



GigaVUE-FM Installation and Upgrade Guide

GigaVUE-FM

Product Version: 6.5

Document Version: 1.1

Last Updated: Thursday, October 10, 2024

(See Change Notes for document updates.)

Copyright 2024 Gigamon Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, transcribed, translated into any language, stored in a retrieval system, or transmitted in any form or any means without the written permission of Gigamon Inc.

Trademark Attributions

Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners.

Gigamon Inc.
3300 Olcott Street
Santa Clara, CA 95054
408.831.4000

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Product Version	Document Version	Date Updated	Change Notes
6.5.00	1.1	10/10/2024	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.5.00	1.0	12/11/2023	The original release of this document with 6.5.00 GA.

Contents

GigaVUE-FM Installation and Upgrade Guide	1
Change Notes	3
Contents	4
About this Guide	8
Minimum Requirements	8
Installing GigaVUE-FM on VMware ESXi	10
Before You Install	10
Prerequisites for GigaVUE-FM	10
VMware ESXi Hardware Requirements	10
Recommended Resource Requirements for Scaled Environments	11
Rules, Notes, and Limitations	13
Reference Values for Disk Space Estimation	13
Install GigaVUE-FM using OVA file on VMware vCenter	14
Install GigaVUE-FM using ISO Image File on VMware ESXi Host	25
Install GigaVUE-FM using ISO Image File on VMware vCenter	26
Initial GigaVUE-FM Configuration	27
Perform Initial Configuration	27
Redeploy GigaVUE-FM Instance (with VMs Already Deployed)	30
Installing GigaVUE-FM on AWS	31
Before You Install	31
Subscribe to GigaVUE Products	31
Initial GigaVUE-FM Configuration	32
Installing GigaVUE-FM on Azure	32
Before You Install	33
Install GigaVUE-FM on Azure	33
Install GigaVUE-FM Using Azure VM Dashboard	33
Install GigaVUE-FM Using Azure Market Place	33
Install and Upgrade GigaVUE-FM	35
Cloud	35
On-premise	35
Installing GigaVUE-FM on GCP	35
Before You Install	35
Prerequisites for GigaVUE-FM	36
Install GigaVUE-FM on GCP	36

Installing GigaVUE-FM on OpenStack	37
Before You Install	37
Install GigaVUE-FM on OpenStack	38
Initial GigaVUE-FM Configuration	40
Installing GigaVUE-FM on Nutanix	40
Before You Install	41
Install GigaVUE-FM on Nutanix	41
Installing GigaVUE-FM on MS Hyper-V	43
Before You Install	43
Windows Server Hardware Requirements	43
Install GigaVUE-FM for Microsoft Hyper-V	44
Install GigaVUE-FM from an ISO Image File	44
Add Additional Virtual Hard Disk and Install GigaVUE-FM	48
Connect and Power On the GigaVUE-FM Virtual Machine	51
Disconnect the ISO Image File	53
Initial GigaVUE-FM Configuration	53
Installing GigaVUE-FM on KVM	56
Before You Install	56
Limitations	56
System Requirements	56
Install GigaVUE-FM for KVM	57
Install GigaVUE-FM from an ISO Image File	57
Initial GigaVUE-FM Configuration	64
Upgrade GigaVUE-FM	66
Important GigaVUE-FM Upgrade Guidance	67
Supported Upgrade Paths for GigaVUE-FM	68
Upgrade GigaVUE-FM from the GigaVUE-FM CLI	69
Upgrade GigaVUE-FM from the UI	71
Upgrade from External Image Server	72
Upgrade with GigaVUE-FM as the Image Server	73
Post-Upgrade Notes	75
Upgrade GigaVUE-FM in Azure	76
Upgrade Options in Azure	77
Upgrade GigaVUE-FM from the UI	77
Upgrade from External Image Server	77
Upgrade with GigaVUE-FM as the Image Server	79
Upgrade GigaVUE-FM using Snapshot in Azure	80
Upgrade the GigaVUE-FM using the Snapshot method	81
Stop GigaVUE-FM Instance	81
Create Snapshot of the GigaVUE-FM Instance	81
Upgrade GigaVUE-FM Instance	82

Upgrade GigaVUE-FM in AWS	83
Upgrade Options in AWS	83
Upgrade GigaVUE-FM from the UI	83
Upgrade from External Image Server	84
Upgrade with GigaVUE-FM as the Image Server	85
Upgrade GigaVUE-FM using Snapshot in AWS	87
At a Glance	87
Stop GigaVUE-FM Instance	88
Create Snapshot of the GigaVUE-FM Instance	88
Upgrade GigaVUE-FM Instance	89
Upgrade GigaVUE Fabric Components	90
Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS	91
Prerequisite	91
Upgrade UCT-V Controller	91
Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy	92
Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure	95
Prerequisite	95
Upgrade UCT-V Controller	95
Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy	97
Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack	100
Prerequisite	101
Upgrade UCT-V Controller	101
Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy	103
Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi	105
Upgrade GigaVUE V Series Node for VMware NSX-T	110
Upgrade GigaVUE V Series Nodes Deployed using GigaVUE-FM	110
Upgrade GigaVUE V Series Node Deployed using VMware NSX-T Manager	111
GigaVUE-FM Administrator Authentication by Platform	112
Initial Credentials for GigaVUE-FM Credentials	112
Logging in to GigaVUE-FM Command Line Interface	114
Post Installation Configurations	114
Install Custom Certificate	114
Pre-requisites	115
Steps	115
Install Rabbit MQ Certificate	116
Syslog and AFI Monitoring Stats Collection	117
Communication between GigaVUE-FM Load Balancer and Web Server	117
Configure rSyslog Server for Receiving TLS/SSL Packets	118
Reference	127
Setting the GigaVUE-FM Admin Password	127

GigaVUE-FM CLI Commands	129
fmctl	129
Additional Sources of Information	138
Documentation	138
How to Download Software and Release Notes from My Gigamon	140
Documentation Feedback	141
Contact Technical Support	142
Contact Sales	142
Premium Support	143
The VUE Community	143
Glossary	144

About this Guide

This guide describes how to install and upgrade the GigaVUE-FM[®] Fabric Manager (GigaVUE-FM).

Installation

- [Installing GigaVUE-FM on VMware ESXi](#)
- [Installing GigaVUE-FM on AWS](#)
- [Installing GigaVUE-FM on Azure](#)
- [Installing GigaVUE-FM on GCP](#)
- [Installing GigaVUE-FM on OpenStack](#)
- [Installing GigaVUE-FM on Nutanix](#)
- [Installing GigaVUE-FM on MS Hyper-V](#)
- [Installing GigaVUE-FM on KVM](#)

Upgrade

- [Important GigaVUE-FM Upgrade Guidance](#)
- [Upgrade GigaVUE-FM](#)
- [Upgrade GigaVUE-FM in Azure](#)
- [Upgrade GigaVUE-FM in AWS](#)

Reference

- [GigaVUE-FM CLI Commands](#)
- [Setting the GigaVUE-FM Admin Password](#)

Minimum Requirements

This section lists the minimum virtual computing resources required for installing GigaVUE-FM¹.

Table 1: Minimum Virtual Computing Requirements for Installing GigaVUE-FM

Minimum Virtual Computing Requirements	
Memory	Minimum 16GB memory
Virtual CPU (vCPU)	2 vCPU

¹GigaVUE-FM software version 6.5.00 runs on Rocky Linux 8.8 (as CentOS is End of Life).

Minimum Virtual Computing Requirements	
Virtual Storage for Guest	80GB <ul style="list-style-type: none">• System Disk - 40GB• Data Disk - 40GB
Virtual Network Interfaces	One vNIC

Installing GigaVUE-FM on VMware ESXi

GigaVUE-FM can be installed on VMware ESXi host and VMware vCenter using OVA file or ISO Image. This section describes how to install GigaVUE-FM on VMware hypervisor, ESXi. It consists of the following main sections:

- [Before You Install](#)
- [Install GigaVUE-FM using OVA file on VMware vCenter](#)
- [Install GigaVUE-FM using ISO Image File on VMware ESXi Host](#)
- [Install GigaVUE-FM using ISO Image File on VMware vCenter](#)
- [Initial GigaVUE-FM Configuration](#) describes the steps to start GigaVUE-FM instance and configure it.
- [Redeploy GigaVUE-FM Instance \(with VMs Already Deployed\)](#) describes how to remove an existing instance and redeploy it.

Before You Install

This section describes the hardware and virtual computing requirements for GigaVUE-FM. Ensure that the time on the VMware ESXi host is set correctly to ensure accuracy of the trending data that is captured.

Prerequisites for GigaVUE-FM

Before Installing GigaVUE-FM, ensure that VMware vSphere Standard, Enterprise, or Enterprise Plus is installed on hardware that meets minimum requirements. Refer [VMware ESXi and NSX-V Hardware Requirements](#) for minimum hardware requirements.

VMware ESXi Hardware Requirements

The following table describes the hardware requirements on which VMware ESXi runs GigaVUE-FM.

Table 1: Hardware Requirements for VMware Hypervisor

Hardware Requirements	
VMware Hypervisor	vSphere ESXi: v7.xx and above. Refer to Supported Hypervisors for VMware for more detailed information.
CPU	One or more 64-bit x86 CPUs with virtualization

Hardware Requirements	
	assist (Intel-VT or AMD-V) enabled. Note: To run GigaVUE-FM, hardware support for virtualization must be enabled on the VMware ESXi host. Make sure that the BIOS option for virtualization support is not disabled. For more information, see your BIOS documentation
RAM	At least 16GB
Disk Space	At least 84GB shared (FC, iSCSI, NFS, or FCoE) or locally attached storage (PATA, SATA, SCSI) OS Requirement: 40GB Data Requirement: 40GB Additional Swap Space: 4GB <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> NOTE: Increase the disk space depending on the configuration load requirements for the given GigaVUE-FM instance. </div>
Network	At least one 1Gb NIC

Recommended Resource Requirements for Scaled Environments

Refer to the following sections for large deployment scenarios of GigaVUE-FM.

For Standalone GigaVUE-FM

The following table displays the minimum recommended requirements for a standalone GigaVUE-FM:

Configuration	Basic Configuration	Medium Configuration	Large Configuration	Large Configuration (GigaVUE-FM Hardware Appliance 2)
CPU				
CPU count(minimum)	2	4	12	32
CPU Min speed (per CPU)	2.30GHz	2.30GHz	2.30GHz	2.10GHz
Memory				
Memory Size	16GB	32GB	128GB	128GB
Disk Space				
OS Disk Size	40GB	40GB	40GB	40GB
Config Disk Size - 15 Days Data	80GB	620GB	1100GB	1100GB
Config Disk Size - 35 Days Data	160GB	1240GB	2200GB	2200GB

Configuration	Basic Configuration	Medium Configuration	Large Configuration	Large Configuration (GigaVUE-FM Hardware Appliance 2)
Config Disk Size - Rollup 35 Days + 120 Days Rollup	200GB	1600GB	2500GB	2500GB
** The disk usage is estimated based on the configuration load defined in the table below (Reference Values for Disk Space Estimation). You must periodically monitor the disk utilization and increase the disk size on need.				
NIC				
Number of NICs	1	1	1	1
Management/Data	1GB	1GB	1GB	1GB
Appliance Scalability				
Number of GigaVUE HC Series/GigaVUE TA Series Devices	Up to 50	Up to 500	Up to 1000	Up to 1000
Number of GigaVUE V Series Nodes	Up to 50	Up to 500	Up to 1000	Up to 1000

For GigaVUE-FM High Availability Instances

The following table displays the minimum recommended requirements for GigaVUE-FM High Availability group:

Configuration	Basic Configuration	Medium Configuration	Large Configuration	Large Configuration (GigaVUE-FM Hardware Appliance 2)
CPU				
CPU count(minimum)	2	4	12	32
CPU Min speed (per CPU)	2.30GHz	2.30GHz	2.30GHz	2.10GHz
Memory				
Memory Size	16GB	32GB	128GB	128GB
Disk Space				
OS Disk Size	40GB	40GB	40GB	40GB
Config Disk Size - 15 Days Data	80GB	620GB	1600GB	1100GB
Config Disk Size - 35 Days Data	160GB	1240GB	3000GB	3000GB
Config Disk Size - Rollup 35 Days + 120 Days Rollup	200GB	1600GB	4300GB	4300GB
** The disk usage is estimated based on the configuration load defined in the table below (Reference Values for Disk Space Estimation). You must periodically monitor the disk utilization and increase the disk size on				

Configuration	Basic Configuration	Medium Configuration	Large Configuration	Large Configuration (GigaVUE-FM Hardware Appliance 2)
need.				
NIC				
Number of NICs	1	1	1	1
Management/Data	1GB	1GB	1GB	1GB
Appliance Scalability				
Number of GigaVUE HC Series/GigaVUE TA Series Devices	Up to 50	Up to 500	Up to 3020	Up to 3020

Rules, Notes, and Limitations

- When deploying GigaVUE-FM in VMware ESXi, use the 'reservation' option and allocate fixed resource for CPU and memory.
- Values may change depending on the hardware used. You must ensure that the hardware you use supports the data rate specified in the table.
- Syslogs must be disabled if more than 1000 nodes are configured in GigaVUE-FM.
- Config sync time for 3000 node system on an average takes 10 minutes and on a maximum can go up to 12 minutes.

Reference Values for Disk Space Estimation

The following table defines the load in system for various system configurations that is used for qualification. Use this as a reference to estimate the disk usage and I/O operation in the system.

	Default (Basic)	Medium	Large	GigaVUE-FM High Availability Large 3000 Nodes
Devices	50	500	1000	3020
Ports	4550	45500	91000	273000
Maps	380	4750	13300	39900
Rules	1900	23750	66500	199500
GigaSMART Operations	250	1250	3500	10500
GigaSMART Groups	40	500	1400	4200
Virtual Ports	250	1250	3500	10500
Syslog Rate (per minute)	40	500	1400	4200
SNMP Traps Rate (per minute)	80	1000	2800	7200

Install GigaVUE-FM using OVA file on VMware vCenter

The GigaVUE-FM software package is distributed as an OVA file.

Use the vSphere Client to install the GigaVUE-FM OVA file. Starting from software version 5.3, you cannot deploy GigaVUE-FM directly from the ESXi host. You must login to the vCenter on the vSphere client to deploy a GigaVUE-FM instance.

IMPORTANT NOTE:



- The OVA file must be stored in a location that is accessible to the vSphere Client. This location cannot be a datastore accessible to the ESXi host which will be the target of the deployment.
- GigaVUE-FM v5.8 is used for illustration purposes only throughout this example. In your deployment, select the version that you are deploying.

The following the steps given below to deploy a GigaVUE-FM instance:

1. Log in to the VMware vCenter web interface.
2. In the vSphere Client, select an inventory object that is a valid parent object of a virtual machine such as data center, cluster, or ESXi host.
3. Right-click the ESXi Host, Cluster, or data center on which you want to deploy GigaVUE-FM 6.5, and then select **Deploy OVF Template**.

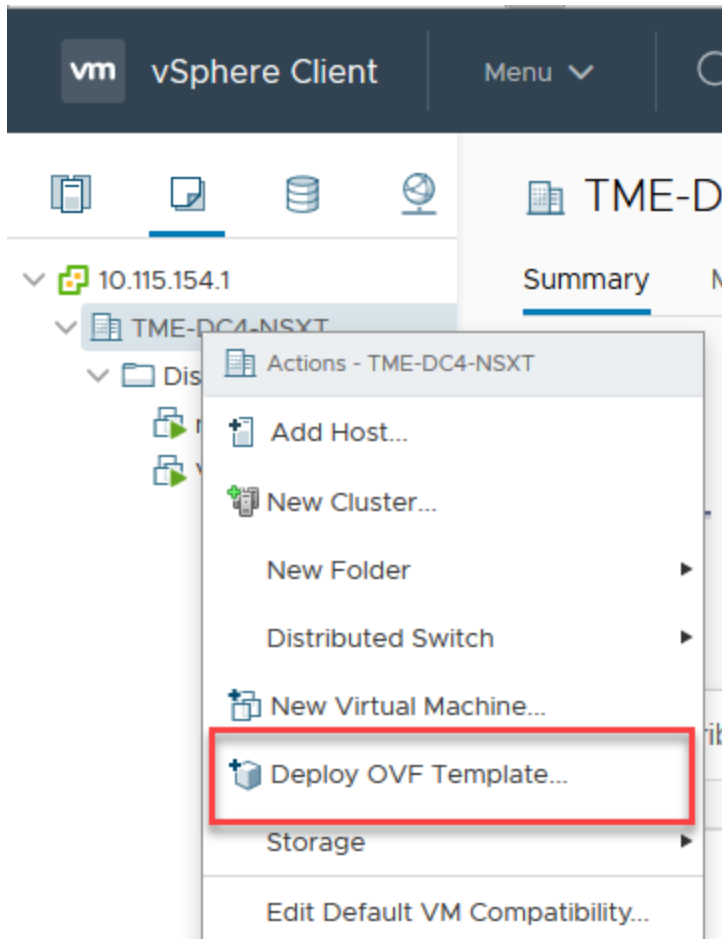


Figure 1 vSphere Client: OVF Template
The Deploy OVF Template wizard opens.

The screenshot shows the 'Deploy OVF Template' wizard in the vSphere Client. The title is 'Deploy OVF Template'. On the left, there is a progress indicator with six steps: 1. Select an OVF template (highlighted in blue), 2. Select a name and folder, 3. Select a compute resource, 4. Review details, 5. Select storage, and 6. Ready to complete. The main content area is titled 'Select an OVF template' and contains the instruction 'Select an OVF template from remote URL or local file system'. Below this, there is a text box with the placeholder text 'Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.' There are two radio button options: 'URL' (which is selected) and 'Local file'. Under the 'URL' option, there is a text input field containing the example URL 'http | https://remoteserver-address/filetodeploy.ovf | .ova'. Under the 'Local file' option, there is a 'Browse...' button and the text 'No files selected.'. At the bottom right of the wizard, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

Figure 2 vSphere Client: Find the Location of the OVA File

4. In the **Select an OVF template** page of the **Deploy OVF Template** wizard, choose one of the following options:
 - a. **URL**—Enter the URL from where you want to download and install the OVF package.
 - b. **Local file**—Click **Browse** to navigate to the OVA file available on your local machine, and then select the OVA file.
5. Click the **Next**. The **Select a name and folder** page of the **Deploy OVF Template** wizard appears.

