric connector integration with VMware vCenter on page 19.
2021-03-09	Updated Minimum system requirements on page 7.
2021-05-13	Updated About FortiManager on VMware ESXi on page 5.
2021-05-28	Updated information about trial licenses and add-on licenses.
2021-06-02	Updated "Deployment package for VMware ESXi" on page 8
2021-07-15	Updated "Deployment package for VMware ESXi" on page 8.
2021-11-24	Updated "Deploying FortiManager on VMware vSphere" on page 10
2022-09-09	Added "Compatibility for VM hardware versions" on page 9. Updated "Deploying the OVF file" on page 11.
2022-11-18	Updated "Minimum system requirements" on page 7.

About FortiManager on VMware ESXi

This document provides information about deploying a FortiManager virtual appliance in VMware vSphere Hypervisor (ESX/ESXi) and VMware vSphere Client environments.

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

This document does not cover configuring and operating the virtual appliance after successfully installing and starting it. For that information, see the [FortiManager Administration Guide](#).

Licensing

Fortinet offers the FortiManager-VM with a limited, free trial license. Stackable licenses can be purchased, letting you expand your VM solution as your environment expands. You can purchase perpetual or subscription-based licenses. Perpetual licenses never expire.

For information on purchasing a FortiManager-VM license, contact your Fortinet-authorized reseller, or visit [How To Buy](#).

When configuring your FortiManager-VM, ensure that you configure hardware settings as the following table outlines and consider future expansion. Contact your Fortinet-authorized reseller for more information.

License	Devices/VDOMs	GB/day of logs with FortiAnalyzer enabled (not stackable)
Trial License	3	0 FortiAnalyzer features not supported
VM-10-UG	+10	2
VM-100-UG	+100	5
VM-1000-UG	+1000	10
VM-5000-UG	+5000	25
VM-10K-UG	+10000	50

See [Minimum system requirements on page 7](#).

See also the [FortiManager product datasheet](#).

Trial license

With a FortiCare account and FortiManager 6.4.1 or later, FortiManager-VM includes a free limited non-expiring trial license.

The free trial license includes support for to add 3 devices/VDOMS and use 3 ADOMs.

The free trial license does not include services or support.

You can activate the trial license when you connect to the GUI for the FortiManager-VM. Full-feature products and services are available for purchase with an add-on license. See [Connecting to the GUI and enabling a trial license on page 17](#).

Add-on license

You must activate a trial license before you can upgrade FortiManager-VM to a purchased add-on license.

See also [FortiManager 6.4 Trial License Guide](#).

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- [Minimum system requirements](#)
- [Deployment package for VMware ESXi](#)
- [Downloading a deployment package](#)

Minimum system requirements



FortiManager-VM has a minimum requirement of 4 CPU, 8 GB of RAM, and 500 GB of disk storage.

The following table lists the minimum system requirements for your VM hardware, based on the number of devices, VDOMs, or ADOMs that your VM manages.

Maximum devices/ VDOMs	VM hardware requirements	
	RAM (GB)	CPU cores
100	8	4
300	16	6
1200	32	6
4000	64	16
10000	128	24



This table does not take into account other hardware specifications, such as bus speed, CPU model, or storage type.



Enabling FortiAnalyzer features requires more resources.

Deployment package for VMware ESXi

Firmware images on the [Customer Service & Support site](#) include FortiManager-VM deployment packages. The following table lists the available VM deployment package:

VM platform	Deployment file
VMware ESXi	ESX/ESXi server: FMG_VM64-vX-buildxxxx-FORTINET.out.ovf.zip VMware Player: FMG_VM64-vX-buildxxxx-FORTINET.out.vmware.zip



For the latest information on virtualization software support, see the corresponding FortiManager Release Notes on the [Fortinet Docs Library](#).

The `.out.ovf.zip` file contains:

File	Description
DATADRIVE.vmdk	The FortiManager-VM log disk in VMDK format.
FMG.vmdk	The FortiManager system hard disk in Virtual Machine Disk (VMDK) format.
FortiManager-VM64.hw14.ovf	OVF template file for VMware ESXi 6.7 and later versions. Only available in 6.4.2 and later.
FortiManager-VM64.hw14.vapp.ovf	OVF template file for VMware vSphere, vCenter, and vCloud (ESXi 6.7 and later). Only available in 6.4.2 and later.
FortiManager-VM64.ovf	OVF template based on Intel e1000 NIC driver.
FortiManager-VM64.vapp.ovf	OVF template file for VMware vSphere, vCenter, and vCloud (earlier than ESXi 6.7).

The `.out.vmware.zip` file, for use with VMware Player, contains:

- FMG.vmdk: The FortiManager system hard disk in VMDK format.
- FortiManager-VM64.ovf: The VMware virtual hardware configuration file.
- DATADRIVE.vmdk: The FortiManager log disk in VMDK format.
- DATADRIVE-S0XX.vmdk: 41 VMDK files used during deployment.

For more information about FortiManager, see the [FortiManager datasheet](#).

Downloading a deployment package

Firmware image FTP directories are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention. Each firmware image is specific to the device model. For example, the `FMG_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip` image, found in the 5.6.0 directory, is specific to the 64-bit Microsoft Hyper-V Server virtualization environment.



You can download the *FortiManager Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the *FortiManager > Download* tab.



Download the `.out` file to upgrade your existing FortiManager installation.

To download deployment packages:

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar select *Download > Firmware Images*. The *Firmware Images* page opens.
2. Select *FortiManager* from the *Select Product* dropdown list, then select *Download*.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on your management computer.

Compatibility for VM hardware versions

FortiManager-VM supports ESXi 6.5 and later versions. Using corresponding hardware versions 13 and later is highly recommended, as mentioned in [Virtual machine hardware versions](#).

It is recommended to upgrade hardware versions incrementally with only one delta at a time. For example, upgrading from 10 to 11, 11 to 12, 12 to 13, then 13 to 14 is recommended, although directly upgrading from 10 to 14 generally has no issues.

To upgrade hardware versions:

1. Log in to vSphere Client web console.
2. In the left pane tree-menu, right-click the FortiManager-VM.
3. From the shortcut menu, select *Compatibility > Schedule VM Compatibility Upgrade*.
4. Click **YES**.
5. From the *Compatible with* dropdown, select the desired compatibility.
6. Click **OK**.
7. Reboot the FortiManager-VM.

Deployment

Prior to deploying the FortiManager, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiManager presume that you are familiar with the management software and terminology of your VM platform.

You might also need to refer to the documentation provided with your VM server. The deployment information in this guide is provided as an example because, for any particular VM server, there are multiple ways of creating a virtual machine - command line tools, APIs, alternative graphical user interface tools.

Before you start your FortiManager appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiManager, you will have access only through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiManager GUI (see [Enabling GUI access on page 17](#)).

Deploying FortiManager on VMware vSphere

After you download the `FMG_VM64-v5-buildxxxx-FORTINET.out.ovf.zip` file and extract the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

Prior to deploying the FortiManager-VM, ensure that you configure the following and they are functioning properly:

- You must install VMware vSphere Hypervisor™ (ESX/ESXi) software on a server and update it to the latest patch release prior to installing FortiManager. Go to [What is a vSphere Hypervisor?](#) for installation details.
- You must install VMware vSphere Client™ on the computer that you will use for managing the FortiManager-VM.