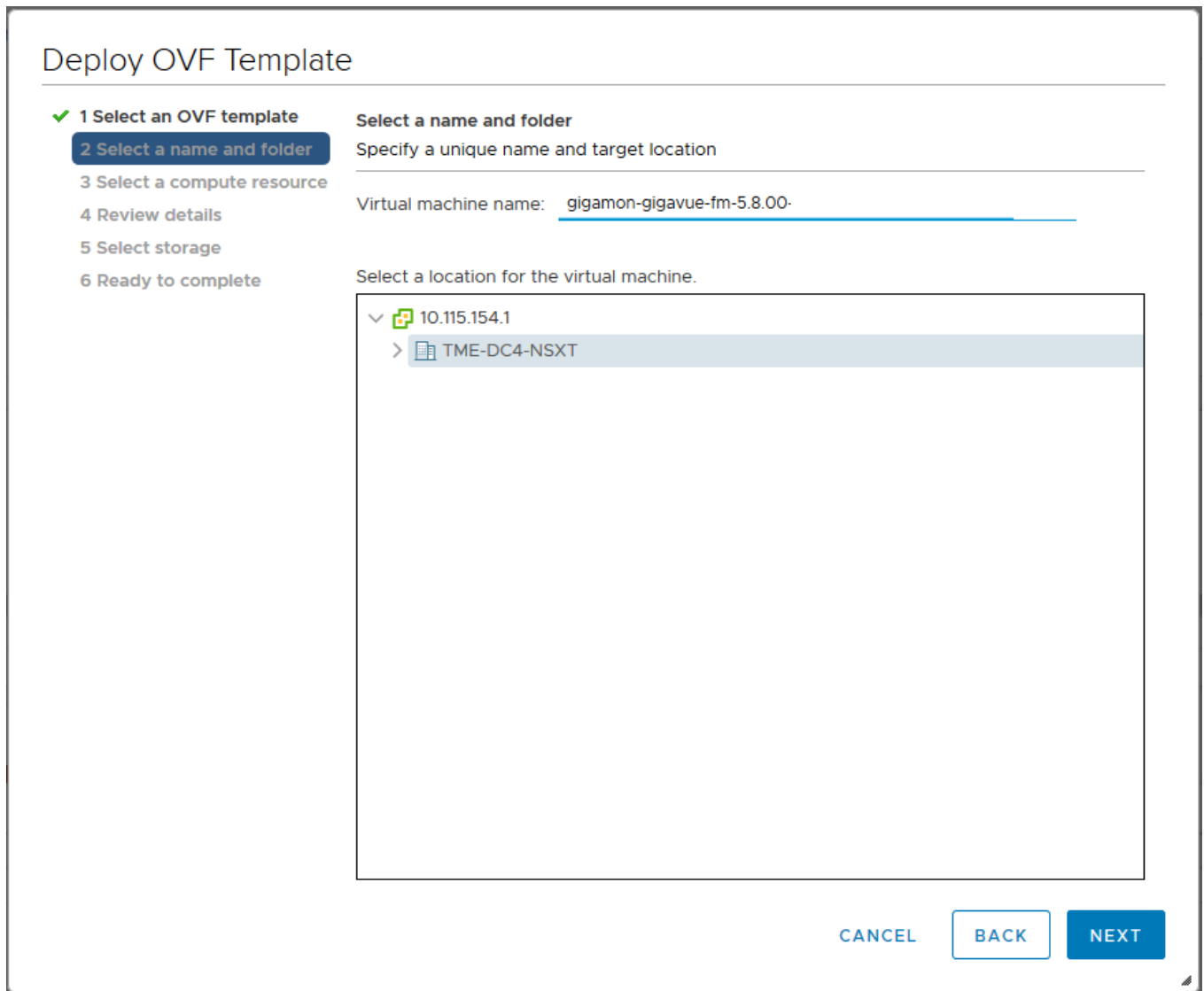


Figure 3 vSphere Client: Enter Name and Location for OVA File on ESXi Server

6. Specify a unique name for the GigaVUE-FM instance, and then select a location and host to which you want to deploy the GigaVUE-FM instance.
7. Click **Next**. The **Select a compute resource** page of the **Deploy OVF Template** wizard appears.

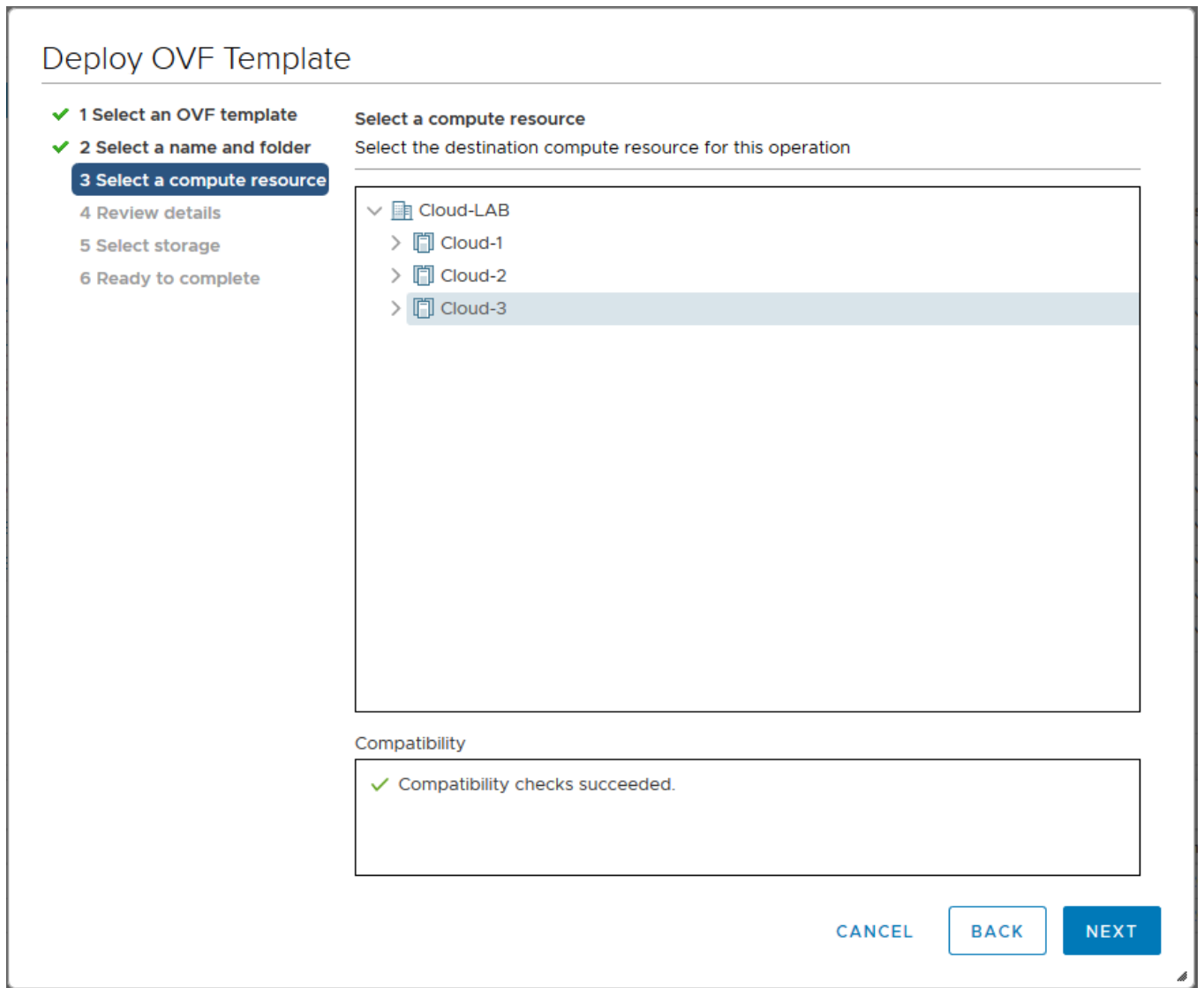


Figure 4 vSphere Client: Select a Compute Resource for the OVF Deployment

8. Select a destination compute host for the OVF deployment. The Deploy OVF Template wizard performs a validation to ensure that the selected host has all the resources required for the GigaVUE-FM deployment.
9. Click **Next**. The **Review details** page of the **Deploy OVF Template** wizard appears.

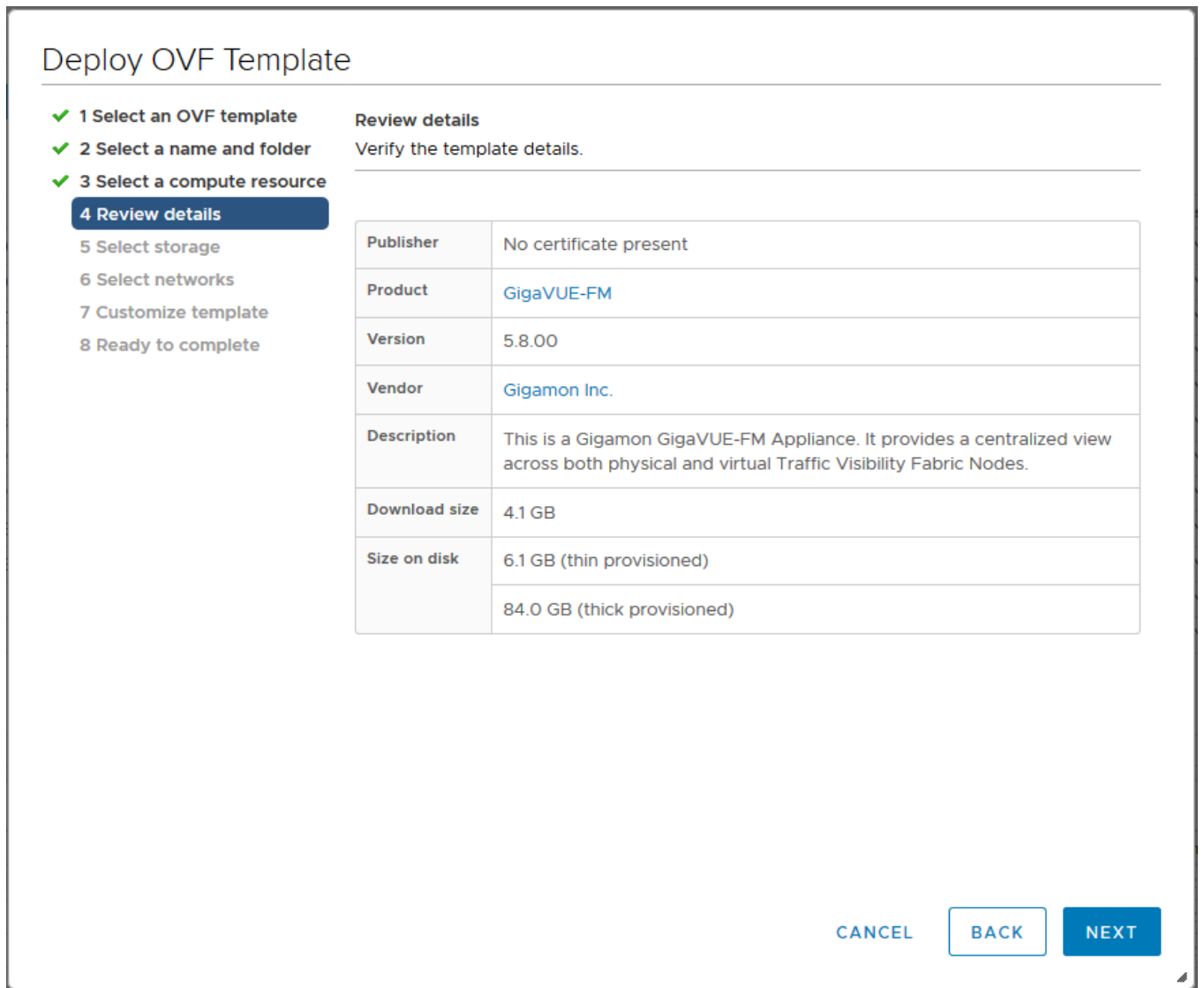


Figure 5 vSphere Client: Review Details

10. Verify the OVF template details, and then click **Next**. The **Select storage** page of the **Deploy OVF Template** wizard appears.

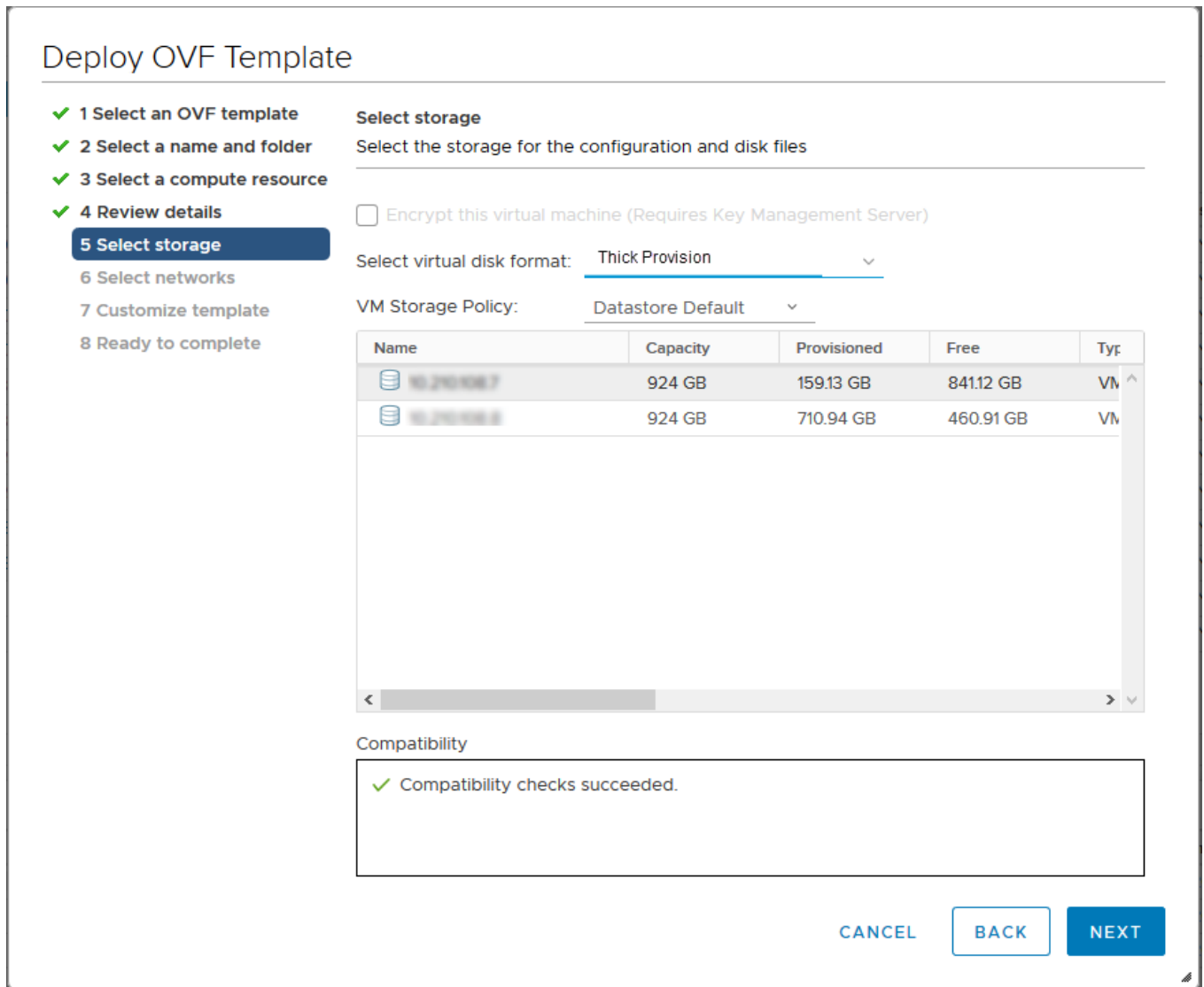


Figure 6 vSphere Client: Select Storage

- From the **Select virtual disk format** drop-down list, select **Thick Provisioning** as the format for the virtual disks and provisioning.

NOTE: You must deploy GigaVUE-FM using **Thick Provisioning**. Any other choice results in GigaVUE-FM not working correctly.

- Select the datastore where the virtual machine's files will be stored.
- Click **Next**. The **Select networks** page of the **Deploy OVF Template** wizard appears.

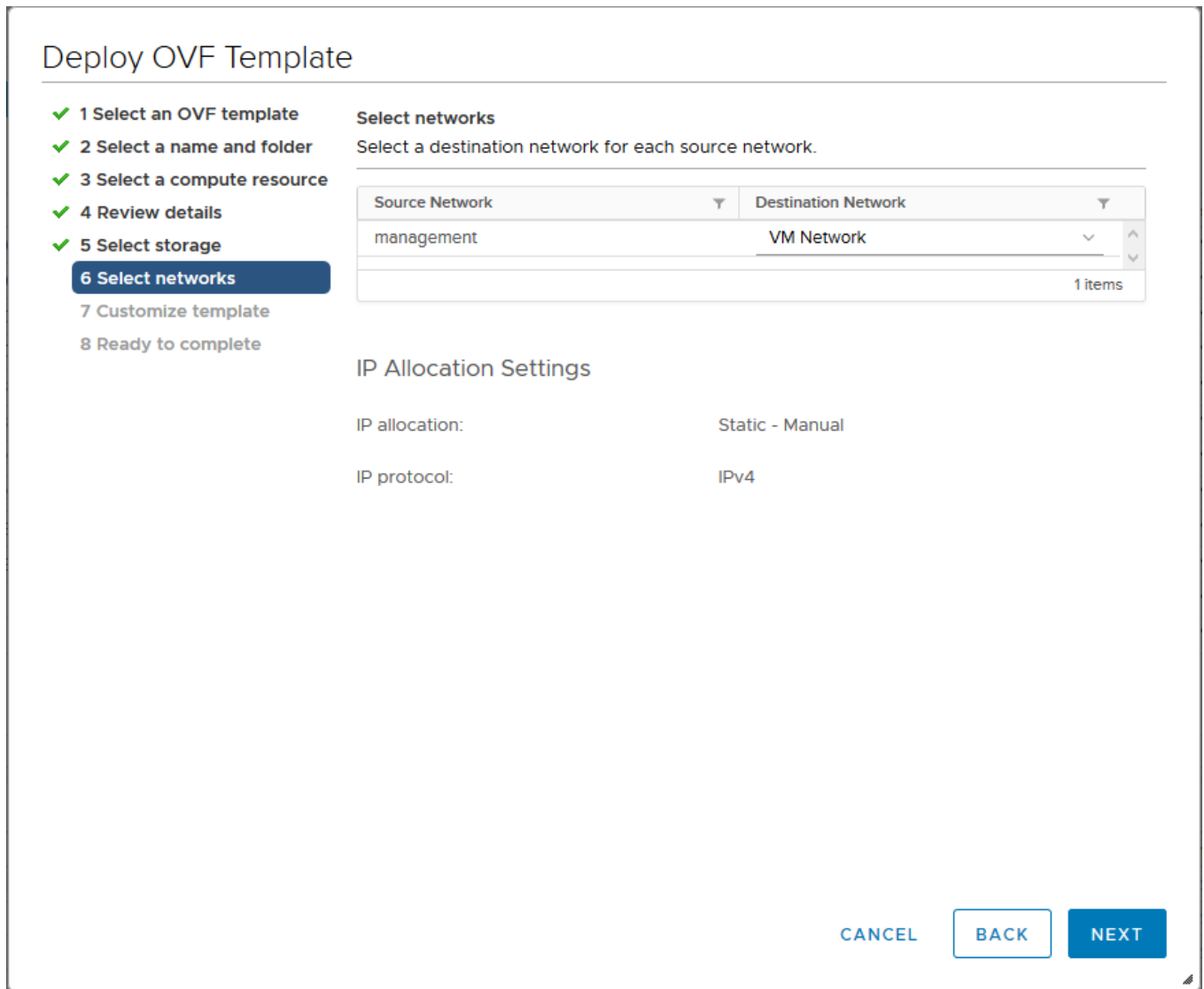


Figure 7 vSphere Client: Select Networks

14. Set network mapping by doing either of the following, depending on how you are deploying, and then click **Next**:
 - **If you are not deploying on a standalone ESXi host**, the **Network Mapping** displays under **Source Networks**. Use the drop-down lists to assign the correct **Destination Network** to the source network.
 - **If you are deploying GigaVUE-FM on a standalone ESXi host**, the network mapping is set automatically by assigning the destination network to the any destination Network. In case of multiple port groups, you need to manually assign the destination network to the any destination network VM Network.

15. Click **Next**. The **Customize template** page of the **Deploy OVF Template** wizard appears.
16. In the **System Hostname** field, enter the hostname of the GigaVUE-FM instance, and then specify **40** GB as the size of the data disk.
17. Set the admin password. When setting the admin password using GigaVUE-FM UI, then the password must be a minimum of 11 characters and a maximum of 30 characters. The characters must include at least:
 - o One numerical character
 - o One upper case character
 - o One lower case character
 - o One special character

NOTE: The password that you set here is applicable only to the GigaVUE-FM Shell. To access the GigaVUE-FM UI, the default username is admin and password is admin123A!!. You can change the password when you first login to the GigaVUE-FM UI.

If the password does not meet the complexity requirements:

- o The system displays an error message in the GigaVUE-FM UI.
 - o The parameters configured above are not passed on to the GigaVUE-FM except the host name parameter.
 - o The static IP addresses that were configured originally will be unavailable after GigaVUE-FM is deployed.
18. (Optional) Complete the IP Networking configurations such as the default gateway for the management port, IP address of the DNS server, and the domain name for this GigaVUE-FM instance.
 19. (Optional) Complete the NTP configurations such as the IP address and version of the NTP server, and then click **Next**.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- 7 Customize template**
- 8 Ready to complete

Customize template
Customize the deployment properties of this software solution.

✓ All properties have valid values
✕

Basic Configuration	4 settings
01. System Hostname	A Unique hostname for this instance. <input style="width: 80%;" type="text" value="GigaVUE-FM-5800"/>
02. Size of Data Disk	The size of the Data Disk in gigabytes. <input style="width: 80%;" type="text" value="40"/>
03. Optional admin password	If set, the default admin password will be set to this value to allow password based login. The password will be good for only a single login. You MUST specify either a password or an SSH Public Key, otherwise you will NOT be able to access your GigaVUE-FM instance. <div style="display: flex; justify-content: space-between;"> <div style="width: 60%;">Password</div> <input style="width: 30%; border: 1px solid #ccc;" type="text"/> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;">Confirm Password</div> <input style="width: 30%; border: 1px solid #ccc;" type="text"/> </div>

CANCEL
BACK
NEXT

Figure 8 vSphere Client: Customize Template

NOTE: You can also choose to perform the IP Networking and NTP configurations by running the **fmctl jump-start** command after you power on the GigaVUE-FM instance at the successful completion of the OVF template deployment. For details, refer to [Perform Network Configurations](#)

The **Ready to Complete** page of the **Deploy OVF Template** wizard appears.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- ✓ 7 Customize template
- 8 Ready to complete

Ready to complete
Click Finish to start creation.

Provisioning type	Deploy OVF From Remote URL
Name	gigamon-gigavue-fm-5.8.00
Template name	gigamon-gigavue-fm-5.8.00
Download size	4.1 GB
Size on disk	6.1 GB
Folder	Workload
Resource	Cloud-2
Storage mapping	1
All disks	Datastore: 10.210.108.7; Format: Thick Provision
Network mapping	1
management	VM Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

CANCEL
BACK
FINISH

Figure 9 vSphere Client: Final Verification Before Installation

20. Verify that all of the settings are correct, and then click **Finish**. The Recent Tasks pane of the vSphere Client Home page shows the progress of the deployment operation.

Recent Tasks		Alarms	
Task Name	Target	Status	Details
Deploy OVF template	gigamon-gigavue-fm...	<div style="width: 5%; height: 10px; background-color: #0056b3;"></div> 5%	✕
Import OVF package	Cloud-2	<div style="width: 7%; height: 10px; background-color: #0056b3;"></div> 7%	✕

Figure 10 vSphere Client: OVF Deployment Progress

When the operation completes, you have successfully deployed a GigaVUE-FM instance.

Important: Clear the browser cache before logging in to GigaVUE-FM.

Install GigaVUE-FM using ISO Image File on VMware ESXi Host

You can install GigaVUE-FM on VMware ESXi host using the ISO image file. Follow the steps given below to install GigaVUE-FM using ISO image on ESXi host:

1. Log in to the VMware ESXi host web interface.
2. Upload the ISO image to the data store. Refer to [Upload Files to Datastores](#) section in the VMware Documentation for detailed information.
3. After uploading the ISO image file, right-click a host in the VMware Host Client inventory and select **Create/Register VM**. The New Virtual Machine wizard opens.
4. In the **Select creation type** tab, select **Create a new virtual machine**. Then, click **Next**.
5. In the **Select a name and guest OS** tab,
 - a. Enter a name for the virtual machine.
 - b. Select the **Guest OS family** as Linux.
 - c. Select the **Guest OS version** as Rocky Linux 8.8 (64-bit).
 - d. Then, click **Next**.
6. In the Customize settings tab, enter the CPU, Memory and Hard disk details. Refer to Minimum Requirements for more detailed information on minimum requirements required to install GigaVUE-FM.
 - a. Click on **Add Hard disk** button to add two virtual disks to this VM. Each virtual disk must have a capacity of at least 40 GiB.
 - b. Select a **Network Adapter**.
 - c. In the **CD/DVD Drive**, select **Datastore ISO file** and the **CD/DVD Media** select the ISO image uploaded in Step 2. Ensure that the Connect check box for both **Network Adapter** and **CD/DVD Drive** is enabled.
 - d. Then, click **Next**.
7. Click **Finish**. Then, power on the virtual machine for the image to boot up.

NOTE: If you install GigaVUE-FM on ESXi version 8 host, change the boot option from EFI (default boot option) to BIOS before the first power on, as GigaVUE-FM supports only BIOS boot option.

8. When the operation is complete, you have successfully deployed a GigaVUE-FM instance.

Install GigaVUE-FM using ISO Image File on VMware vCenter

You can install GigaVUE-FM on VMware vCenter using the ISO image file. Follow the steps given below to install GigaVUE-FM using ISO image on vCenter:

1. Log in to the VMware vCenter web interface.
2. In the vSphere Client, select an inventory object that is a valid parent object of a virtual machine such as data center, cluster, or ESXi host.
3. Right-click the ESXi Host, Cluster, or data center on which you want to deploy GigaVUE-FM6.5, and then select **Files** in the top navigation bar. Then click on **Upload Files** and then upload the ISO image file.
4. Click on the **Actions** button on the top and select **New Virtual Machine**. The New Virtual Machine wizard opens.
5. In the **Select a creation type** tab, select **Create a new virtual machine**. Then, click **Next**.
6. In the **Select a name and folder** tab, specify a unique name for the GigaVUE-FM instance, and then select a location and host to which you want to deploy the GigaVUE-FM instance.
7. Click **Next**. The **Select a compute resource** page of the **New Virtual Machine** wizard appears.
8. Select a destination compute host for the virtual machine deployment. The New Virtual Machine wizard performs a validation to ensure that the selected host has all the resources required for the GigaVUE-FM deployment.
9. Click **Next**. The **Select storage** page of the **New Virtual Machine** wizard appears. Select the datastore where the virtual machine's files will be stored. Then, Click **Next**.
10. The **Select compatibility** page of the **New Virtual Machine** wizard appears. Select compatibility for this virtual machine depending on the ESXi hosts used in your environment. Then, Click **Next**.
11. The **Select a guest OS** page of the **New Virtual Machine** wizard appears.
 - a. Select the **Guest OS family** as Linux.
 - b. Select the **Guest OS version** as Rocky Linux 8.8 (64-bit).
 - c. Then, click **Next**.

NOTE: GuestOS version is displayed as RockyLinux only if the vSphere version is either 6.7 U3p or 7.0 U3c. For other versions of vSphere, CentOS 4/5 is only displayed. Use the drop-down to select RockyLinux.

12. The **Customize hardware** page of the **New Virtual Machine** wizard appears, enter the CPU, Memory and Hard disk details. Refer to Minimum Requirements for more detailed information on the minimum requirements required to install GigaVUE-FM.
 - a. Go to **Add New Device > Hard disk** to more than one hard disk. Add a secondary hard disk with at least 40GB memory. In the **Disk Provisioning**, select **Thick Provision** or **Thin Provision**.
 - b. Select a **Network Adapter**.
 - c. In the **CD/DVD Drive**, select **Datastore ISO file** and the **CD/DVD Media** select the ISO image uploaded in Step 3.
 - d. Click Next.
13. The **Ready to Complete** page of the **New Virtual Machine** wizard appears.
14. Verify that all of the settings are correct, and then click **Finish**. The Recent Tasks pane of the vSphere Client Home page shows the progress of the deployment operation.
15. When the operation is complete, you have successfully deployed a GigaVUE-FM instance.

Important: Clear the browser cache before logging in to GigaVUE-FM.

Initial GigaVUE-FM Configuration

After you have deployed a new GigaVUE-FM instance, you can choose to perform some initial configuration before you start using GigaVUE-FM. This procedure only needs to be performed once for each GigaVUE-FM instance deployed.

NOTE: Use care when Shutting Down or Rebooting a GigaVUE-FM. **Never** directly Power-Off the virtual machine. In VMware ESXi environment when using vSphere client, ALWAYS use **Shut Down Guest OS** or **Restart Guest** functions from VMware. Access is available from either the FILE menu or from the appropriate buttons on the GigaVUE-FM console. Failure to follow these steps may lead to database corruption issues.

Perform Initial Configuration

Before powering on GigaVUE-FM, you can optionally perform the following:

- [Perform Network Configurations](#)
- [Add Additional vNIC, vCPUs, and Increase Memory](#)

Perform Network Configurations

To perform the initial configuration:

1. Log in to GigaVUE-FM using one of the following methods:
 - If you have a static IP address set up for the GigaVUE-FM, log in through SSH.

- o If you do not have a static IP address set up for the GigaVUE-FM, complete the following steps:
 - a. Log in to the VMware vCenter web interface.
 - b. Go to **Menu > VMs and Templates**.
 - c. Right-click the GigaVUE-FM virtual machine, and select **Open Remote Console**.
 - d. Log in with your GigaVUE-FM Shell credentials.
- 2. Perform the following steps to complete the initial configuration:
 - a. Run the **fmctl jump-start** command. The Initial System Configuration screen appears as shown in the following figure:

Initial System Configuration

Hostname	unconfigured-gigavue-fm		
Domain Name			
Enable DHCP4	yes	Enable DHCP6	yes
IPv4 Address		IPv6 Address	
CIDR		CIDR	
Gateway		Gateway	
DNS Servers			
Search Domains			
Enable NTP	no	NTP Servers	0.centos.pool.ntp.org 1.centos.pool.ntp.org
		NTP Version	4

< **OK** > <Cancel>

- b. Provide a unique hostname for GigaVUE-FM. Note that the hostname may contain letters, numbers, periods (.), and hyphens (-), but may not begin with a hyphen. No other special characters are permitted.

- c. Enter the required domain name.
- d. Decide whether to use DHCP for the management interface. Choose one of the following options:
 - If you enter **yes**, the **IPv4 Address** or **IPv6 Address, CIDR, Gateway, DNS Servers**, and **Search Domains** are dynamically set up for the management interface.
 - If you enter **no**, you must provide the following:
 - i. **IPv4 Address** or **IPv6 Address**, and the respective **CIDR** and **Gateway**.
 - ii. In the **DNS Servers** field, provide the address of any additional name servers required. Enter the set of IP addresses with spaces in between.
 - iii. In the **Search Domains** field, provide the required DNS domains with spaces in between.
- e. You can choose to either enable or disable NTP. In the **Enable NTP** field, enter one of the following:
 - **Yes**—Use NTP to synchronize the time between GigaVUE-FM virtual machine and the NTP server. In the **NTP Servers** and **NTP Version** fields, enter the NTP server address and the version number of the NTP server.
 - **No**—you can skip the next step and directly save your configurations.
- f. Select **OK** to save your configurations.
- g. Reboot your GigaVUE-FM virtual machine.

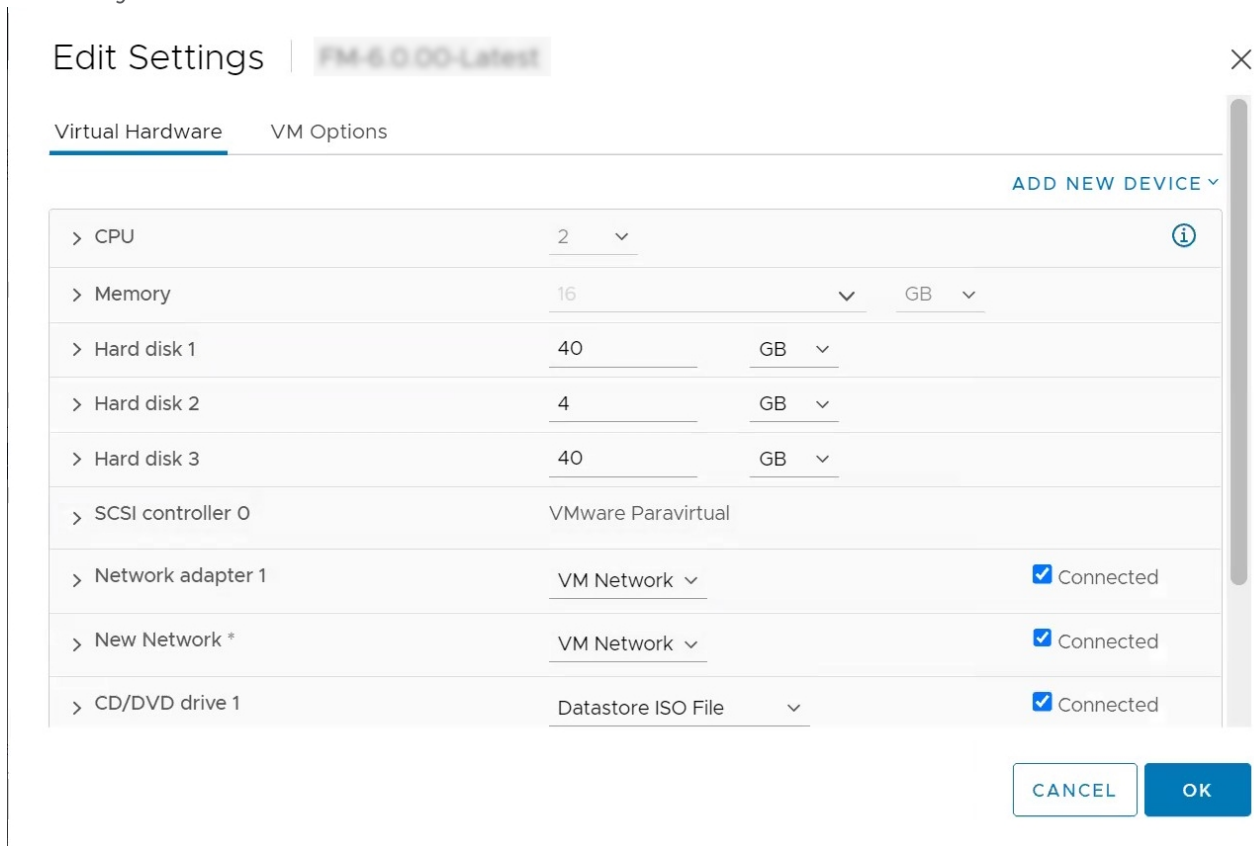
You can now access GigaVUE-FM by opening a browser and entering its IP address (the IP address you specified).

Add Additional vNIC, vCPUs, and Increase Memory

Gigamon allows you to configure GigaVUE-FM with two network interfaces—eth0 and eth1. The network interface eth0 can be configured to connect to a network used to manage Gigamon devices. The other network interface eth1 can be configured to connect to a network hosting different servers like SMTP server, Archive server, and so on.

Follow the steps given below to add Additional vNIC, vCPUs, and increase memory:

1. Right-click the GigaVUE-FM instance and select **Edit Settings...** . The **Edit Settings** dialog box opens.
2. Click on the **Virtual Hardware** tab, edit the memory and CPU details to increase the memory and add vCPUs.



3. Click on the Add New Device drop-down in the top right corner.
4. Select Network Adapter under Network. A New device (additional vNIC) is added to GigaVUE-FM.

Redeploy GigaVUE-FM Instance (with VMs Already Deployed)

If there is a need to remove an existing instance of GigaVUE-FM and reinstall it, delete all the virtual centers configured in the Virtual > Management > Virtual Center tab prior to deleting the GigaVUE-FM. To re-install GigaVUE-FM, refer to the [Install GigaVUE-FM using OVA file on VMware vCenter](#) or [Install GigaVUE-FM for Microsoft Hyper-V](#).

Installing GigaVUE-FM on AWS

This section describes how to install GigaVUE-FM on AWS. It consists of the following sections:

- [Before You Install](#) describes the pre-requisites and the preparatory steps required for installing GigaVUE-FM.
- [Subscribe to GigaVUE Products](#) describes the steps to deploy GigaVUE-FM on AWS.
- [Initial GigaVUE-FM Configuration](#) describes the steps to start GigaVUE-FM instance and configure it

Before You Install

Before installing GigaVUE-FM on AWS environment refer to Prerequisites topic in the *GigaVUE Cloud Suite Deployment Guide - AWS* for detailed instructions on the basic requirements required for installing GigaVUE-FM on AWS.

Subscribe to GigaVUE Products

You can deploy the GigaVUE Cloud Suite for AWS from the AWS Marketplace. The following GigaVUE Cloud Suite products are listed in the AWS Marketplace:

- GigaVUE V Series Node
- GigaVUE V Series Controller
- GigaVUE-FM
- UCT-V Controller

To subscribe to the GigaVUE products, perform the following steps:

1. Login to your AWS account.
2. Go to <https://aws.amazon.com/marketplace/>.
3. In the **Search** field, type Gigamon and click Search.
4. In the "Pricing model" section, filter the list by checking the box next to "Bring Your Own License"
5. Select the latest version GigaVUE Cloud Suite BYOL version. For more information on Licensing, refer to [Licensing GigaVUE Cloud Suite](#) .
6. Click **Continue to Subscribe**. The Terms and Conditions page is displayed.
7. Review the Terms and Conditions and then click "**Accept Terms**".
8. Review the summary and then click "**Continue to Configuration**".

9. In the "**Configure this software**" page, enter the following details for your deployment and click "**Continue to Launch**":
 - a. **Fulfillment Option:** <Leave Default>
 - b. **Software Version:** <Leave Default>
 - c. **Region:** <Select your specific Region>
10. In the Configure this software page, select the following:
 - a. **Choose Action:** <Launch from Website>
 - b. **EC2 Instance Type:** <select desired size>.
 - c. **VPC Settings:** <Indicate your desired VPC>
 - d. **Subnet Settings:** <Indicate your desired Subnet>
 - e. **Security Group Settings:** <Indicate your security group settings>
 - f. **Key Pair:** <Indicate your desired key>
 - g. Click Launch.

After subscribing and deploying the GigaVUE-FM, you must change the default username and password. For more information, see [Initial GigaVUE-FM Configuration](#).