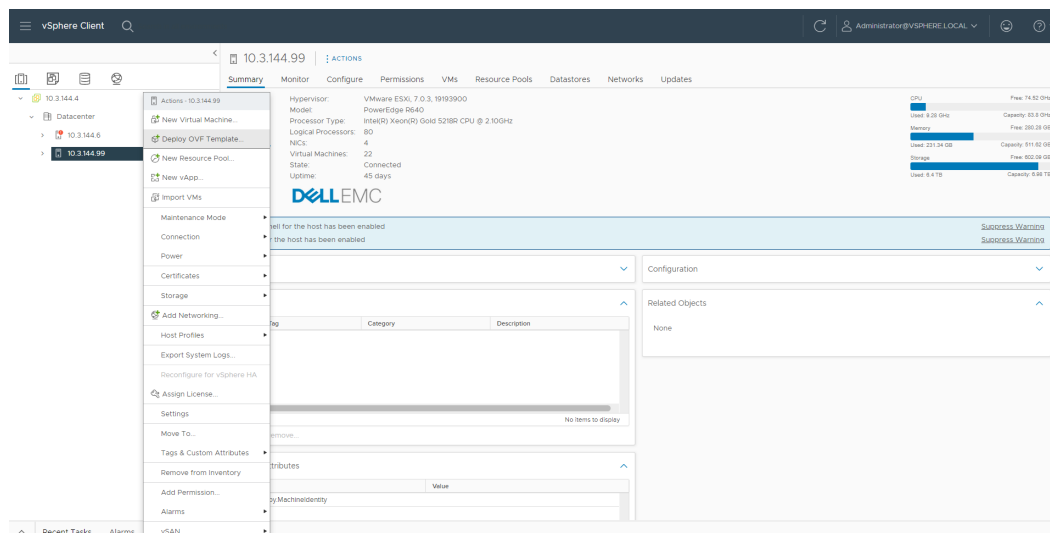
This section includes the following topics:

- [Deploying the OVF file](#)
- [Configuring hardware settings](#)
- [Powering on the VM](#)

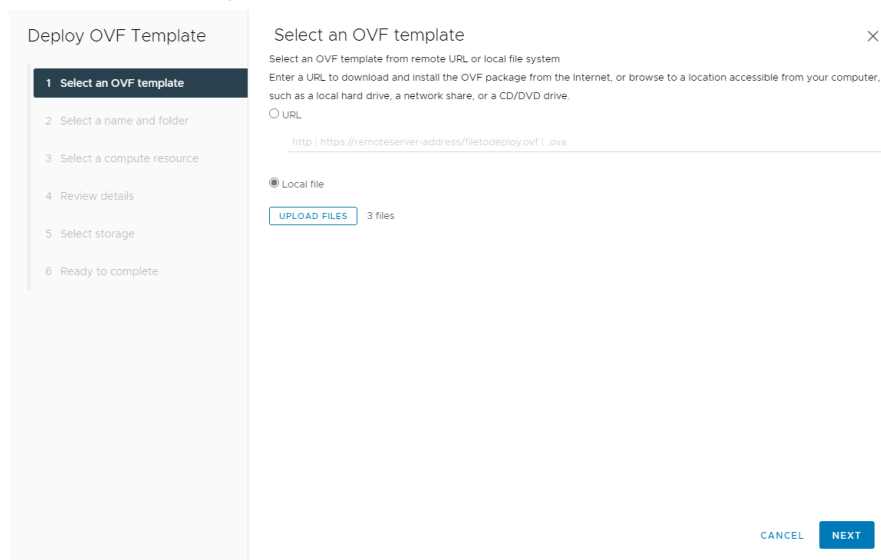
Deploying the OVF file

To deploy the OVF file template:

1. Log in to vSphere Client web console.
2. In the sidebar tree, right-click the intended physical host.



3. From the shortcut menu, select *Deploy OVF Template*....
The *Deploy OVF Template* wizard displays.
4. Using the *Deploy OVF Template* wizard, configure the FortiManager-VM:
 - a. Select an OVF Template.



- i. Select the *Local file* radio button.
- ii. Click *Browse* and select all OVF related files.

iii. Click *NEXT*.



Alternatively, you can upload the OVF from a remote server. In this case, select the *URL* radio button and enter the URL of the OVF file.

Make sure all necessary files from the deployment package are in the same path. See "Deployment package for VMware ESXi" on page 8.

b. Select a name and folder.

The screenshot shows the 'Deploy OVF Template' wizard with step 2, 'Select a name and folder', highlighted. The left sidebar lists steps 1 through 6. The main panel has a title 'Select a name and folder' and a subtitle 'Specify a unique name and target location'. The 'Virtual machine name:' field contains 'FortiAnalyzer-VM64'. Below, a tree view shows a folder structure with 'Datacenter' selected. At the bottom are 'CANCEL', 'BACK', and 'NEXT' buttons.

i. In the *Virtual machine name* field, enter a name for the VM.

The name can contain up to 80 characters and must be unique within the inventory folder.

ii. From the tree menu, select the location for the VM.

iii. Click *NEXT*.

c. Select a compute resource.

The screenshot shows the 'Deploy OVF Template' wizard with step 3, 'Select a compute resource', highlighted. The left sidebar lists steps 1 through 6. The main panel has a title 'Select a compute resource' and a subtitle 'Select the destination compute resource for this operation'. A tree view shows a folder structure with '10.3.144.99' selected. Below the tree, a 'Compatibility' section shows a green checkmark and the text 'Compatibility checks succeeded.' At the bottom are 'CANCEL', 'BACK', and 'NEXT' buttons.

i. From the tree menu, select the physical machine.

ii. Click *NEXT*.

d. Review details.

The screenshot shows the 'Deploy OVF Template' wizard with the 'Review details' step selected. The wizard has a sidebar with steps 1 through 8. The main area displays the details of the selected OVF template.

Review details	
Verify the template details.	
Publisher	No certificate present
Description	FortiAnalyzer Virtual Appliance by Fortinet Technologies Inc. (http://www.fortinet.com)
Download size	325.7 MB
Size on disk	Unknown (thin provisioned) 504.0 GB (thick provisioned)

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT.

i. After reviewing the OVF details, click **NEXT**.

e. License agreements.

The screenshot shows the 'Deploy OVF Template' wizard with the 'License agreements' step selected. The wizard has a sidebar with steps 1 through 8. The main area displays the end-user license agreement text.

License agreements

The end-user license agreement must be accepted.
Read and accept the terms for the license agreement.

End User License Agreement for FortiAnalyzer Virtual Appliance

NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT ACCEPT THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT YOU

☒ I accept all license agreements.

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT.

i. After reviewing the license agreements, select the checkbox for *I accept all license agreements*.

ii. Click **NEXT**.

f. Select storage.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage**
- Select networks
- Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

☐ Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Cluster	Size
data	---	6.98 TB	14.87 TB	602.09 GB	VMFS 6		

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

i. From the *Select virtual disk format* dropdown, select one of the following:

- *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
- *Thick Provision Eager Zeroed*: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
- *Thin Provision*: Allocates the disk space only when a write occurs to a block, but the Virtual Machine File System (VMFS) reports the total volume size to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Once a Thin Provisioned block is allocated, it remains in the volume regardless of whether you have deleted data.



If you know your environment will expand in the future, adding hard disks larger than the FortiManager base license requirement and utilizing Thin Provision when setting the OVF Template disk format is recommended. This allows your environment to expand as required while not taking up more space in the SAN than needed.

- From the menu, select the data storage location.
- Click *NEXT*.

g. Select networks.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks**
- Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
Network 1	VM Network ▾
Network 2	VM Network ▾
Network 3	VM Network ▾
Network 4	VM Network ▾

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

i. Map the networks used in this OVF template to networks in your inventory.