Initial GigaVUE-FM Configuration

It may take several minutes for the GigaVUE-FM instance to initialize. After the initialization is completed, you can verify the instance through the web interface as follows:

1. In your EC2 Instances page, select the launched GigaVUE-FM instance and expand the page in the **Descriptions** tab to view the instance information.
2. Copy and paste the Public IP address into a new browser window or tab.
3. Copy the Instance ID from the **Descriptions** tab.

If GigaVUE-FM is deployed inside AWS, use **admin** as the username and the **Instance ID** as the default password for the admin user to login to GigaVUE-FM, for example i-079173111e2d73753 (**Instance ID**).

Use **admin** as the default username to login to the instance using the AWS CLI.

After logging into GigaVUE-FM, you are prompted to change the default password.

Installing GigaVUE-FM on Azure

This section describes how to install GigaVUE-FM on Azure. It consists of the following sections:

- [Before You Begin](#) describes the pre-requisites and the preparatory steps required for installing GigaVUE-FM.
- [Install GigaVUE-FM on Azure](#) describes the steps to install and deploy GigaVUE-FM on Azure.

Before You Install

You must create an account and configure a VNet as per your requirements. Refer to *Before You Begin* topic in the *GigaVUE Cloud Suite Deployment Guide - Azure* for detailed instructions.

Install GigaVUE-FM on Azure

The GigaVUE-FM can be launched from the Azure VM dashboard or Azure Marketplace.

Install GigaVUE-FM Using Azure VM Dashboard

Go to **Azure VM Dashboard > Virtual Machines**, click **Create** to create an Azure Virtual Machine. Refer to [Create a Linux virtual machine in the Azure](#) topics in Azure Documentation for more information. Enter the details as mentioned in [Table 1: GigaVUE-FM Installation Steps](#).

Install GigaVUE-FM Using Azure Market Place

Go to Azure Market Place, search for Gigamon. The latest version of Gigamon GigaVUE Cloud Suite for Azure appears. Open the latest version of GigaVUE-FM. Review and accept the terms for Gigamon GigaVUE Cloud Suite for Azure. Refer to [Enable Subscription for GigaVUE Cloud Suite for Azure](#) for more detailed information on how to enable the subscription and accept the terms of use. Refer to [Create a Linux virtual machine in the Azure](#) topics in Azure Documentation for more information. Enter the details as mentioned in [Table 1: GigaVUE-FM Installation Steps](#).

The following table describes the important fields.

Table 1: GigaVUE-FM Installation Steps

Field	Description
Basics	
Subscription	Select your subscription.
Resource Group	Select an existing resource group or create a new resource group. For more information, refer to Create a resource group topic in the Azure Documentation.

Field	Description
Virtual machine name	Enter a name for the VM.
Region	Select a region for Azure VM.
Image	Select the latest GigaVUE-FM images. NOTE: You cannot select multiple images for a VM. Refer to Configure GigaVUE Fabric Components in Azure for more details on configuring GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller in Azure.
Size	The recommended instance types are as follows: <ul style="list-style-type: none"> GigaVUE-FM - Standard_D4s_v3 UCT-V Controller - Standard_B1ms V Series Node - Standard_D4s_v4 V Series Proxy - Standard_B1ms
Authentication Type	We support only SSH public key authentication type <ul style="list-style-type: none"> SSH public key <ul style="list-style-type: none"> Enter the administrator username for the VM. Enter the SSH public key pair name. NOTE: The username "gigamon" is reserved for internal use. Do not create a user with the name "gigamon"
Disks	
Disk Size	The required disk size for GigaVUE-FM is 2 x 40GB .
Networking	
Virtual Network	Select an existing VNet or create a new VNet. For more information, refer to Create a virtual network topic in the Azure Documentation. On selecting an existing VNet, the Subnet and the Public IP values are auto-populated.
Configure network security group	Select an existing network security group or create a new network security group. For more information, refer to Network Security Groups . Configure the Network Security Group to allow GigaVUE-FM to communicate with the rest of the components.

NOTE: Verify the summary before proceeding to create. It will take several minutes for the VM to initialize. After the initialization is completed, you can verify the VM through the Web interface.

After the deployment, navigate to the VM overview page, copy the **Public IP address**, and paste it in a new web browser tab.

Install and Upgrade GigaVUE-FM

You can install and upgrade the GigaVUE-FM[®] Fabric Manager (GigaVUE-FM) on cloud platforms or on-premises.

Cloud

- Azure - To install GigaVUE-FM inside your Azure environment, you can launch the GigaVUE-FM instance in your VNet.
 - Installation: Refer to [Install GigaVUE-FM on Azure](#).
 - Upgrade: Refer to Upgrade GigaVUE-FM in Azure topic in GigaVUE-FM Installation and Upgrade Guide.
- GigaVUE-FM can also be installed in any of the cloud platform. Refer to GigaVUE-FM Installation and Upgrade Guide for more detailed information on how to install GigaVUE-FM in public, private or hybrid cloud platforms.
 - Upgrade: Refer to Upgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

On-premise

To install and upgrade GigaVUE-FM in your enterprise data center, refer to GigaVUE-FM Installation and Upgrade Guide available in the [Gigamon Documentation Library](#).

- Installation: Refer to GigaVUE-FM Installation and Upgrade Guide.
- Upgrade: Refer to Upgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

Installing GigaVUE-FM on GCP

This section describes how to install GigaVUE-FM on GCP. It consists of the following sections:

- [Before You Install](#) describes the pre-requisites and the preparatory steps required for installing GigaVUE-FM.
- [Install GigaVUE-FM on GCP](#) describes the steps to install and deploy GigaVUE-FM on GCP.

Before You Install

This section describes the hardware and virtual computing requirements for GigaVUE-FM.

Prerequisites for GigaVUE-FM

Minimum Virtual Computing Requirements	
Machine type	e2-standard-4
Memory	16GB
Virtual CPU (vCPU)	4vCPU
Additional Disk Size	40GB

Install GigaVUE-FM on GCP

The GigaVUE-FM can be launched from the Google Cloud Platform. The following instructions describes how to launch GigaVUE-FM in your Google Cloud Platform. Refer to [Create and Start a VM Instance](#) topics in GCP Documentation for more information.

Parameter	Description
Basics	
Name	Enter a name for the Instance.
Region	Select a region for Instance.
Zone	Select a zone for GCP instance.
Machine Configuration	
Machine Type	The recommended instance type is as follows: <ul style="list-style-type: none"> GigaVUE-FM - e2-standard-4
Boot Disk: Click Change . Select the Custom Image tab.	
Image	Select the latest GigaVUE-FM images. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> NOTE: You cannot select multiple images for a VM. </div>
Firewall	
Allow HTTP traffic	Enable the check box to allow HTTP traffic
Allow HTTPS traffic	Enable the check box to allow HTTPS traffic
Advanced Options	
Networking	
Network Interface	Select the Network Interface, the Network and the Subnetwork values.
SSH Keys	<ul style="list-style-type: none"> SSH keys <ul style="list-style-type: none"> Enter the admin under username.

Parameter	Description
	<ul style="list-style-type: none"> o Enter the SSH public key under key.
Disks	
Disk Size	The required disk size for GigaVUE-FM is 40GB .

After the instance deployment, navigate to the VM instances page, copy the **External IP**, and paste it in a new web browser tab.

If GigaVUE-FM is deployed in GCP, use **admin123A!!** as the password for the **admin** user to login to GigaVUE-FM. You must change the default password after logging in to GigaVUE-FM.

Installing GigaVUE-FM on OpenStack

This section describes how to install GigaVUE-FM on OpenStack. It consists of the following sections:

- [Before You Install](#) describes the pre-requisites and the preparatory steps required for installing GigaVUE-FM.
- [Install GigaVUE-FM on OpenStack](#) describes the steps to install and deploy GigaVUE-FM on OpenStack.
- [Initial GigaVUE-FM Configuration](#) describes the steps to start GigaVUE-FM instance and configure it.

Before You Install

Before installing GigaVUE-FM on OpenStack environment, follow the steps given in the Before You Begin topic in the GigaVUE Cloud Suite Deployment Guide - OpenStack for minimum compute requirements and pre-requisites.

Install GigaVUE-FM on OpenStack

To launch the GigaVUE-FM instance inside the cloud:

1. Log into Horizon.
2. From the Horizon GUI, select the appropriate project, and select **Compute > Images**. The list of existing images is displayed.
3. Select the GigaVUE-FM image and click **Launch**. The Launch Instance dialog box is displayed.
4. In the **Details** tab, enter the following information and Click **Next**.

Parameter	Attribute
Instance Name	Initial hostname for the instance
Availability Zone	Availability zone where the image will be deployed.
Count	Number of instances to be launched

5. In the **Source** tab, verify that the selected GigaVUE-FM image is displayed under **Allocated** section and click **Next**.
6. In the **Flavor** tab, select a flavor complying the [Minimum Compute Requirements](#) and then move the flavor from the **Available** section to the **Allocated** section. The selected GigaVUE-FM flavor is displayed under Allocated and click **Next**.
7. In the **Networks** tab, select the specific network for the GigaVUE-FM instance from the **Available** section and then move the Network to the **Allocated** section. The selected network is displayed under Allocated and Click **Next**.
8. In the **Network Ports** tab, click **Next** again.
9. In the **Security Groups** tab, select the appropriate security group for the GigaVUE-FM instance from the **Available** section and then move the Security Group to the **Allocated** section. For information about the security groups, refer to [Security Group](#). The selected security group is displayed under Allocated. Click **Next**.
10. In the **Key Pair** tab, select the existing key pair from the **Available** section and then move the Key Pair to the **Allocated** section. or create a new key pair. For information about the key pairs, refer to [Key Pairs](#). The selected key pair is displayed under Allocated. Click **Next**.
11. Click **Launch Instance**. The GigaVUE-FM instance takes few minutes to fully initialize.
12. From the Horizon GUI, navigate to **Compute > Instances**. You can view the launched instance displayed in the **Instances** page. During the initial boot-up sequence, click **Associate Floating IP**. The **Manage Floating IP Associations** dialog box appears.

13. In the Manage Floating IP Associations dialog box, enter the following information and click **Associate**.

Parameter	Attribute
IP Address	Floating IP address of the instance
Port to be associated	Port for the GigaVUE-FM instance

The Floating IP is then displayed in the **IP Address** column of the corresponding Instance.

Initial GigaVUE-FM Configuration

After you have deployed a new GigaVUE-FM instance, you need to perform an initial configuration before you can start using GigaVUE-FM. This is a one-time activity that must be performed for each GigaVUE-FM instance deployed.

1. From the Horizon GUI, navigate to **Compute > Instances**.
2. In the Instances page, click the GigaVUE-FM instance name. The GigaVUE-FM instance **Overview** tab is displayed by default.
3. Click the **Console** tab and the **Instance Console** appears.
4. Log in as admin with password as admin123A!! and then the console prompts you to change the default password.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.9.1.el7.x86_64 on an x86_64

123 login:

CentOS Linux 7 (Core)
Kernel 3.10.0-1062.9.1.el7.x86_64 on an x86_64

123 login: admin
Password:
You are required to change your password immediately (root enforced)
Changing password for admin.
(current) UNIX password:
New password:
Retype new password:
[admin@123 ~]$\
```

NOTE: You can also choose to perform the IP Networking and NTP configurations by running the **fmctl jump-start** command after you power on the GigaVUE-FM instance

5. To access GigaVUE-FM GUI, enter **wget -q -O - http://169.254.169.254/latest/meta-data/instance-id** command in the Instance Console and retrieve the instance ID in the format of **i-000000##** which is the default password for the admin user. If GigaVUE-FM is deployed inside OpenStack, use the **Instance ID** as the password for the admin user to login to GigaVUE-FM, however if GigaVUE-FM is deployed outside OpenStack, use admin123A!! as the default admin password.

Installing GigaVUE-FM on Nutanix

This section describes how to install GigaVUE-FM on Nutanix. It consists of the following sections:

- [Before You Install](#) describes the pre-requisites and the preparatory steps required for installing GigaVUE-FM.
- [Install GigaVUE-FM on Nutanix](#) describes the steps to install and deploy GigaVUE-FM on Nutanix.

Before You Install

This section describes the requirements and prerequisites to configure the GigaVUE Cloud Suite for Nutanix. Refer to Before You Begin topic in the *GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide* for prerequisites and minimum compute requirements.

Before installing GigaVUE-FM on Nutanix environment you must upload the recent GVM, and Fabric Controller qcow2 image file to the Prism Central. Refer to Upload Fabric Images topic in the *GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide* for more details on how to upload fabric images..

Install GigaVUE-FM on Nutanix

To launch the GigaVUE-FM instance from the Prism Central:

1. Log in to the [Gigamon Customer Portal](#) and click on Software and Release Notes.
2. Then, search **qcow2** in the search file field.
3. Use the **Filter by** option to filter your search by Product, Release, Release Type and Release date. Select GigaVUE-FM as the product, and the enter the release version in the release field.
4. The QCOW2 file appears in the list view. Click on the latest QCOW2 file to download it.
5. Log in to Prism Central.
6. In Prism Central, select **Dashboard > Virtual Infrastructure > VMs**. The VMs page appears.

NOTE: You can view the uploaded images under **Virtual Infrastructure > Images**. For more detailed information on how to upload fabric images refer Upload Fabric Images topic in the *GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide*..

7. On the VMs page, click **Create VM**. The **Create VM** window appears.

NOTE: If the device has more than one cluster, select the required cluster in the **Cluster Selection** window.

8. Enter or select the values as described in the following table.

Field	Description
General Configuration	<ul style="list-style-type: none"> • Name—Enter a name for the VM. • Description—Enter description for the VM. (optional) • Timezone—Select the time zone from the drop-down list.
Compute Details	<ul style="list-style-type: none"> • vCPU(s)—number of vCPUs required. Minimum value is 2vCPUs. However, the recommended value is 4vCPUs. • Number Of Cores Per vCPU—number of cores per vCPU. • Memory—memory size of the vCPU(s). Minimum value is 16GB.
Disks	Add, edit or delete the disks. Add the GigaVUE-FM qcow2 disk image and a Container (second disk), minimum of 40GB for the VM. Select the primary image (GigaVUE-FM qcow2) as Boot Device.
Network Adapters (NIC)	Add a minimum of 1 vNIC for traffic management.
VM Host Affinity (Optional)	Set Affinity by choosing the required nodes to run GigaVUE-FM or a particular VM.

9. Click **Save** and the new VM appears on the VMs list with the **Power State** as **Off**.
10. Select the new VM and then select **Actions > Power On**. The new VM is now Active.
11. Select the new VM and then select **Actions > Launch console**. The GigaVUE-FM console appears.
12. Log in to the GigaVUE-FM console as admin with the user name as admin and default password admin123A!! and you are requested to change the password.

NOTE: You can also choose to perform the IP Networking and NTP configurations by running the **fmctl jump-start** command after you power on the GigaVUE-FM instance. Refer to Perform Network Configurations topic in the *GigaVUE-FM Installation and Upgrade Guide* for more details on how to use **fmctl jump-start** to perform the initial network configuration.

You can also log in to GigaVUE-FM by logging in to WebUI using the configured IP address using the default user name **admin** and the default password admin123A!!.

Installing GigaVUE-FM on MS Hyper-V

This section describes how to install and configure GigaVUE-FM in a Microsoft Hyper-V environment. It consists of the following main sections:

- [Before You Install](#) describes the preparatory steps and the hardware requirements required for installing GigaVUE-FM.
- [Install GigaVUE-FM for Microsoft Hyper-V](#) describes the steps to install and deploy GigaVUE-FM.
- [Initial GigaVUE-FM Configuration](#) describes the steps to start GigaVUE-FM instance and configure it.

Before You Install

This section describes the hardware and virtual computing requirements for GigaVUE-FM. Before installing GigaVUE-FM, ensure that a supported version of Windows Server is installed on hardware that meets minimum requirements for hardware requirements).

Ensure that the GigaVUE-FM time is set correctly to ensure accuracy of the trending data that is captured.

The Hyper-V implementations provided by the following Windows Server versions have been tested and found to operate acceptably with GigaVUE-FM:

- Windows Server 2012 R2 and later

Windows Server Hardware Requirements

The following table describes the minimum requirements for the hardware on which Microsoft Hyper-V runs GigaVUE-FM.

Minimum Hardware Requirements	
Hypervisor	Microsoft Hyper-V
CPU	One or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled. Note: To run GigaVUE-FM, hardware support for virtualization must be enabled. Make sure that the BIOS option for virtualization support is not disabled. For more information, see your BIOS documentation

Minimum Hardware Requirements	
RAM	At least 16GB
Disk Space	At least 84GB shared (FC, iSCSI, NFS, or FCoE) or locally attached storage (PATA, SATA, SCSI). NOTE: Increase the disk space depending on the configuration load requirements for the given GigaVUE-FM instance.
Network	At least one 1Gb NIC

NOTE: Refer to the Microsoft documentation for information on enabling Hyper-V.

The following table lists the virtual computing resources that the Windows Server must provide for each GigaVUE-FM instance.

Minimum Virtual Computing Requirements	
Memory	Minimum 8GB memory
Virtual CPU	2 vCPU
Virtual Storage for Guest	84GB Virtual IDE (the Hyper-V default) <ul style="list-style-type: none"> • System Disk - 40GB • Swap Disk - 4GB • Data Disk - 40GB
Virtual Network Interfaces	1 vNIC using Hyper-V Virtualized NIC (the Hyper-V default)

Install GigaVUE-FM for Microsoft Hyper-V

The GigaVUE-FM software package for Microsoft Hyper-V environments is distributed as an **ISO image** file. This section describes how to deploy a fresh installation of GigaVUE-FM on a Hyper-V host.

Install GigaVUE-FM from an ISO Image File

Use the Hyper-V Manager to install the GigaVUE-FMISO image file.

NOTE: The ISO image file must be stored in a location that is accessible to the Hyper-V Manager.

To create the Virtual Machine for GigaVUE-FM in Microsoft Hyper-V:

1. Click **Start > Administrative Tools > Hyper-V Manager** to open the Hyper-V Manager.
2. From the Actions pane, click **New > Virtual Machine**. Refer to [Figure 10](#) **Opening the Virtual Machine Wizard**.

The **New Virtual Machine Wizard** opens.

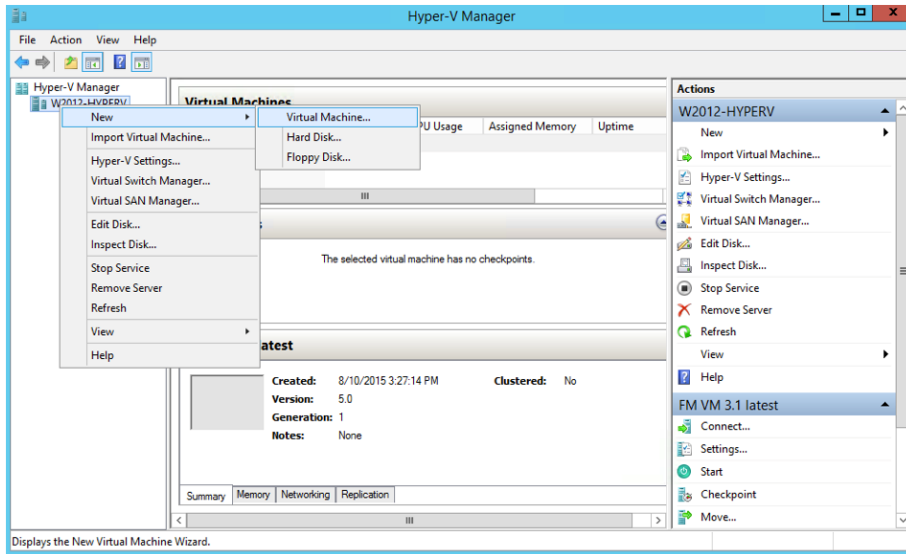


Figure 1 Opening the Virtual Machine Wizard

3. Read the notes on the Before You Begin screen (refer to [Figure 2 Before You Begin Screen](#)), and then click **Next** to continue.

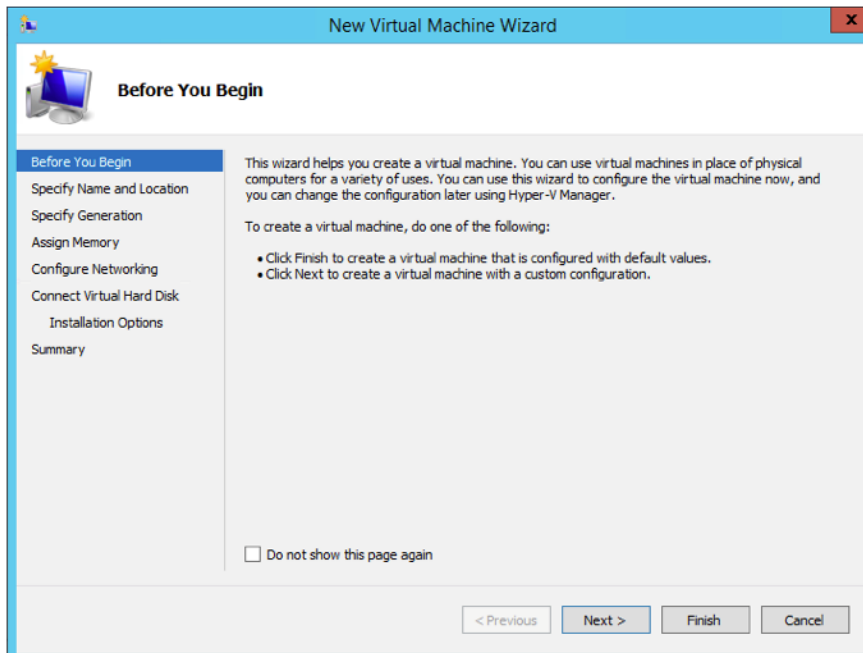


Figure 2 Before You Begin Screen

4. After the **Specify Name and Location** page of the **New Virtual Machine Wizard** opens, do the following:
 - a. Supply a descriptive name for the GigaVUE-FM virtual machine in the **Name** field.

By default, the virtual machine will be stored in the default configuration folder shown in the **Location** text box. You can change this default location by checking the **Store the virtual machine in a different location** check box and providing a custom path.

b. Click **Next** to continue.

5. On the **Specify Generation** page of the **New Virtual Machine Wizard**, select **Generation 1**

NOTE: It is important to select Generation 1 and not Generation 2. Selecting Generation 2 may lead to failure of the GigaVUE-FM installation process because the CD Drive is presented as an SCSI device and not IDE.

6. Click **Next** to continue.

The **Assign Memory** page of the **New Virtual Machine Wizard** opens.

7. Change the **Memory** assigned to this virtual machine to **16384** MB, and then click **Next** to continue.

The **Configure Networking** page of the **New Virtual Machine Wizard** opens.

8. From the Connection drop-down list, select the virtual network to which GigaVUE-FM will connect to, and then click **Next** to continue.

The **Connect Virtual Hard Disk** page of the **New Virtual Machine Wizard** opens, which is shown in [Figure 3 Connect Virtual Hard Disk Page](#).

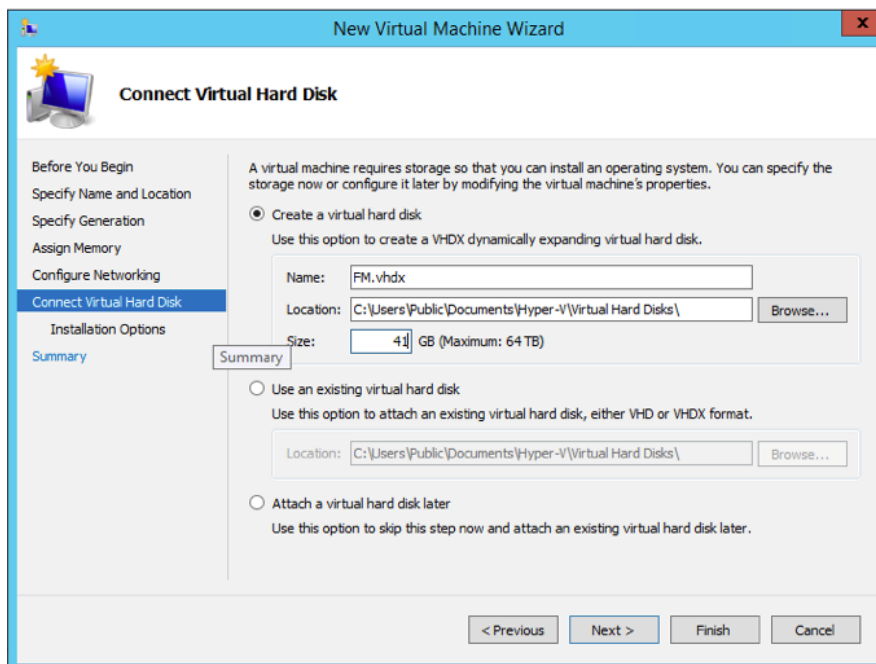


Figure 3 Connect Virtual Hard Disk Page

9. Select the **Create a virtual hard disk** option and set the **Size** to **41 GB**.

You can accept the default **Name** and **Location** or customize them according to your needs. When you have finished, click **Next** to continue.

The **Installation Options** page of the **New Virtual Machine Wizard** opens, which is shown in [Figure 4 Install Options Page](#).

10. Use this dialog box to select the ISO image file for GigaVUE-FM. As shown in the figure [Figure 4 Install Options Page](#), set the following options:
 - a. Select the option **Install an operating system from a bootable CD/DVD-ROM**.
 - b. Set the **Media** option to **Image file (.iso)**.
 - c. Use the **Browse** button to navigate to the GigaVUE-FM ISO image file.
 - d. Click **Next** to continue.

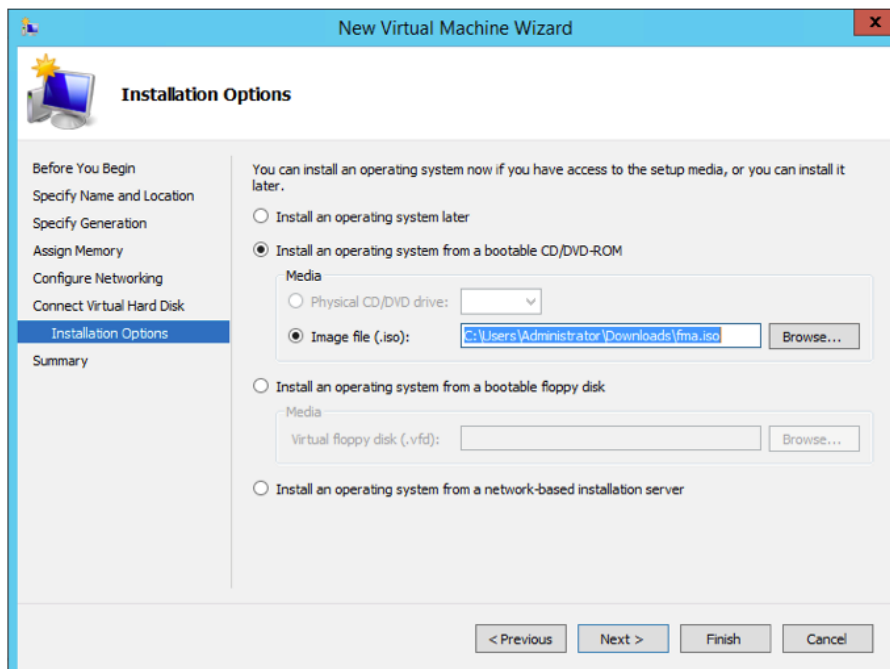


Figure 4 *Install Options Page*

After you click **Next**, the summary page of the **New Virtual Machine Wizard** opens, showing the settings that you configured for the GigaVUE-FM virtual machine.

11. Click **Finish** to create the GigaVUE-FM virtual machine as configured. Alternatively, you can use the **Previous** button to go back and change settings.

The New Virtual Machine Wizard only creates the GigaVUE-FM virtual machine, returning you to the Hyper-V Manager when creation is complete. The new GigaVUE-FM virtual machine is listed in the **Action** pane by the name you supplied during installation.

The procedures given below will take you through the steps of adding an additional virtual hard disk and actually installing GigaVUE-FM.

Add Additional Virtual Hard Disk and Install GigaVUE-FM

To add an additional virtual hard disk and install GigaVUE-FM:

1. In Hyper-V Manager, from the Actions pane, select the newly added GigaVUE-FM virtual machine, and then click **Settings**.
2. In the Settings page, select **IDE Controller 0**.
3. In the IDE Controller pane that appears to the right, select **Hard Drive**, and then click **Add**. Refer to the following figure:

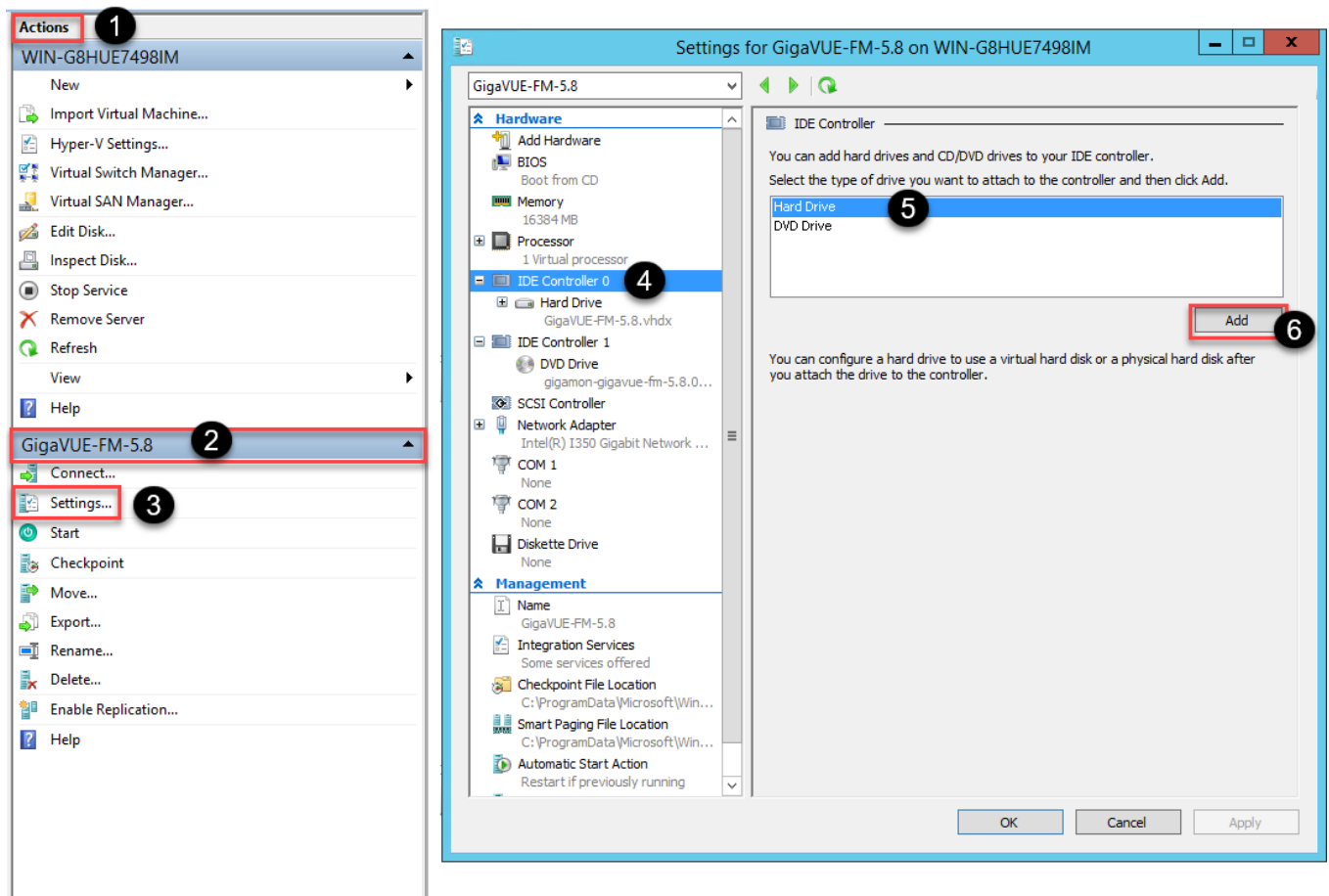


Figure 5 Navigating to Add Additional Hard Disk