Network 1 maps to port1 of the FortiManager. You must set the destination network for this entry to access the device console.

ii. Click *NEXT*.

h. Ready to complete.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Ready to complete**

Ready to complete

✓ **Select a name and folder**

Name	FortiAnalyzer-VM64
Template name	FortiAnalyzer-VM64
Folder	Datacenter

✓ **Select a compute resource**

Resource	10.3.144.99
----------	-------------

✓ **Review details**

Download size	325.7 MB
---------------	----------

✓ **Select storage**

Size on disk	504.0 GB
Storage mapping	1
All disks	Datastore: data; Format: Thick provision lazy zeroed

✓ **Select networks**

Network mapping	4
Network 1	VM Network
Network 2	VM Network
Network 3	VM Network
Network 4	VM Network

IP allocation settings

CANCEL BACK FINISH

i. After verifying the information, click *FINISH* to start the deployment.

You may need to configure the FortiManager hardware settings before powering on the VM. See "Configuring hardware settings" below.

Configuring hardware settings

Before powering on your FortiManager-VM, you must configure the virtual memory, virtual CPU, and virtual disk.

To configure hardware settings:

1. In the vSphere Client, select the VM from the tree menu in the left pane.
2. In the VM Hardware pane, click *Edit Settings....*

The *Edit Settings* dialog displays.

Device	Value	Unit	Options
CPU	4		Info icon
Memory	8	GB	
Hard disk 1	4,004,882,8125	GB	
Hard disk 2	500	GB	
SCSI controller 0	VMware Paravirtual		
Network adapter 1	VM Network		<input checked="" type="checkbox"/> Connect...
Network adapter 2	VM Network		<input checked="" type="checkbox"/> Connect...
Network adapter 3	VM Network		<input checked="" type="checkbox"/> Connect...
Network adapter 4	VM Network		<input checked="" type="checkbox"/> Connect...
Video card	Specify custom settings		
VMCI device			
Other	Additional Hardware		

3. In the *CPU* field, adjust the number of CPU cores as required.
4. In the *Memory* field, adjust the memory size as required. See "Minimum system requirements" on page 7 to determine your required memory.
5. In the *Hard disk 2* field (the log disk), adjust the size required. You should not edit *Hard disk 1*.



The FortiManager-VM allows you to add twelve virtual log disks to a deployed instance. When adding additional hard disks, use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

6. Click *OK* to apply your changes.

Powering on the VM

You can now proceed to power on your FortiManager.

- Select the FortiManager in the left pane, then click *Power on the virtual machine* in the *Getting Started* tab.
- Select the VM in the left pane, then click *Power On* in the toolbar.
- Right-click the VM in the left pane, then select *Power > Power On* from the right-click menu.

Once the VM starts, proceed with the initial configuration. See [Configuring initial settings on page 17](#).

Configuring initial settings

Before you can connect to the FortiManager-VM, you must configure basic network settings via the CLI console. Once configured, you can connect to the FortiManager GUI.

Enabling GUI access

To enable GUI access to the FortiManager, you must configure the IP address and network mask of the appropriate port on the FortiManager. The following instructions use port 1.



You can determine the appropriate by matching the network adapter's MAC address and the HWaddr that the CLI command `diagnose fmnetwork interface list` provides.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the FortiManager and access the console window. You might need to press *Enter* to see the login prompt.
2. At the FortiManager login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask.

```
config system interface
  edit port1
    set ip <IP address> <netmask>
  end
```



The port management interface should match the first network adapter and virtual switch that you have configured in the hypervisor VM settings.

4. To configure the default gateway, enter the following commands:

```
config system route
  edit 1
    set device port1
    set gateway <gateway_ipv4_address>
  end
```



The Customer Service & Support portal does not currently support IPv6 for FortiManager license validation. You must specify an IPv4 address in the support portal and the port management interface.

Connecting to the GUI and enabling a trial license

Once you have configured a port's IP address and network mask, you can connect to the GUI by using a web browser.

To connect to the GUI and enable a trial license:

1. Launch a web browser, and enter the IP address you configured for the port management interface.
2. At the login page, click the *Login with FortiCloud* button to start the process of activating your free trial license.

See also [FortiManager 6.4 Trial License Guide](#).

Upgrading to an add-on license

You must activate a trial license before you can upgrade FortiManager-VM to a purchased add-on license.

See also [FortiManager 6.4 Trial License Guide](#).

Configuring your FortiManager

Once the FortiManager license has been validated, you can configure your device.



If the amount of memory or number of CPUs is too small for the VM, or if the allocated hard drive space is less than the licensed VM storage volume, warning messages show in the GUI in the *System Resources* widget on the dashboard and in the *Notification* list.

For more information on configuring your FortiManager, see the [FortiManager Administration Guide](#).

Security Fabric connector integration with VMware vCenter

You can create SDN connectors for VMware vCentre to allow FortiGate to retrieve dynamic addresses from VMware vCenter via FortiManager.

Following is an overview of how to configure an SDN connector for VMware vCenter:

1. Create an SDN connector for VMware vCenter. See [To create SDN connectors for VMware vCenter: on page 19.](#)
2. Create a dynamic address object that references the SDN connector for VMware vCenter. See [To create dynamic addresses: on page 20.](#)
3. Create a firewall policy. See [To create firewall policies: on page 21.](#)
4. Install the changes to FortiGate. See [To install changes to FortiGate: on page 22.](#)

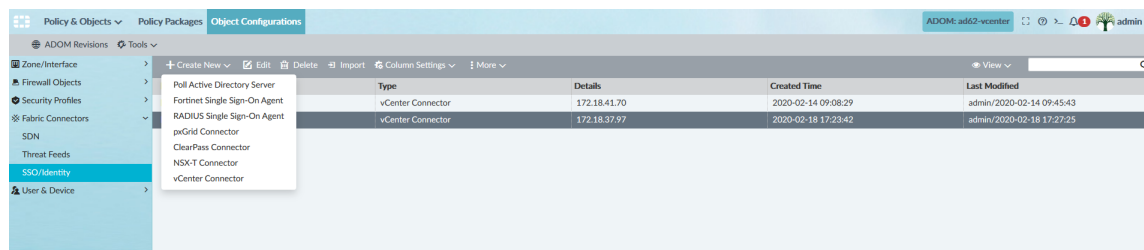
FortiGate can retrieve dynamic addresses from VMware vCenter via FortiManager.

This example assumes that VMware vCenter is already set up.

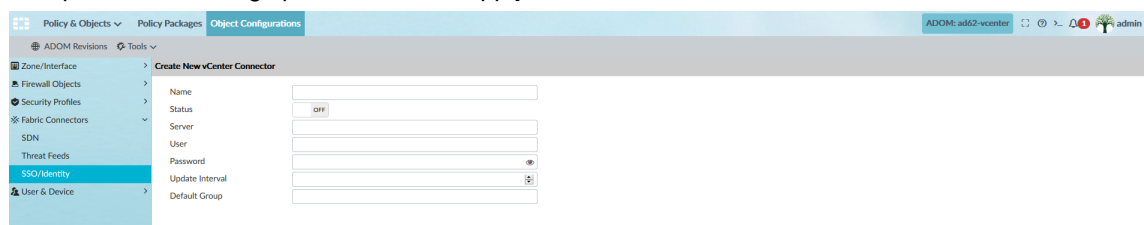
To create SDN connectors for VMware vCenter:

1. Go to *Policy & Objects > Object Configurations > Fabric Connectors > SSO/Identity*.
2. Click *Create New > vCenter Connector*.

The pane opens.



3. Complete the following options, and click *Apply & Refresh*:



The *Rule* section displays.

4. Under *Rule*, click *Create New*.

5. Complete the following options, and click **OK**.

Create New Rule

Name: FGv6

Rule:

ip	name	vmuid	vmid	ne
10.101.14.1	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	du
10.151.119.1	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	du
172.18.41.145	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	VI
fe80::250:56ff:feb1:56ce::	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	VI
fe80::344f:8997:36f2:3016::	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	du
fe80::b487:3a63:6245:e41d::	ms_tc7	503187c0-a86a-1b7a-ef05-f73092abaa56	34934	du

[Total: 6]

OK Cancel

FortiManager retrieves IP addresses from the VMware vCenter server.

Policy & Objects Policy Packages Object Configurations

ADOM Revisions Tools

Zone/Interface Firewall Objects Security Profiles Fabric Connectors SDN Threat Feeds SSO/Identity User & Device

Edit vCenter Connector

Name: fmg-stress

Status: ON

Server: 172.18.41.70

User: ellen@vsphere.local

Password: *****

Update Interval: 30

Default Group: stress1

Rule

Name	Rule
FGv6	name=FGv6*
ej-2k	name=ej_vlan*
ej-vlan124	name=ej_vlan124*
ej-vlan124-top3-001	name=ej_vlan124-top3-0001
ej-vlan128	name=ej_vlan128*

Connector Users

Search...

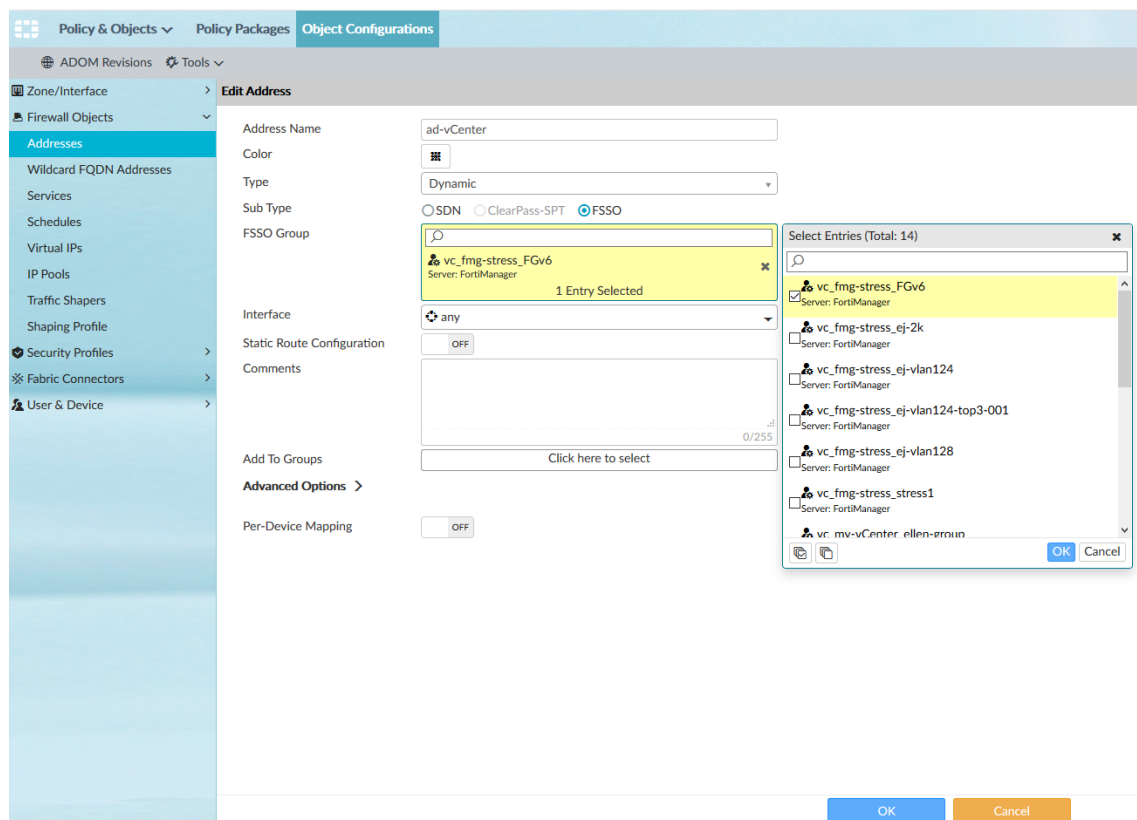
- vc_fmg-stress_FGv6 (250/250)
- vc_fmg-stress_ej-2k (1747/1747)
- vc_fmg-stress_ej-vlan124 (250/250)
- vc_fmg-stress_ej-vlan124-top3-001 (1/1)
- vc_fmg-stress_ej-vlan128 (250/250)
- vc_fmg-stress_stress1 (83/83)

Apply & Refresh OK Cancel

To create dynamic addresses:

1. Go to *Policy & Objects > Object Configurations > Firewall Objects > Addresses*.
2. Click *Create New > Address*, or double-click an existing address object to open it for editing.

3. Complete the following options, and click **OK**.
 - a. In the *Address Name* field, enter a name.
 - b. In the *Type* field, select *Dynamic*.
 - c. For *Sub Type*, select *FSSO*.
 - d. In the *FSSO Group* box, select the SDN connector that you created.
 - e. Set the remaining objects as desired.



The dynamic address is created.

To create firewall policies:

1. Go to *Policy & Objects > Policy Packages*.
2. In the tree menu, click *IPv4 Policy* under the target FortiGate.

3. Click *Create New*, or double-click an existing policy to open it for editing.

The screenshot shows the FortiGate GUI with the 'Edit IPv4 Policy' dialog box open. The dialog is titled 'Edit IPv4 Policy' and is part of the 'Policy Packages' section. The left sidebar shows the tree structure with 'FortiGate-VM_root' and 'IPv4 Policy' selected. The main area has tabs for 'Policy Package', 'Install', 'ADOM Revisions', 'Tools', 'Collapse All', and 'Object Selector'. The 'Policy Package' tab is active. The configuration fields include: Name (p1), Incoming Interface (any), Outgoing Interface (any), Source Internet Service (OFF), Source Address (all), Source User (+), Source User Group (+), FSSO Groups (+), Destination Internet Service (OFF), Destination Address (ad-vCenter), Service (ALL), Schedule (always), Action (Deny, Accept, IPSEC), Log Violation Traffic (checked), and Generate Logs when Session Starts (unchecked). There is a 'Comments' field at the bottom. At the bottom right, there are 'OK' and 'Cancel' buttons.

4. Complete the options, and click *OK*.
The policy package is created.

To install changes to FortiGate:

1. Go to *Policy & Objects > Policy Packages*.
2. In the tree menu, right-click *Installation Targets* under the target FortiGate, and select *Install Wizard*.
The *Install Wizard* dialog box opens.
3. Select *Install Policy Package & Device Settings*.

4. In the *Policy Package* list, select the policy package, and click *Next*.

Install Wizard - Policy Package and Device Setting (FortiGate-VM_root)

Please select one or more devices to install (Use checkbox or Ctrl or Shift key for multiple selections) Search...