A new Hard Drive entry is added under IDE Controller 0.

4. Select the Hard Drive entry.
5. In the Hard Drive pane that appears to the right, select **Virtual hard disk**, and then click **New** as shown in the following figure:

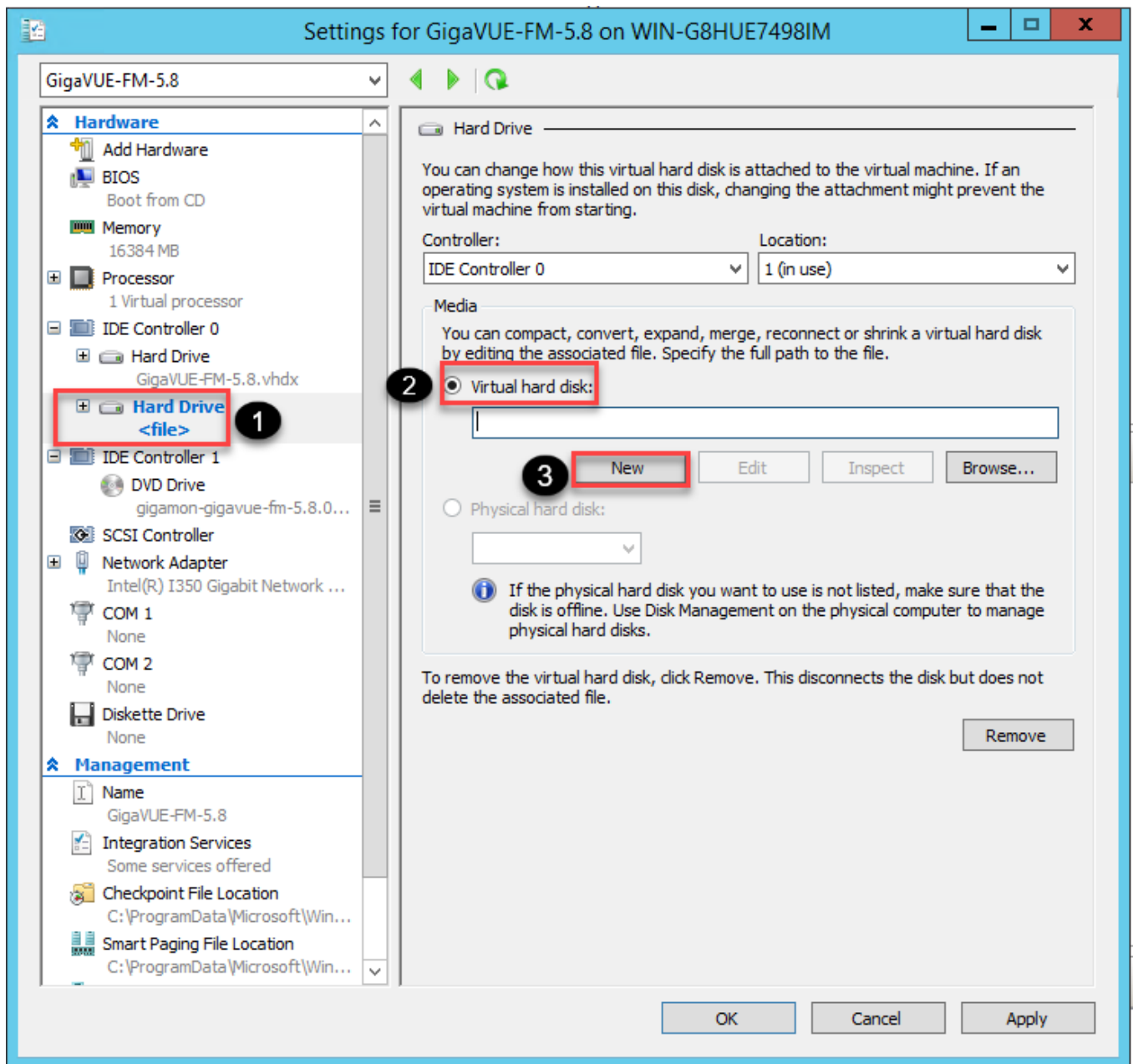


Figure 6 Navigating to the New Virtual Hard Disk Wizard

The **New Virtual Hard Disk Wizard** opens.

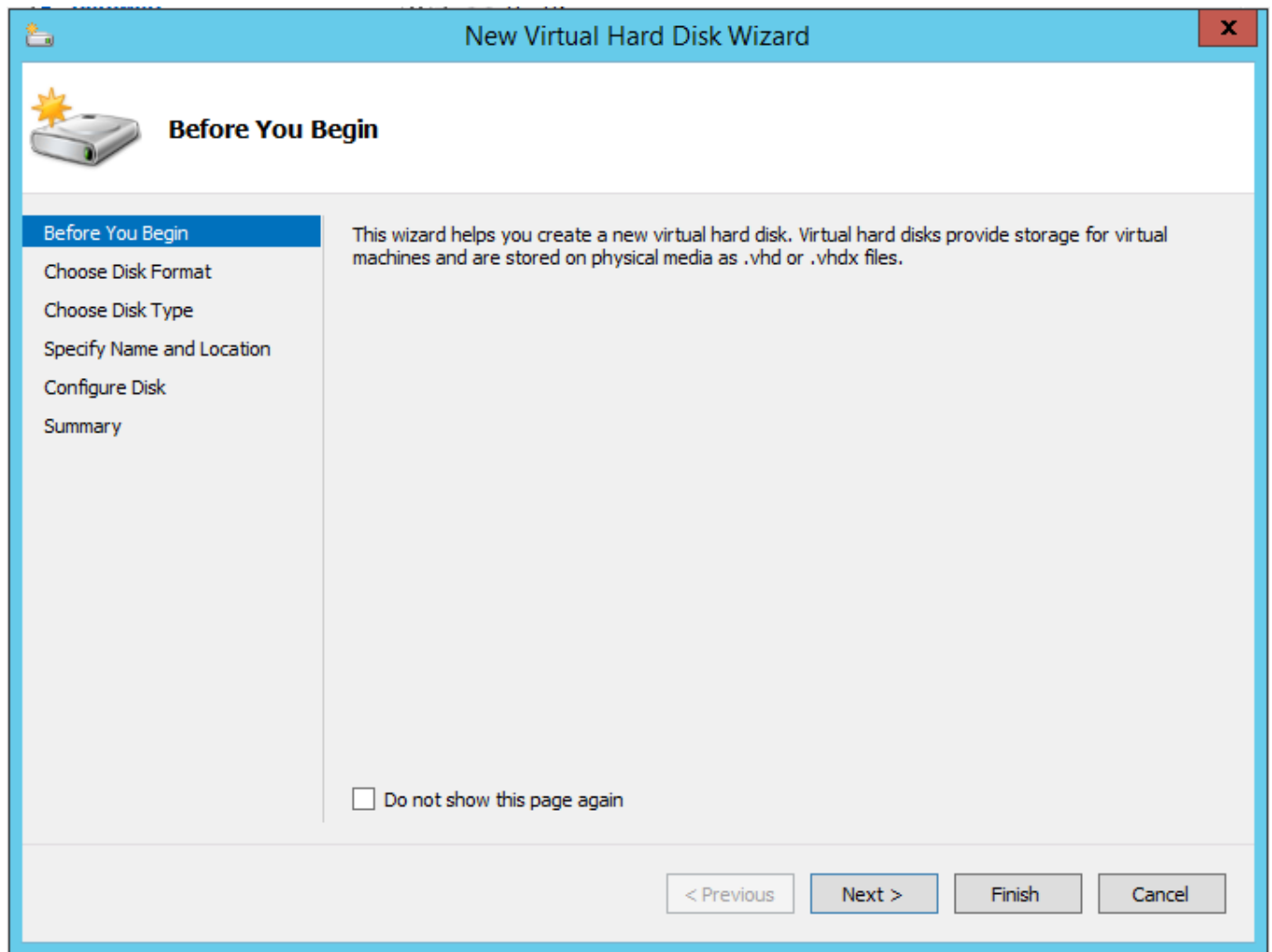


Figure 7 *New Virtual Hard Disk Wizard*

6. Click **Next** to go to the Choose Disk Format page of the wizard.
7. Select the required format that you want to use for the virtual hard disk, and then click **Next**.

The Choose Disk Type page of the wizard appears.

8. Select the required disk type for the virtual hard disk, and then click **Next**.

The Specify Name and Location page of the wizard appears.

9. Specify a unique name for the virtual hard disk, and then browse and select the location where you want to save the disk.
10. Click **Next**. The Configure Disk page of the wizard appears.
11. You can choose one of the following options to configure the virtual hard disk:
 - o Create a blank virtual hard disk of size 41 GB.
 - o Choose a physical hard disk from which you can copy the contents into the new virtual hard disk.

- Browse and select a virtual hard disk from which you can copy the contents into the new virtual hard disk.
12. Click **Next** to exit the New Virtual Hard Disk Wizard.
 13. Click **OK**. The GigaVUE-FM installation begins as shown in the following figure:

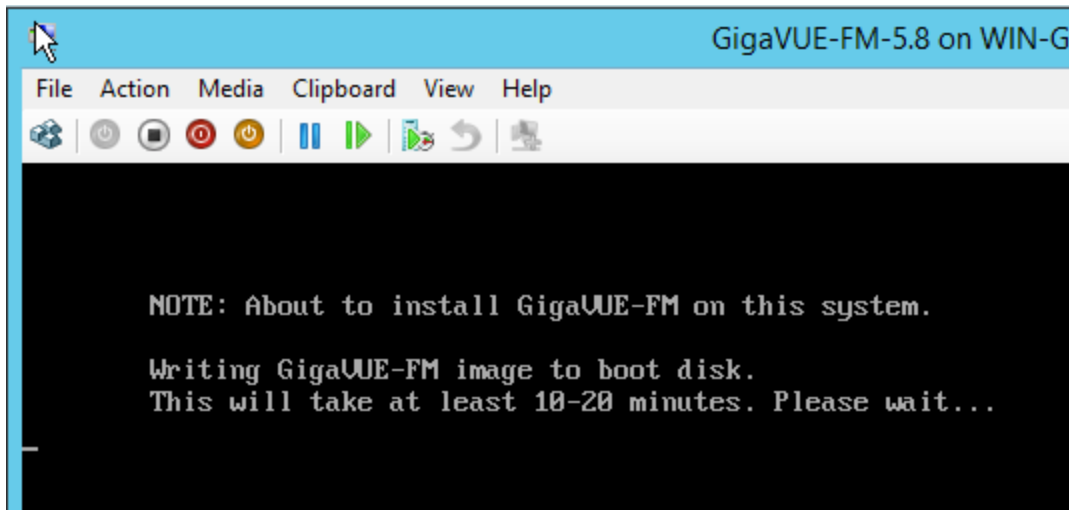


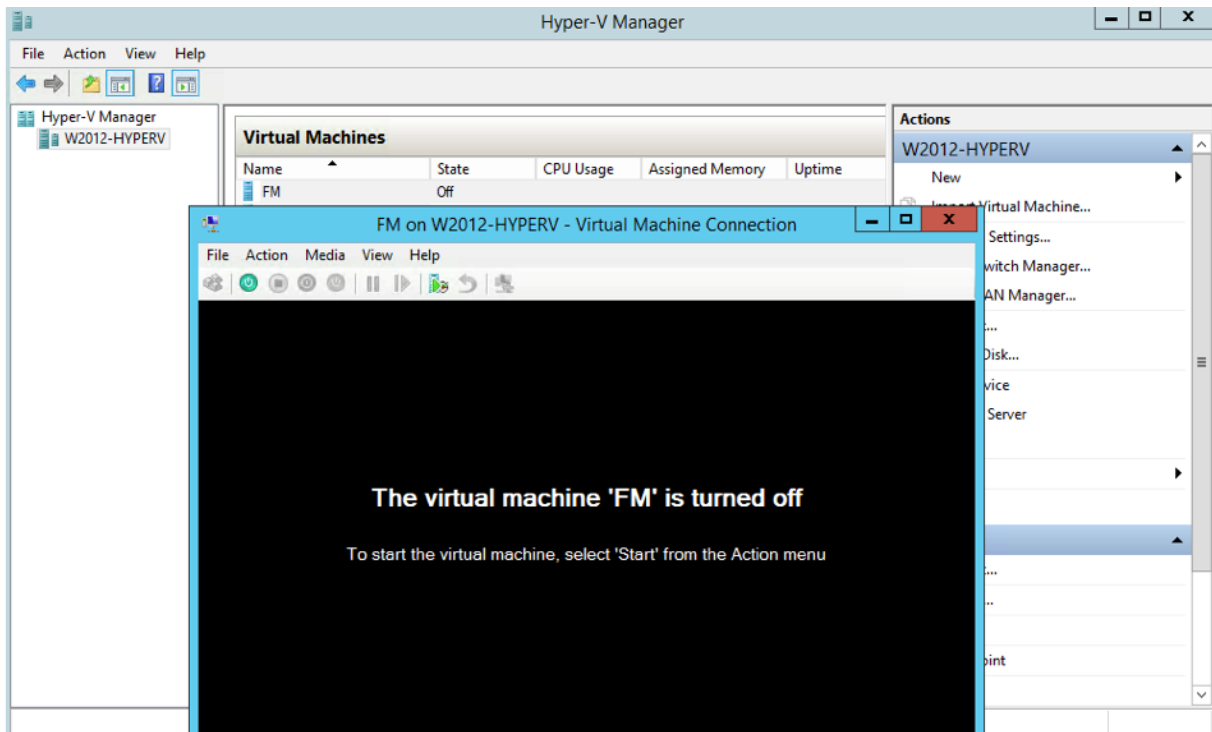
Figure 8 *GigaVUE-FM Installation Begins*

It may take several minutes for the installation to complete. The system will reboot after the installation is completed.

Connect and Power On the GigaVUE-FM Virtual Machine

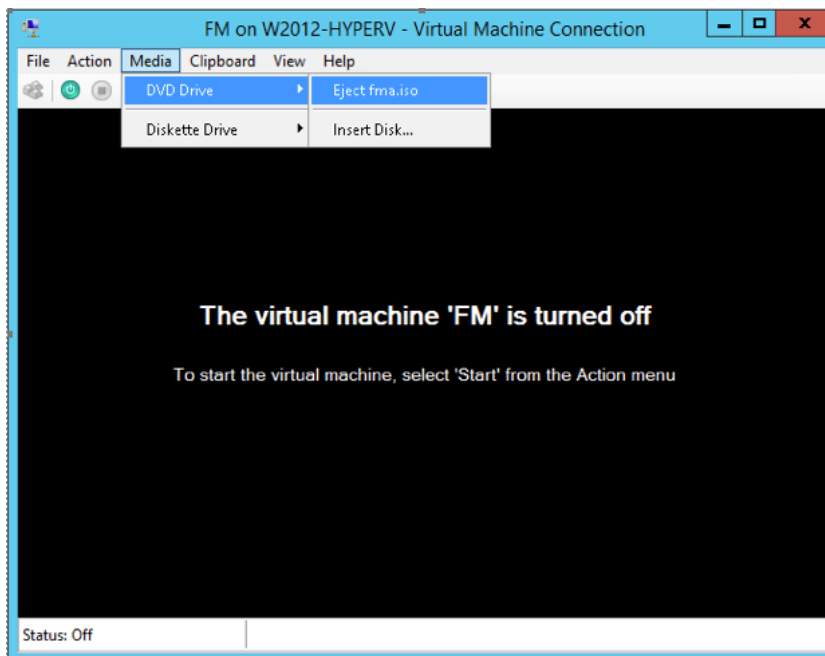
The next step is to connect to the GigaVUE-FM virtual machine from within Hyper-V Manager and start it. This begins the actual installation of the GigaVUE-FM Virtual Appliance from the connected ISO image file. Once GigaVUE-FM finishes installing from the ISO image file, you will then disconnect the ISO image file and restart the virtual machine.

1. In Hyper-V Manager, locate the **Virtual Machines** entry in the results pane, right-click the GigaVUE-FM virtual machine, and click the **Connect** option.
2. The Virtual Machine Connection tool opens for the GigaVUE-FM virtual machine.



3. Select **Action > Start** to start the GigaVUE-FM virtual machine from the Virtual Machine Connection tool.
4. The GigaVUE-FM virtual machine powers on. You can monitor the progress of the system start in the Virtual Machine Connection tool.

The system power-on can take several minutes as GigaVUE-FM is installed from the ISO image file. Disconnect the media before Powering On as shown below:



Disconnect the ISO Image File

It is important to disconnect the ISO image file before you power on GigaVUE-FM again so you don't have to go through the image install process again. Disconnect the ISO image file as follows:

1. In Hyper-V Manager, locate the **Virtual Machines** entry in the results pane and select the GigaVUE-FM virtual machine.
2. In the **Actions** pane, click the **Settings** entry under the GigaVUE-FM virtual machine name.

A Settings dialog box for the GigaVUE-FM virtual machine appears.

3. Select the **DVD Drive** entry in the panel on the left of the Settings dialog box and change its setting from **Image file** to **None**, as shown in the figure below.
4. Click the **OK** button to apply the changes.

This concludes the installation procedure for GigaVUE-FM on Hyper-V. The next step is to power on the virtual machine and perform its initial configuration, as described in [Initial GigaVUE-FM Configuration](#).

IMPORTANT: Clear the browser cache before logging in to GigaVUE-FM.

Initial GigaVUE-FM Configuration

After you have deployed a new GigaVUE-FM instance, you need to perform an initial configuration before you can start using GigaVUE-FM. This procedure only needs to be performed once for each GigaVUE-FM instance deployed.

NOTE: Use Care When Shutting Down or Rebooting GigaVUE-FM. **Never** directly Power-Off the virtual machine. For Microsoft Hyper-V environment, you cannot use any of the reset, or turn-off hooks. Using either of these may lead to corruption that will prevent proper GigaVUE-FM operation.

The best ways to **shutdown** a GigaVUE-FM on Hyper-V is to use either Shutdown or Ctrl+Alt+Del from the **Action** button on the virtual console.

To perform the initial configuration:

1. Click **Start > Administrative Tools > Hyper-V Manager**.

NOTE: Make sure you have already disconnected the ISO image file used to install GigaVUE-FM. Refer to [Disconnect the ISO Image File](#) for details.

2. Locate the **Virtual Machines** entry in the results pane, right-click the GigaVUE-FM virtual machine, and click the **Connect** option. The Virtual Machine Connection tool opens for the GigaVUE-FM virtual machine.
3. Select **Action > Start** to start the GigaVUE-FM virtual machine from the Virtual Machine Connection tool. The GigaVUE-FM virtual machine powers on and displays a login prompt.
4. Log in as **admin** with password **admin123A!!**. You will be prompted to change your password. After you change and confirm your password, perform the following steps:
 - a. Run the **fmctl jump-start** command. The Initial System Configuration screen appears as shown in the following figure:

Initial System Configuration

Hostname	unconfigured-gigavue-fm		
Domain Name			
Enable DHCP4	yes	Enable DHCP6	yes
IPv4 Address		IPv6 Address	
CIDR		CIDR	
Gateway		Gateway	
DNS Servers			
Search Domains			
Enable NTP	no	NTP Servers	0.centos.pool.ntp.org 1.centos.poo
		NTP Version	4

< OK > <Cancel>

- b. Provide a unique hostname for GigaVUE-FM. Note that the hostname may contain letters, numbers, periods (.), and hyphens (-), but may not begin with a hyphen. No other special characters are permitted.

- c. Enter the required domain name.
- d. Decide whether to use DHCP for the management interface. Choose one of the following options:
 - If you enter **yes**, the **IPv4 Address** or **IPv6 Address, CIDR, Gateway, DNS Servers**, and **Search Domains** are dynamically set up for the management interface.
 - If you enter **no**, you must provide the following:
 - i. **IPv4 Address** or **IPv6 Address**, and the respective **CIDR** and **Gateway**.
 - ii. In the **DNS Servers** field, provide the address of any additional name servers required. Enter the set of IP addresses with spaces in between.
 - iii. In the **Search Domains** field, provide the required DNS domains with spaces in between.
- e. You can choose to either enable or disable NTP. In the **Enable NTP** field, enter one of the following:
 - **Yes**—Use NTP to synchronize the time between GigaVUE-FM virtual machine and the NTP server. In the **NTP Servers** and **NTP Version** fields, enter the NTP server address and the version number of the NTP server.
 - **No**—you can skip the next step and directly save your configurations.
- f. Select **OK** to save your configurations.
- g. Reboot your GigaVUE-FM virtual machine.

You can now access GigaVUE-FM by opening a browser and entering its IP address (the IP address you specified).

Installing GigaVUE-FM on KVM

This section describes how to install and configure GigaVUE-FM in a KVM environment. It consists of the following main sections:

- [Before You Install](#) describes the pre-requisites and the preparatory steps required for installing GigaVUE-FM.
- [Install GigaVUE-FM for KVM](#) describes the steps to install and deploy GigaVUE-FM on KVM environment.
- [Initial GigaVUE-FM Configuration](#) describes the steps to start GigaVUE-FM instance and configure it.

Before You Install

This section describes the hardware requirements and the limitations for installing GigaVUE-FM in a KVM environment. Before you begin, ensure that the GigaVUE-FM time is set correctly to ensure accuracy of the trending data that is captured.

Limitations

You can install GigaVUE-FM in a KVM environment, but you cannot access GigaVUE-FM through CLI in a KVM environment using SSH. In KVM, you can only access the GigaVUE-FM CLI using the VNC console.

System Requirements

This section describes the hardware and virtual computing requirements for GigaVUE-FM.

Linux Server Hardware Requirements

The following table describes the minimum requirements for the hardware on which KVM runs GigaVUE-FM.

Minimum Hardware Requirements	
Hypervisor	KVM Supported (tested on previous versions of GigaVUE-FM) <ul style="list-style-type: none"> ▪ v2.0.0
CPU	One or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled.

Minimum Hardware Requirements	
	Note: To run GigaVUE-FM, hardware support for virtualization must be enabled. Make sure that the BIOS option for virtualization support is not disabled. For more information, see your BIOS documentation.
RAM	At least 16GB.
Disk Space	At least 84GB shared (FC, iSCSI, NFS, or FCoE) or locally attached storage (PATA, SATA, SCSI). NOTE: Increase the disk space depending on the configuration load requirements for the given GigaVUE-FM instance.
Network	At least one 1Gb NIC.

The following table lists the virtual computing resources that the Linux Server must provide for each GigaVUE-FM instance.

Minimum Virtual Computing Requirements	
Memory	Minimum 8GB memory
Virtual CPU	2 vCPU
Virtual Storage for Guest	84GB <ul style="list-style-type: none"> • System Disk - 40GB • Swap Disk - 4GB • Data Disk - 40GB
Virtual Network Interfaces	One vNIC

Install GigaVUE-FM for KVM

The GigaVUE-FM software package for KVM environments is distributed as an **ISO image** file. The following sections describes how to deploy a fresh installation of GigaVUE-FM on a KVM host.

These steps are only valid for new installations of GigaVUE-FM.

Install GigaVUE-FM from an ISO Image File

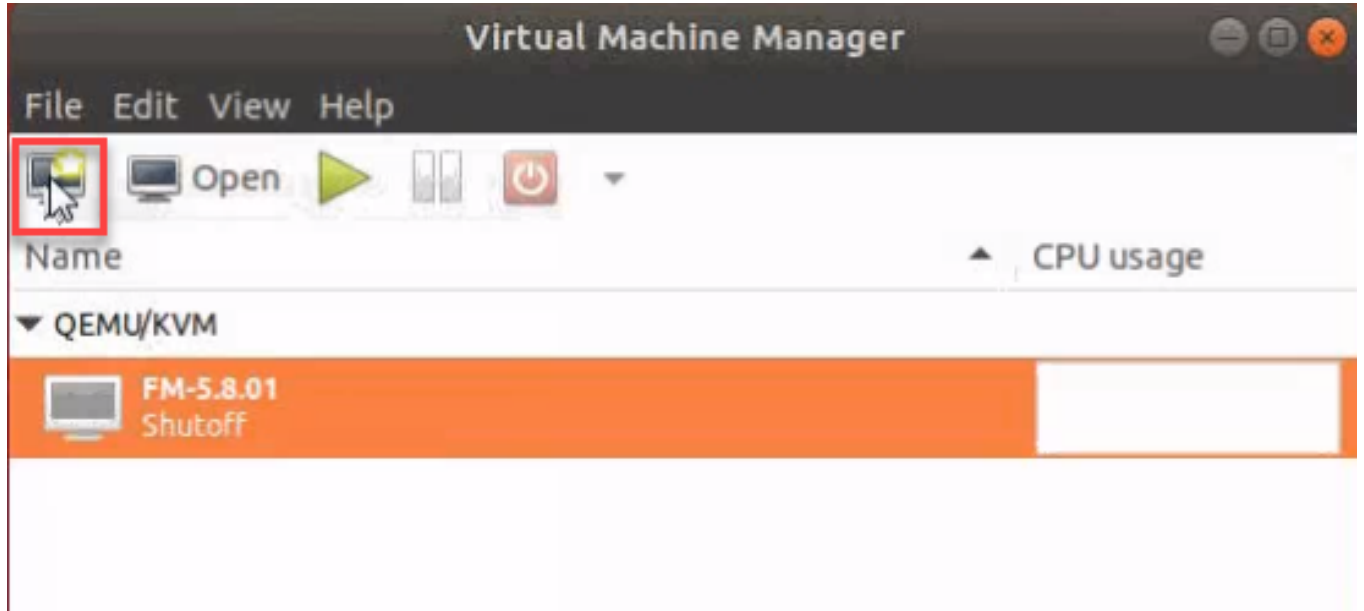
Use the Virtual Machine Manager to install the GigaVUE-FMISO image file.

NOTE: The ISO image file must be stored in a location that is accessible to the Manager.

To create the Virtual Machine for GigaVUE-FM in KVM:

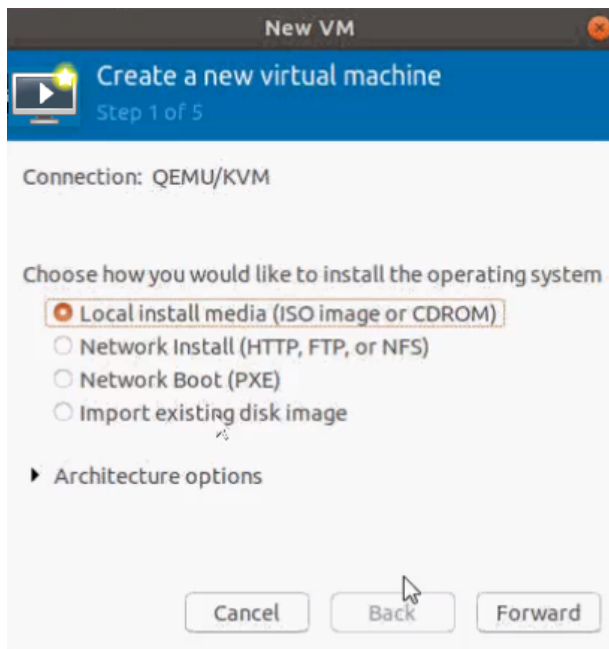
NOTE: These instructions use “Virtual Machine Manager” to create and manage the virtual machines (VMs).

1. Open the Virtual Machine Manager, and then click the **Create a new virtual machine** icon as shown in the following figure:

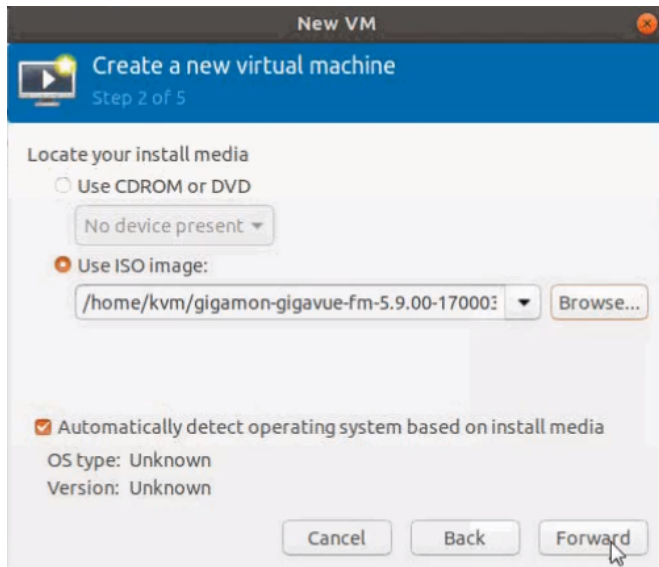


The **New Virtual Machine Wizard** opens.

2. Select **Local install media (ISO image or CDROM)**, and then click **Forward** to continue.

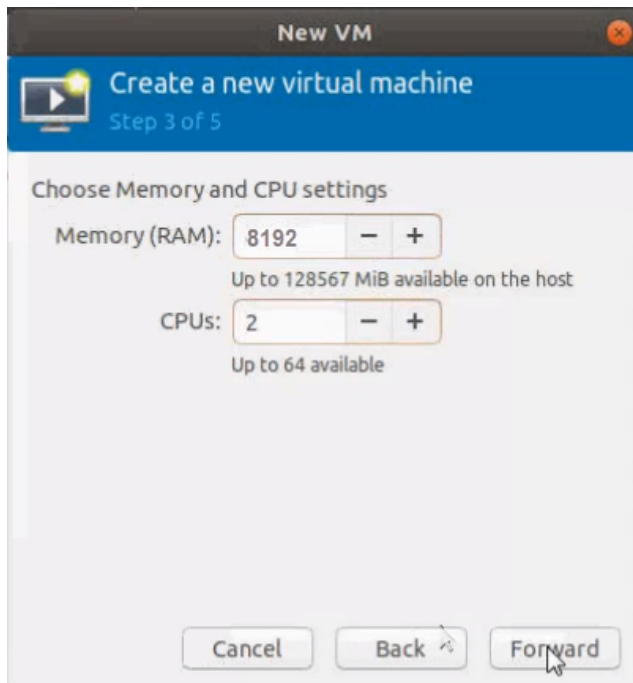


3. Browse and select the location from where to upload the GigaVUE-FM ISO image, and then select the **Automatically detect operating system based on install media** check box.



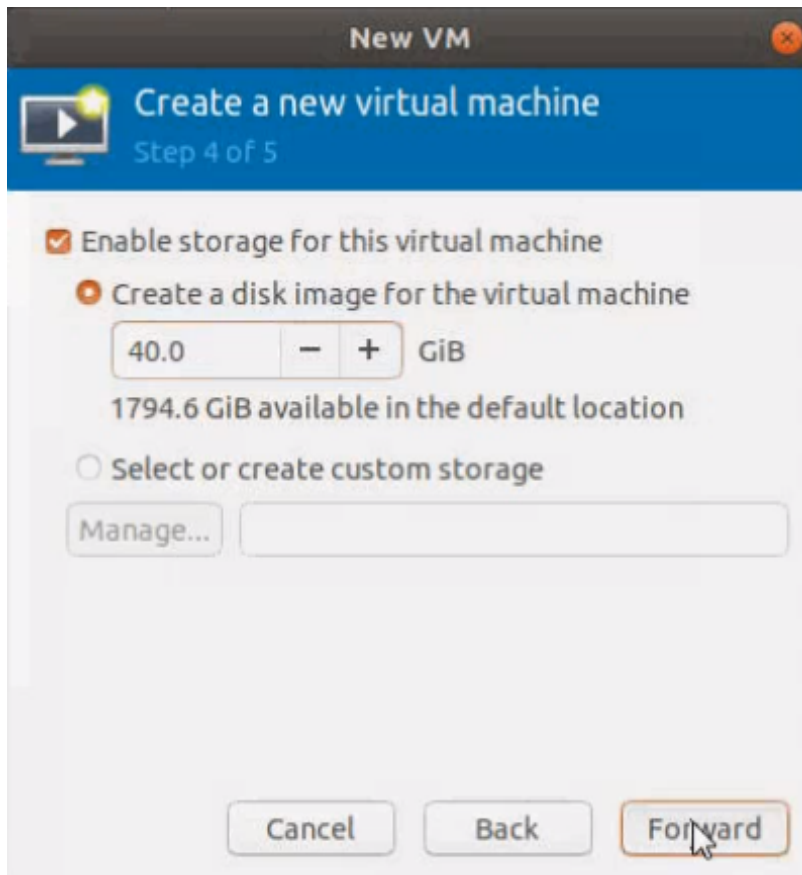
Click **Forward** to continue.

4. Set the **Memory** and **CPU** Settings.



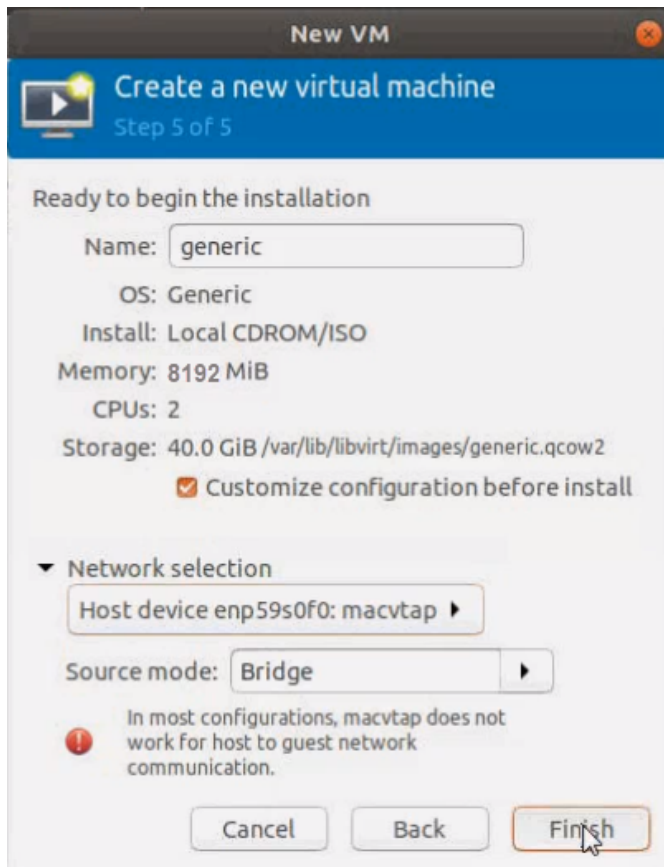
Click **Forward** to continue.

5. Select the **Enable storage for this virtual machine** check box, and set the **Size** to **40Gb**.

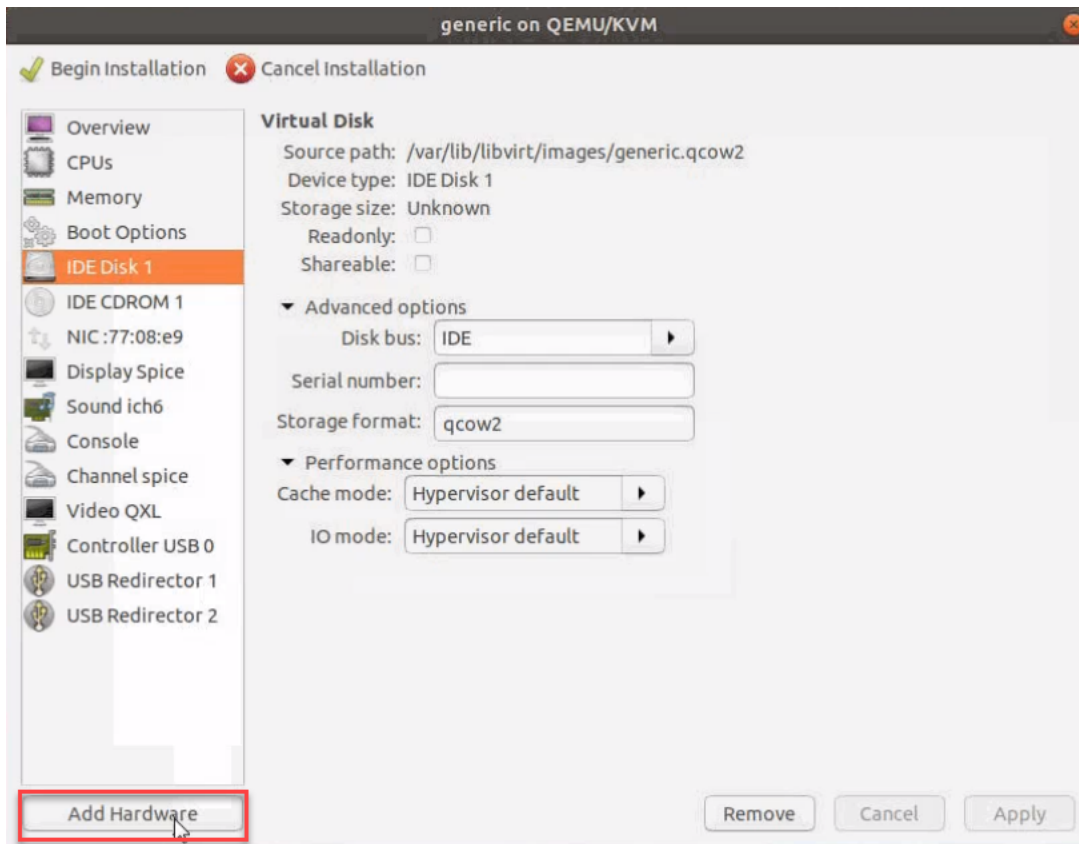


Click **Forward** to continue.

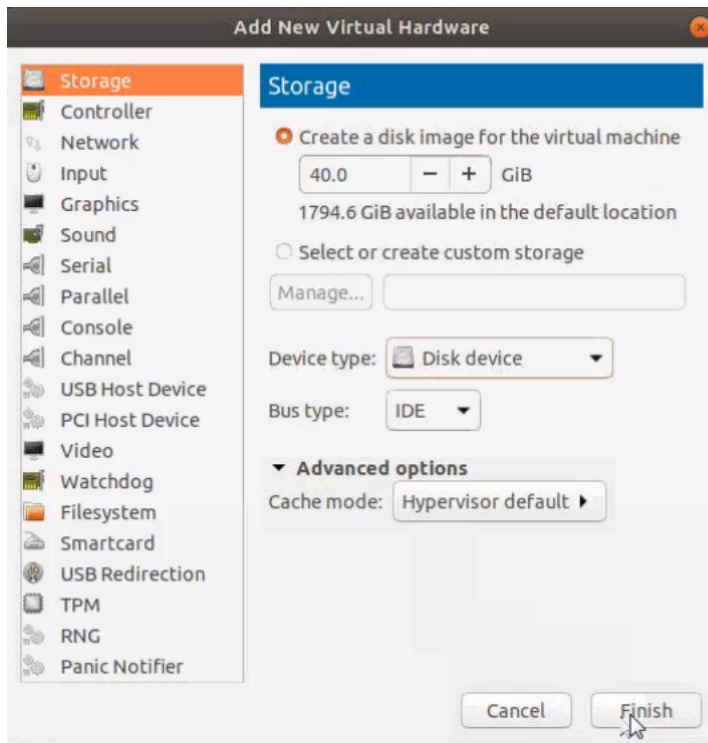
6. On the next screen, complete the following:
 - a. Enter a unique name for the virtual machine.
 - b. Select the **Customize configuration before install** check box.
 - c. From the **Network Selection** drop-down list, select the required network communication option.
 - d. From the **Source mode** drop-down list, select **Bridge**.
 - e. Click **Finish**.



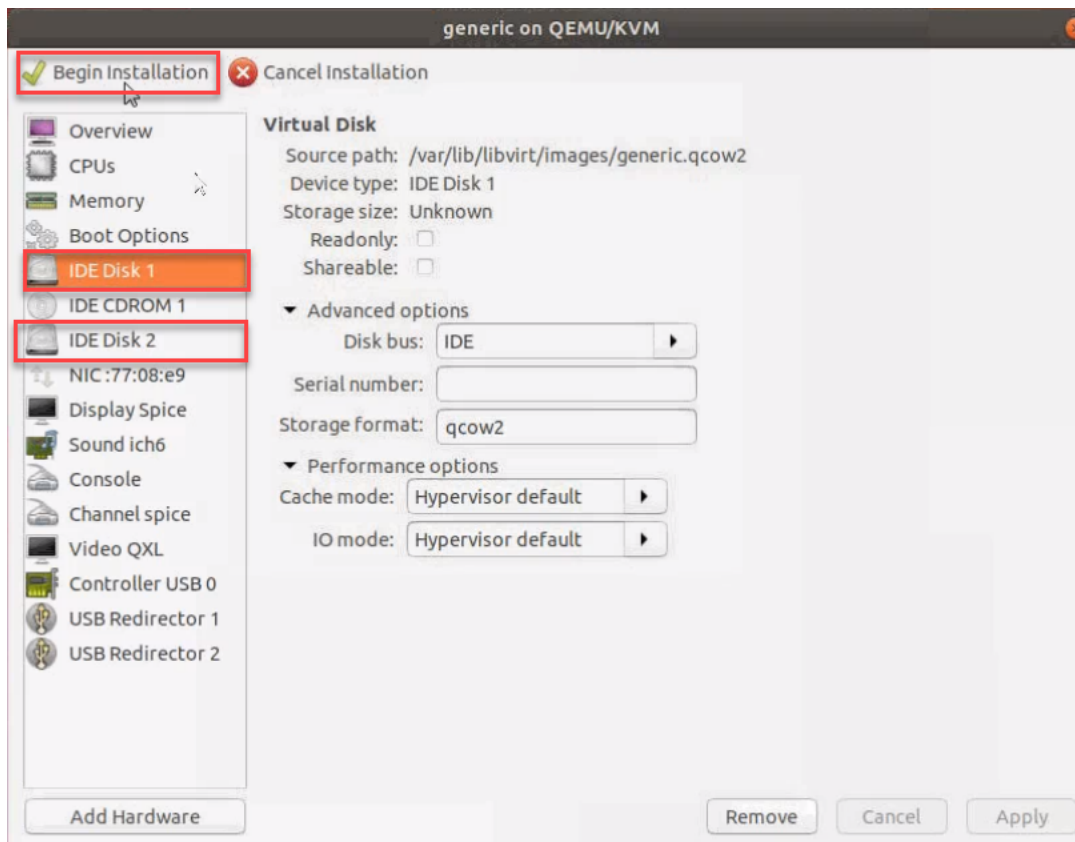
The summary screen appears as shown in the following figure:



7. Verify the options that you have selected, and then click **Add Hardware** to add the second disk.