<input checked="" type="checkbox"/>	▲ Device Name	IP Address	Platform
<input checked="" type="checkbox"/>	FortiGate-VM	10.59.8.162	FortiGate-VM64

< Back Next > Cancel

5. Complete the options, and click *Next*.

The policy package is installed.

FortiGate can retrieve dynamic addresses from VMware vCenter via FortiManager.

FortiGate VM64 FortiGate-VM

ad-vCenter resolves to:

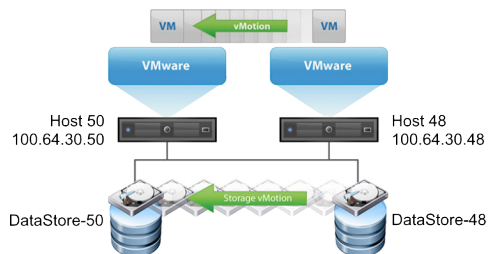
- 10.5.32.1
- 10.5.32.2
- 10.5.32.3
- 10.5.32.4
- 10.5.32.5
- 10.5.32.6
- 10.5.32.7
- 10.5.32.8
- 10.5.32.9
- 10.5.32.10
- 10.5.32.11
- 10.5.32.12
- 10.5.32.13
- 10.5.32.14
- 10.5.32.15
- 10.5.32.16
- 10.5.32.17
- 10.5.32.18
- 10.5.32.19
- 10.5.32.20
- 10.5.32.21
- 10.5.32.22
- 10.5.32.23
- 10.5.32.24
- 10.5.32.25
- 10.5.32.26
- 10.5.32.27
- 10.5.32.28
- 10.5.32.29
- 10.5.32.30
- 10.5.32.31
- 10.5.32.32
- 10.5.32.33
- 10.5.32.34
- 10.5.32.35
- 10.5.32.36
- 10.5.32.37
- 10.5.32.38
- 10.5.32.39
- 10.5.32.40
- 10.5.32.41
- 10.5.32.42
- 10.5.32.43
- 10.5.32.44

Type	Details	Interface	Visibility	Ref.
Subnet	0.0.0.0/0		Visible	0
Subnet	0.0.0.0/0		Hidden	0
IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (sslroot)	Visible	0
Dynamic (FSSO)	vc_fmgs-stress_FGv6		Visible	1
Subnet	0.0.0.0/0		Visible	1

vMotion in a VMware environment

This guide provides sample configuration of a vMotion FortiManager-VM in a VMware environment. VMware vMotion enables the live migration of a running FortiManager-VM from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. It also provides transparency to users.

The following depicts the network topology for this sample deployment. In this sample deployment, there are two hosts, Host 48 (100.64.30.48) and Host 50 (100.64.30.50), that are members of Cluster 1 in the DataCenter 1. The vCenter server (vcenter67.fmg.lab) manages DataCenter 1.

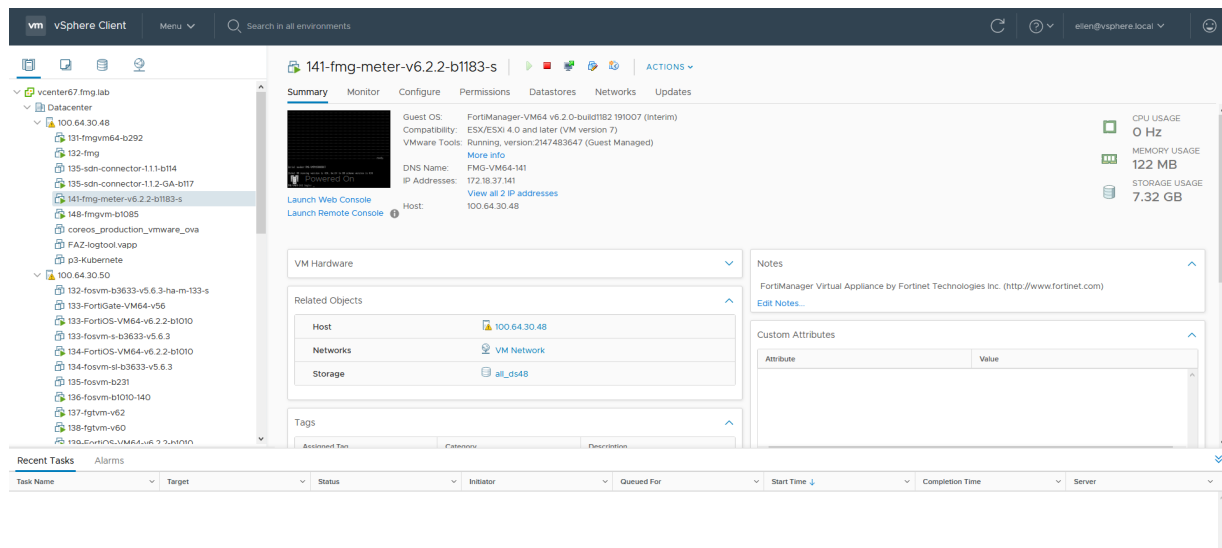


This configuration requires the following prerequisites:

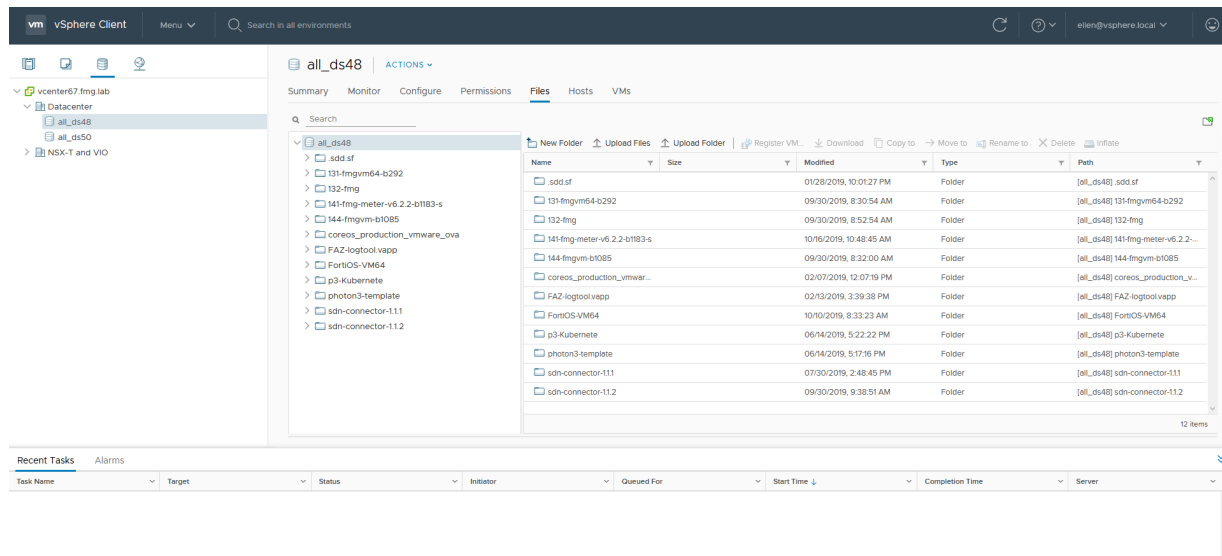
- You have set up the vCenter server and created the data center and cluster.
- Host 48 and Host 50 are members of the cluster.
- A Gigabit Ethernet network interface card with a VMkernel port enabled for vMotion exists on both ESXi hosts.
- A FortiManager-VM that is set up and able to handle traffic.

To migrate the FortiManager-VM on the vCenter web portal:

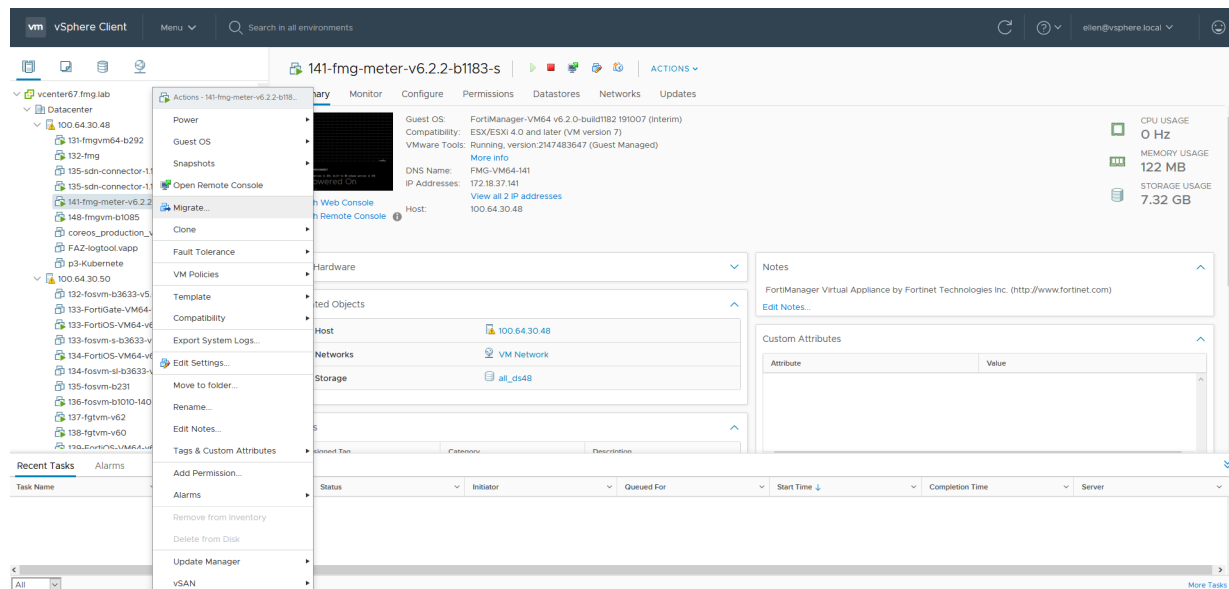
1. Log in to the vCenter web portal.
2. Verify the current location of the FortiManager-VM:
 - a. Go to the FortiManager-VM.
 - b. On the *Summary* tab, check the *Host*. In this example, the host is currently Host 48 (100.64.30.48).



- c. Go to *Storage > Files*. Check that the FortiManager-VM is located in the correct datastore. In this example, the datastore is currently Datastore 48, in Host 48.

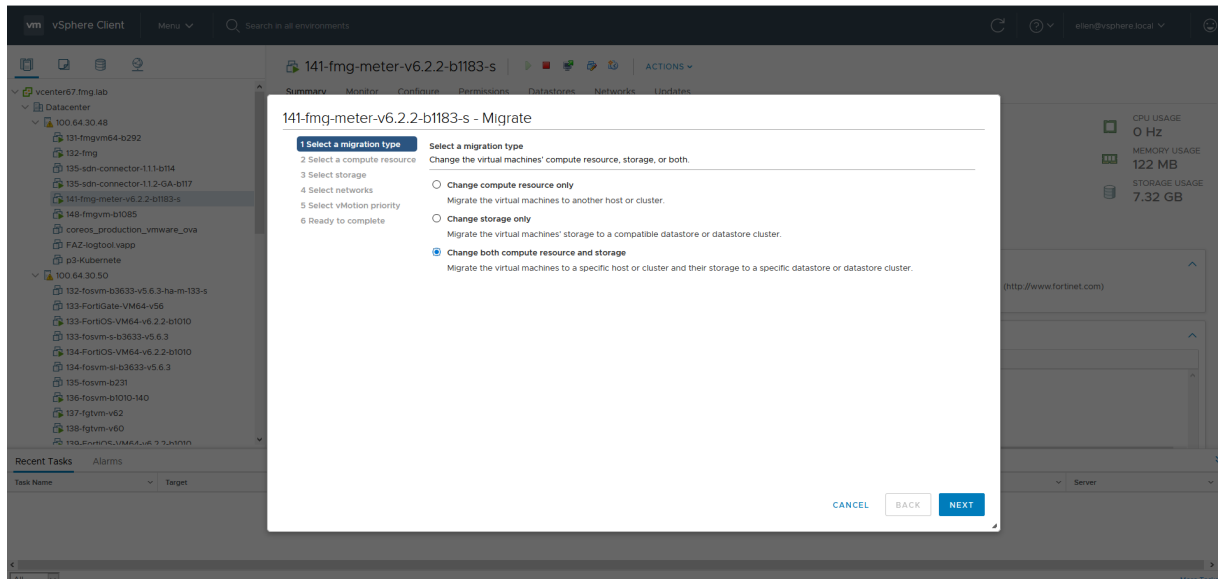


3. Right-click the FortiManager-VM and select *Migrate*.

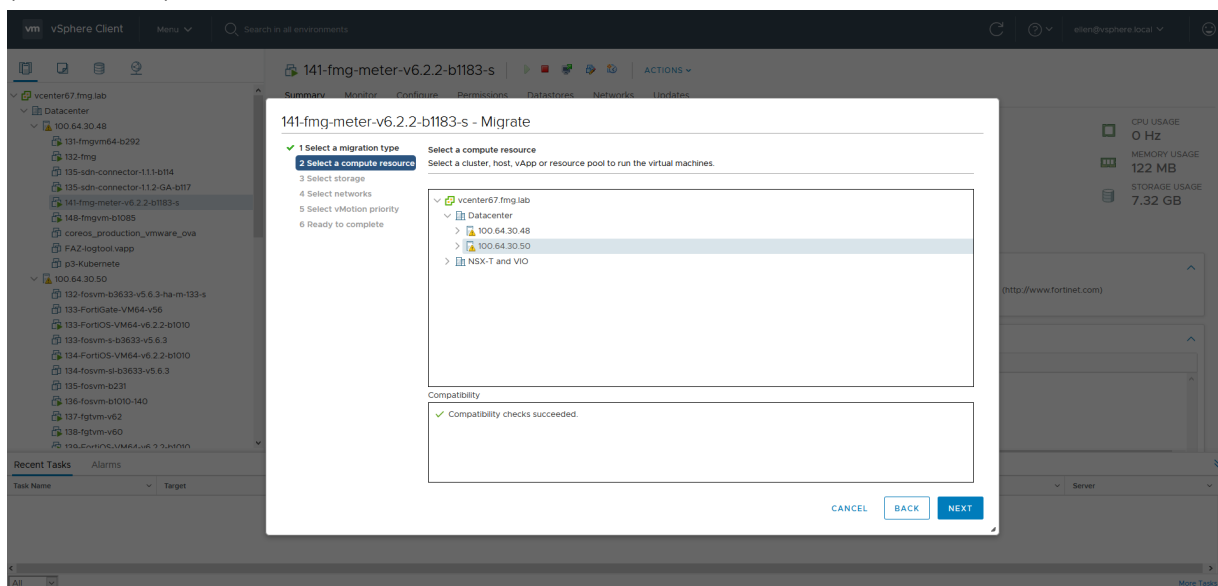


4. Configure the migration options:

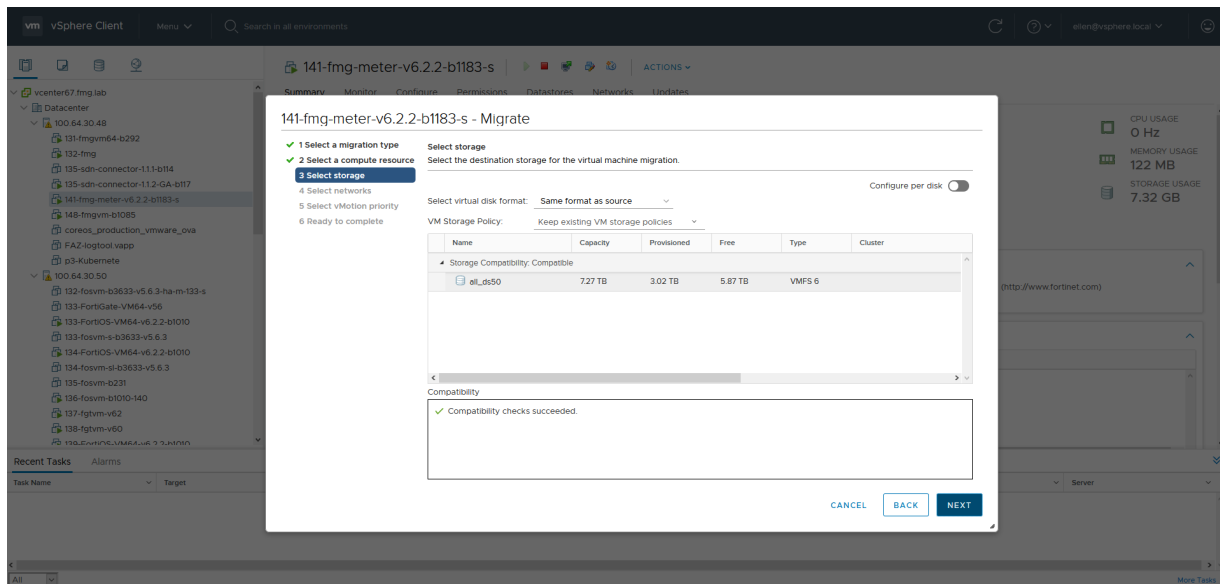
- a. For *Select a migration type*, select *Change both compute resource and storage*. Click *NEXT*.



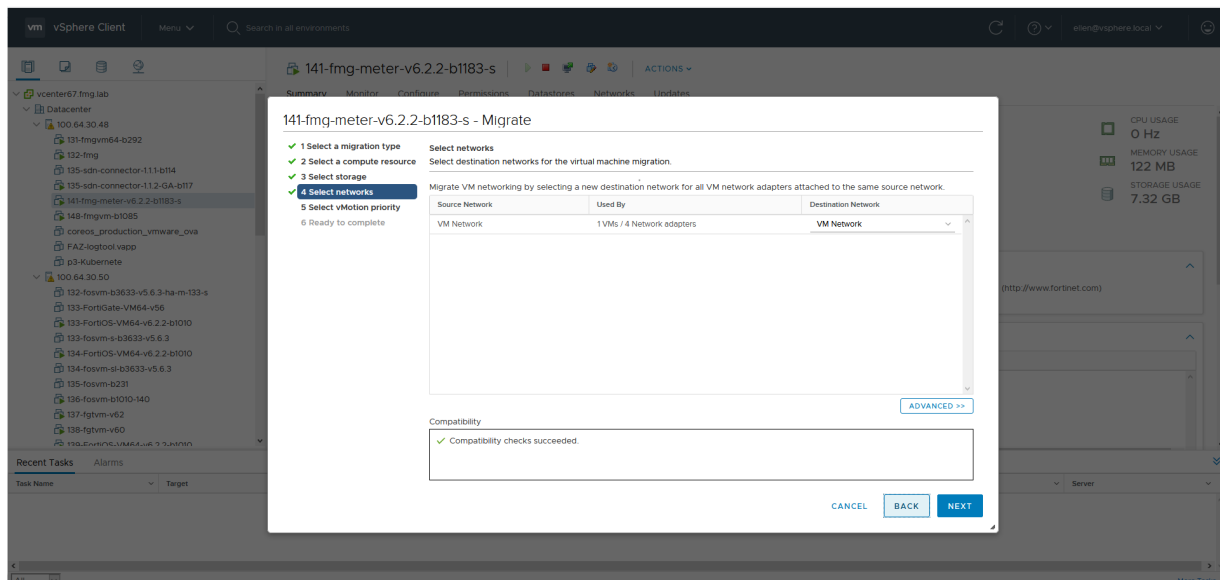
- b. For *Select a compute resource*, select the desired new compute resource. In this example, Host 50 (100.64.30.50) is selected. Click *NEXT*.



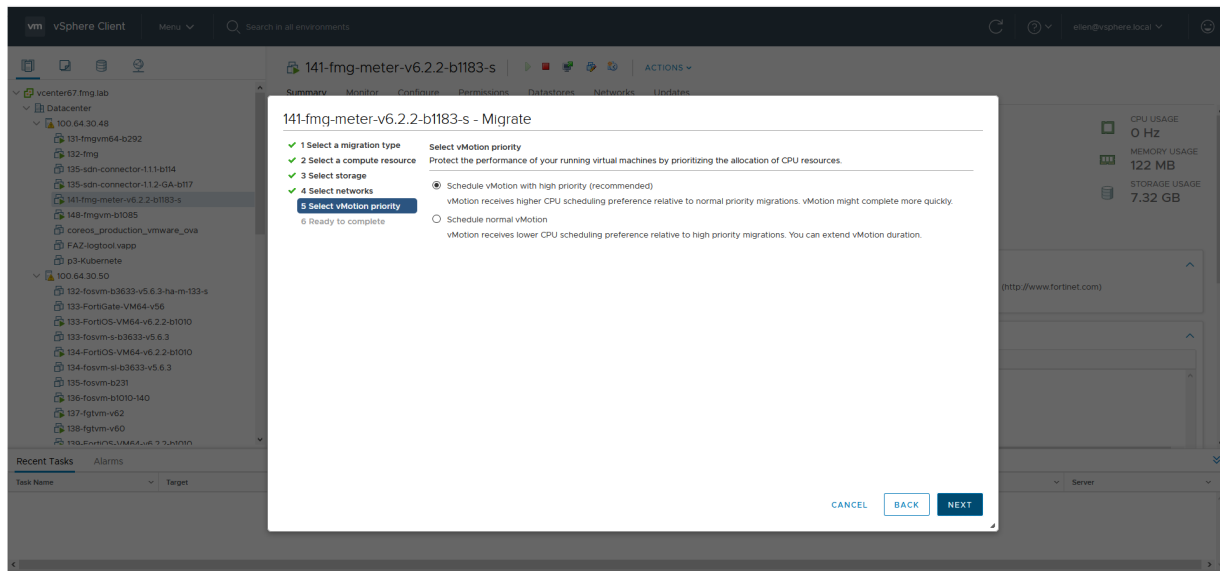
- c. For *Select storage*, select the storage associated with the selected compute resource. In this example, Datastore 50 (as corresponds to Host 50) is selected. Click *NEXT*.



- d. For **Select networks**, select the desired destination network at the selected compute resource. In this example, the source network is at Host 48, and the destination network is at Host 50. Click **NEXT**.



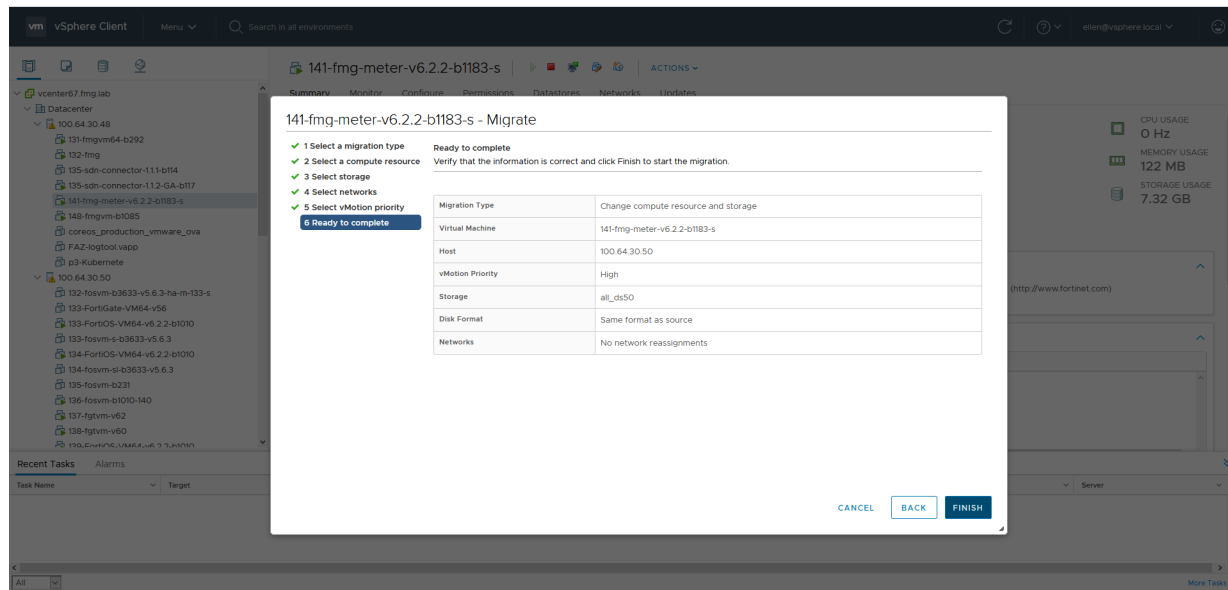
- e. For *Select vMotion priority*, select *Schedule vMotion with high priority (recommended)*. Click *NEXT*.



5. Before initiating the migration, open the CLI for the FortiManager-VM to check on traffic during the migration. Enter `diagnose sniffer packet any 'icmp and host 8.8.8.8'` to check if traffic is stable. If no traffic is lost during migration and the FortiManager-VM SSH session does not break, the output resembles the following:

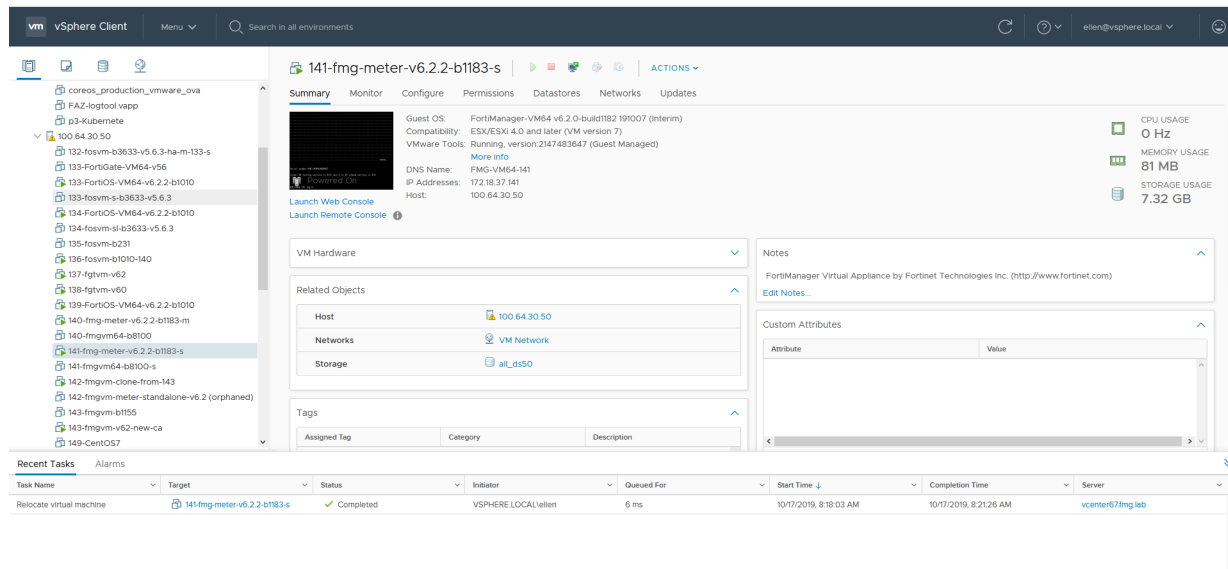
```
172.18.37.141 - PuTTY
login as: admin
FMG-VM64 # diagnose sniffer packet any 'icmp and host 8.8.8.8'
interfaces=[any]
filters=[icmp and host 8.8.8.8]
33.400203 172.18.37.141 -> 8.8.8.8: icmp: echo request
33.404667 8.8.8.8 -> 172.18.37.141: icmp: echo reply
34.404168 172.18.37.141 -> 8.8.8.8: icmp: echo request
34.408597 8.8.8.8 -> 172.18.37.141: icmp: echo reply
35.408051 172.18.37.141 -> 8.8.8.8: icmp: echo request
35.412351 8.8.8.8 -> 172.18.37.141: icmp: echo reply
36.412048 172.18.37.141 -> 8.8.8.8: icmp: echo request
36.416418 8.8.8.8 -> 172.18.37.141: icmp: echo reply
47.288064 172.18.37.141 -> 8.8.8.8: icmp: echo request
47.292522 8.8.8.8 -> 172.18.37.141: icmp: echo reply
48.292039 172.18.37.141 -> 8.8.8.8: icmp: echo request
48.296336 8.8.8.8 -> 172.18.37.141: icmp: echo reply
49.296071 172.18.37.141 -> 8.8.8.8: icmp: echo request
49.300337 8.8.8.8 -> 172.18.37.141: icmp: echo reply
50.300221 172.18.37.141 -> 8.8.8.8: icmp: echo request
50.304531 8.8.8.8 -> 172.18.37.141: icmp: echo reply
62.673839 172.18.37.141 -> 8.8.8.8: icmp: echo request
62.678341 8.8.8.8 -> 172.18.37.141: icmp: echo reply
63.676059 172.18.37.141 -> 8.8.8.8: icmp: echo request
63.680348 8.8.8.8 -> 172.18.37.141: icmp: echo reply
```

6. Click *FINISH*.



After a few seconds, the FortiManager-VM is migrated to the new compute resources, in this case Host 50.

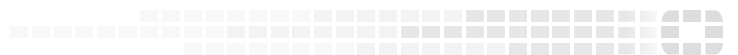
7. Log into the vCenter web portal. Go to the FortiManager-VM. On the *Summary* tab, the *Host* is now the new compute resources, in this case Host 50 (100.64.30.50).



8. Go to *Storage > Files*. It shows that the FortiManager-VM is now located in a new datastore, in this example Datastore 50.



FORTINET®



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.