8. In the Add New Virtual Hardware screen, set the disk size to **40Gb**.



- Click **Finish**. The summary screen appears again where you can verify the details of IDE Disk 2 that you added. Click **Begin Installation**.



Once the installation is complete, the virtual machine launches.

Initial GigaVUE-FM Configuration

After you have deployed a new GigaVUE-FM instance, you need to perform an initial configuration before you can start using GigaVUE-FM. This procedure only needs to be performed once for each GigaVUE-FM instance deployed.

To perform the initial configuration:

1. Open Virtual Machine Manager.
2. Locate the **Virtual Machines** entry in the results pane, right-click the GigaVUE-FM virtual machine, and click the **Open** option.

The Virtual Machine Connection tool opens for the GigaVUE-FM virtual machine.

3. Open the GigaVUE-FM virtual machine from the Virtual Machine tool.
4. The GigaVUE-FM virtual machine powers on and displays a login prompt.
5. Log in as **admin** with password **admin123A!!**. You will be prompted to change your password. After you change and confirm your password, perform the following steps:
 - a. Run the **fmctl jump-start** command. The Initial System Configuration screen appears as shown in the following figure:

Initial System Configuration

Hostname	unconfigured-gigavue-fm		
Domain Name			
Enable DHCP4	yes	Enable DHCP6	yes
IPv4 Address		IPv6 Address	
CIDR		CIDR	
Gateway		Gateway	
DNS Servers			
Search Domains			
Enable NTP	no	NTP Servers	0.centos.pool.ntp.org 1.centos.pool.ntp.org
		NTP Version	4

< **OK** > <Cancel>

- b. Provide a unique hostname for GigaVUE-FM. Note that the hostname may contain letters, numbers, periods (.), and hyphens (-), but may not begin with a hyphen. No other special characters are permitted.

- c. Enter the required domain name.
- d. Decide whether to use DHCP for the management interface. Choose one of the following options:
 - If you enter **yes**, the **IPv4 Address** or **IPv6 Address, CIDR, Gateway, DNS Servers**, and **Search Domains** are dynamically set up for the management interface.
 - If you enter **no**, you must provide the following:
 - i. **IPv4 Address** or **IPv6 Address**, and the respective **CIDR** and **Gateway**.
 - ii. In the **DNS Servers** field, provide the address of any additional name servers required. Enter the set of IP addresses with spaces in between.
 - iii. In the **Search Domains** field, provide the required DNS domains with spaces in between.
- e. You can choose to either enable or disable NTP. In the **Enable NTP** field, enter one of the following:
 - **Yes**—Use NTP to synchronize the time between GigaVUE-FM virtual machine and the NTP server. In the **NTP Servers** and **NTP Version** fields, enter the NTP server address and the version number of the NTP server.
 - **No**—you can skip the next step and directly save your configurations.
- f. Select **OK** to save your configurations.
- g. Reboot your GigaVUE-FM virtual machine.

You can now access GigaVUE-FM by opening a browser and entering its IP address (the IP address you specified).

Upgrade GigaVUE-FM

This section describes how to upgrade GigaVUE-FM to the latest version in VMware ESXi host, Microsoft HyperV environment, or private cloud environment.



IMPORTANT:

- **Before you upgrade**, read [Important GigaVUE-FM Upgrade Guidance](#) for special guidelines and caveats related to upgrading from specific versions of GigaVUE-FM.
- Upgrade requires the underlying processor having AVX instruction set support.
 - Once the GigaVUE-FM is migrated to the host which supports the AVX, the GigaVUE-FM must be power cycled so that the current host's processor flags will be chosen.
- If GigaVUE-FM is deployed in AWS or Azure, follow the steps in the below mentioned section to upgrade GigaVUE-FM:
 - [Upgrade GigaVUE-FM in AWS](#)
 - [Upgrade GigaVUE-FM in Azure](#)

At a high level, the upgrade process involves the following steps:

1. Before starting an upgrade to GigaVUE-FM, get the latest image, upgrade information, and Release Notes from the [Software & Release Notes](#) download page (login required) on the Gigamon Community.
2. Be sure to review the *GigaVUE Release Notes* for the latest release before performing the upgrade.
 - Ensure your environment supports any specified system requirements.
 - Check the minimum memory requirements in the new release as they may change between releases.
3. Once the GigaVUE-FM image is obtained, download it to a server within your environment. This must be a server that your current GigaVUE-FM instance can access to upload it.
4. **(Important)** Save your current configuration using the facilities provided by the hypervisor before upgrading.
5. Verify that the GigaVUE-FM instance time is set correctly to ensure accuracy of the trending data that is captured.
6. Perform the upgrade using either the Command-Line Interface (CLI) or the GigaVUE-FM User Interface (UI).

Upgrade Methods:

- Upgrade GigaVUE-FM from the GigaVUE-FM CLI
- Upgrade GigaVUE-FM from the UI

Important GigaVUE-FM Upgrade Guidance

To upgrade GigaVUE-FM, the recommended procedure is to back up your current configuration and perform the pre-upgrade checks (memory requirements, the maximum number of images) before installing the image. You can upgrade via the GigaVUE-FM GUI or CLI. It is recommended that you plan your upgrade before performing any upgrade steps. Refer [Supported Upgrade Paths for GigaVUE-FM](#) for details on upgrade path.

Best Practice: Before performing an upgrade, in addition to taking a backup of GigaVUE-FM, also take a Sysdump, which provides valuable configuration information that is not captured in the backup. You can use the Sysdump after the upgrade to troubleshoot any upgrade-related issues with your configurations.

GigaVUE-FM Upgrade Guidance for Application Intelligence

Starting from Software version 6.5.00, Application Intelligence solution can be configured from the Monitoring Session Page. You cannot create a new Application Intelligence Session or edit an Application Intelligence Session for virtual environment from the **Application Intelligence** page.

In the Monitoring Session page, Application Filtering can be configured either with Pass All or Advanced Rules in the fifth Rule Set. You cannot configure Application Filtering with both Pass All and Advanced Rules in the fifth Rule set. Therefore, before upgrading your GigaVUE-FM to 6.5.00, ensure that none of the existing Application Intelligence Session has Application Filtering configured with both Advanced Rules as Drop and No Rule Match Pass All in the fifth rule set. Otherwise, after upgrading to 6.5.00, you must delete that particular Application Intelligence Session to continue with your migration process.

For this reason, before upgrading to 6.5.00, you must edit the fifth rule set in the Application Filtering such that either only Advanced Rule as Drop or No Rule Match Pass All exists. Else, after upgrading to 6.5.00, you must delete that particular Application Intelligence Session to continue with your migration process. Refer to Migrate Application Intelligence Session to Monitoring Session section in the respective cloud deployment guides for more detailed information on how to migrate the existing Application Intelligence Session to the Monitoring Session page.

GigaVUE-FM Migration Guidance

GigaVUE-FM v5.8.01 introduced several significant changes that included improvements in usability and performance. These changes involved upgrading and replacing databases and changing the underlying operating system. For this reason, when upgrading from any pre-5.8.xx version of FM to version 5.8.xx or above, you must first migrate your existing configurations and data such as audit logs, events, syslogs, and statistics from your current pre-5.8.xx GigaVUE-FM version to GigaVUE-FM v6.5.00.

Special migration steps and supported upgrade paths are provided under [Migrate GigaVUE-FM](#) in the [5.10 Documentation](#). After GigaVUE-FM v5.10.xx, migration is no longer needed when upgrading to future versions. For supported upgrade paths requiring a special migration step, see [Supported GigaVUE-FM Migration and Upgrade Paths](#).

Supported Upgrade Paths for GigaVUE-FM

Supported upgrade paths for GigaVUE-FM 5.8 and above:

You can upgrade your GigaVUE-FM instance to any of the subsequent two versions. For example, you can upgrade your GigaVUE-FM 5.8.xx instance to either GigaVUE-FM 5.9.xx or 5.10.xx. If you want to upgrade your GigaVUE-FM 5.8.xx to 6.5.xx, your supported upgrade path is 5.8.xx > 5.10.xx > 5.12.xx > 5.14.xx > 5.16.xx > 6.1.xx > 6.3.xx > 6.5.xx.

NOTES:

- For upgrades to versions 5.11.xx and 5.12.xx, a password change is mandated.
- For all other versions, the password change is mandated only if the current password is a default password.

*Password change is mandated for all passwords during upgrade.

**Password change is only mandated if the current password is using the default password.

GigaVUE-FM Upgrade Rules and Notes

- **Best Practice:** Always upgrade your GigaVUE-FM instance before upgrading the GigaVUE-OS nodes. You can upgrade the attached nodes from the device or from GigaVUE-FM. The latter is recommended. Refer to *“Upgrading Software on a GigaVUE-FM Node or a Cluster from GigaVUE-FM”* in the *GigaVUE Fabric Management Guide*.

- **If upgrading from GigaVUE-FM versions lower than 5.10.xx:** You cannot directly upgrade your GigaVUE-FM instance to release 5.10.00 from a release prior to 5.8.xx. If your current version of GigaVUE-FM is 5.7.xx or lower and you want to upgrade to software version 6.5.xx, you must first migrate to GigaVUE-FM 5.10.xx and then upgrade to 5.11.xx.

NOTE: For instructions on how to migrate refer to [Migrate GigaVUE-FM](#) in GigaVUE 5.10 Documentation.

- **If upgrading from GigaVUE-FM versions lower than 5.5.00:** While upgrading from any version lower than 5.5.00, an association of more than one VPort to the same GigaSMART group needs to be removed for any existing GTP GigaSMART operation.
- **If upgrading from GigaVUE-FM versions lower than 5.4.00:** Be aware of the minimum memory requirement changes between releases. Earlier releases specified 4GB of memory for the OVA template; whereas versions after 5.4.00 require 8GB and versions after 5.7.00 require 16GB. If the existing virtual or physical hardware running GigaVUE-FM is configured with less memory than required, then increase the amount of memory available to the GigaVUE-FM machine. Refer to GigaVUE-FM Memory and CPU Requirements in the *GigaVUE Release Notes* for additional details.

Upgrade GigaVUE-FM from the GigaVUE-FM CLI

The following steps describe how to upgrade an existing GigaVUE-FM deployment to the current release.

1. Verify that only three images are present on the GigaVUE-FM server.
2. Download the new image into GigaVUE-FM using either HTTP, HTTPS, FTP, SCP, or SFTP.
3. Install the new image.
4. Change boot partition.
5. Upgrade GigaVUE-VM (Optional).

Notes:

- It is important that you must be a user with `fm_super_admin` role when upgrading the image on the existing GigaVUE-FM.
- GigaVUE-FM backup and restore files use a text based format; binary backups or restore on physical nodes are not supported. For binary backups, you must use the CLI commands rather than GigaVUE-FM. For more information about the CLI commands, refer to the *GigaVUE-OS CLI Reference Guide*.
- In your commands use the actual file names of the image(s) you are fetching, managing, or deploying.

Step 1: Verify that only three images are present on GigaVUE-FM server

1. To begin an upgrade, open a SSH session and log into GigaVUE-FM.
2. Check the number of images currently available for installation with the following command from the GigaVUE-FM CLI:

```
$ fmctl image list
```

Important: If there are three images listed in the **Images available to be installed** section of the **fmctl image** list output, Gigamon recommends you to delete existing older images. GigaVUE-FM will display a warning if you attempt to fetch a fourth image.

3. To delete an existing image from the server use the following command:

```
$ fmctl image delete <Filename>
```

4. Go to [Step 2: Fetch the latest release of GigaVUE-FM](#).

Step 2: Fetch the latest release of GigaVUE-FM

Gigamon provides an FTP site where the new release image file resides. To fetch the latest release, do the following:

1. Locate the image file for the new release.
2. Copy the image to your file server.
3. Use the **fmctl image fetch** command to retrieve the software image from your file server. The CLI shows you the progress of the image fetch with a series of hash marks, returning you to the system prompt when complete.

NOTE: The **image fetch** command supports the use of HTTP, HTTPS, FTP, SCP, or SFTP for the transfer of images. The examples are provided to show the syntax only. In your commands, use your actual login credentials and the actual name of the image file you wish to fetch.

- a. The following command uses SCP to retrieve the **gigamon-gigavue-fm-6.5 image** image from the image server with the IP address using login and password.

```
fmctl image fetch <download URI> [<filename>]
```

```
$ fmctl image fetch scp://user:password@<IP address>/gigamon-gigavue-fm-6.5.img
```

- b. The following command uses FTP to retrieve the same image using login and password.

```
$ fmctl image fetch ftp://user:password@<IP address>/gigamon-gigavue-fm-6.5.img
```

4. Go to [Step 3: Install the latest release of the GigaVUE-FM](#).

Step 3: Install the latest release of the GigaVUE-FM

Use the **image install** command to install the downloaded image file. When running the following command, the process will first verify that the filename used for the image is suitable for installation prior to installing the image. For example, to install the image downloaded in the previous step and provide the location for boot location for installation.

To check current boot location:

```
$ fmctl image show
```

This command lists the current boot partition, which can be 1 or 2. Use 2 if the current partition is 1 and vice e versa.

```
$fmctl image install <Filename> <Boot location>
```

Step 4: Change the boot partition

Set the image you just installed to boot next with the following command. This ensures that at the next boot the latest image will be picked up.

```
$ fmctl image boot next
```

GigaVUE-FM will reboot with the next boot image and GigaVUE-FM will be upgraded.

Step 5: Upgrade GigaVUE-VM (Optional)

After upgrading GigaVUE-FM, you must also upgrade any deployed GigaVUE-VM. Otherwise, maps may not work and the GigaVUE-VM will be unreachable. For information about upgrading GigaVUE-VM, refer to the “*Bulk Upgrading GigaVUE-VM Nodes*” section in the *GigaVUE Cloud Suite Deployment Guide - VMware*.

Upgrade GigaVUE-FM from the UI

This section describes the steps to upgrade GigaVUE-FM from the UI. You can upgrade by using an image that is located on an external image server, or you can use GigaVUE-FM as the image server.

IMPORTANT: After upgrading GigaVUE-FM, it is recommended to clear the cache and refresh the browser to avoid any potential browser issues.

Keep in mind the following rules and notes before you upgrade GigaVUE-FM from the UI:

- When using the GigaVUE-FM UI to upgrade GigaVUE-FM, you can only upgrade to the currently available version or to the next version. You cannot downgrade.

- When using the Firefox browser, clear the cache before upgrading to prevent issues with the browser.
- When upgrading GigaVUE-FM to the latest image file, the upgrade operation will fail if GigaVUE-FM already has three image files. Delete the unused image files before proceeding to download a new image file.

NOTE: You can enable auto-purge of GigaVUE-FM images using an API. Contact Gigamon Technical Support for assistance.

- Starting from software version 5.15.00, subsequent GigaVUE-FM upgrade operation to higher versions deletes the upgraded GigaVUE-FM image file irrespective of the completion status. For example, when upgrading from 5.15.00 to 5.16.00, irrespective of whether the upgrade process fails or succeeds, GigaVUE-FM deletes the 5.16.00 image file at the end of the upgrade process.


Upgrade from External Image Server

This section provides the steps for upgrading the GigaVUE-FM from an image stored on an external server. The image can be transferred from the server to the GigaVUE-FM using SCP file protocol.

To upgrade with an image stored on an external image server, do the following:

1. Upload the image to the external image server to make it available to GigaVUE-FM.
To obtain software images, register on the [Gigamon Customer Portal](#) and download the software.
2. Add the image server to GigaVUE-FM. This stores the credentials, image file name, and IP address of the server on GigaVUE-FM.

To add the image server:

- a. On the left navigation pane, click .
- b. Select **System** on the left navigation panel and go to **Images > External Servers**. The External Servers page appears.
- c. Click **Add**. The Add External Server page appears.
- d. On the Images Server page, specify the following:
 - An alias to help identify the image server.
 - The host IP address of the server.
 - The protocol to use for the download: SCP.
 - The user name and password.
- e. Click **Save**.

The External Server page displays the newly added external server. From the **Admin** drop-down list in the top right corner of the window, select **Upgrade** to open the FM Image Upgrade page as shown in the following figure.

Software Upgrade

Image File

Select the file server where you have uploaded the image file.



Image Server: 

Image File Path:

To monitor the progress and status of the upgrade, click  “GigaVUE Administration Guide”.

3. On the FM Image Upgrade page, click on the Image Server field and select the server added in [Step 2](#).
4. In the Image File Path, enter the image path and filename on the external file server.
5. Upgrade any deployed GigaVUE-FM-VMs.

After upgrading GigaVUE-FM, you must also upgrade any deployed GigaVUE-FM-VMs. Otherwise, maps may not work and the GigaVUE-FM-VMs will be unreachable. For information about upgrading GigaVUE-FM-VM, refer to the “*Bulk Upgrading GigaVUE-VM Nodes*” section in the *GigaVUE Cloud Suite Deployment Guide - VMware*.

Upgrade with GigaVUE-FM as the Image Server

This section provides the steps for upgrading GigaVUE-FM when GigaVUE-FM is used as the file server instead of an external server.


Upgrading from GigaVUE-FM 5.6.01 to 5.7.xx.00 or 5.7.01 via an internal image will not work because internal server storage does not function during the upgrade procedure. Alternatively, you can upgrade using an external image server or the GigaVUE-FM CLI or you can use the GigaVUE-FM internal storage to store the GigaVUE-FM image, and point to it as if it were an external server as follows :

1. Add the GigaVUE-FM 5.7 image under the GigaVUE-FM internal image server (/config/gigamon/imagesRepo).
2. Configure the GigaVUE-FM external server with the GigaVUE-FM IP address.
3. Initiate the upgrade process, select External Image Server, and then specify the path to the GigaVUE-FM Image file that you added in step 1 (/config/gigamon/imagesRepo/fma5700.img).

To upgrade a GigaVUE-FM using internal image files, do the following:

1. Download the images from the Gigamon website and place them where they can be available for uploading to GigaVUE-FM.

To obtain software images, register on the [Gigamon Customer Portal](#) and download the software.

2. Upload the images file to GigaVUE-FM.
 - a. On the left navigation pane, click  and select to **System > Images > Internal Image Files**.
 - b. On the Internal Image File page, click **Upload**.
 - c. Click **Browse** to locate the image file.
 - d. Click **OK** to upload the file. The page displays the progress of the upload.

After the upload completes, you can see the GigaVUE-FM image to use for the upgrade on the Internal Images Files page.

3. Click the **Admin** drop-down list on the top right of the window and select **Upgrade**.
4. On the FM Image Upgrade page, click in the **Image Server** field and select **Internal Image Server**.

Software Upgrade

Image File

Select the file server where you have uploaded the image file.

Image Server: ▾

Version: ▾


Image File:

- From the **Version** drop-down list, select the version to which you are upgrading.

NOTE: You can only upgrade to another instance of the current version or the immediate next version. Downgrading to a lower version is not supported through the UI.

- Click **Upgrade**.

NOTE: When you change the IP address of the GigaVUE-FM instance using the jump-start configuration, the internal database and the in-memory caches of the GigaVUE-FM instance are not updated. The Database continues to have the IP address of the old GigaVUE-FM, and the image upgrade using the internal server option does not work. To fix this, you must restart the GigaVUE-FM instance after upgrade.

On the left navigation pane, click  , to monitor the progress and status of the upgrade and select **Events** on the left navigation pane. Also, email notifications are sent if email notifications have been configured.

Post-Upgrade Notes

Intent Based Orchestration (IBO): IBO Policies are removed when upgrading from any pre-5.11 version of GigaVUE-FM to version 5.11.00 or above. You must recreate the IBO Policies after upgrading to 5.11.00 or above. However if you have upgraded your GigaVUE-FM to 5.15.00 or above, the IBO policies will be retained. Refer to the "Orchestrated Configurations" section in the *GigaVUE Fabric Management Guide* for more details on how to create policy.

Storage Management: The time period specified for the storage management settings will be configured to the default values when upgrading to GigaVUE-FM v5.11.xx. After completing the upgrade, you must reconfigure the time period to the required values.

Remember to upgrade your GigaVUE-VM deployments: When upgrading GigaVUE-FM, you must also upgrade your GigaVUE-VM deployments. GigaVUE-FM and GigaVUE-VM must be in the same software version. For the steps to upgrade GigaVUE-VM, refer to the “*Bulk Upgrading GigaVUE-VM Nodes*” section in the *GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide*.

Tags Applied to Resources: After you upgrade to software version 5.11.0.0, duplicate tag values will not get associated to nodes and ports while adding and removing nodes from the clusters. However, the existing duplicate tags on the resources do not get cleaned up as part of the upgrade. You must run the following script (bundled with 5.11) to remove the duplicate tags of nodes/clusters and ports.

Script name: `duplicate_tags_removal`.

NOTE: It is recommended that a sudo privileged user runs this script. The default admin user is a sudo privileged user.

To run the script:

1. SSH to GigaVUE-FM.
2. Execute `sudo duplicate_tags_removal`.
3. You can see the logs in the console.

Application Intelligence Session: After the GigaVUE-FM upgrades to software version 6.4.00, your existing application intelligence session's export interval will be updated to five minutes. After upgrading to 6.4.00, you will lose the complete historical application visualization data except for the last 24 hours. Refer to "View the Application Intelligence Dashboard" section in the GigaVUE Fabric Management Guide for more details.

Important: Clear the browser cache before logging in to GigaVUE-FM.

Upgrade GigaVUE-FM in Azure

This chapter describes how to upgrade the GigaVUE-FM instance deployed on Azure.

Refer to the following sections for details:

- [Upgrade Options in Azure](#)
- [Upgrade GigaVUE-FM from the UI](#)
- [Upgrade GigaVUE-FM using Snapshot in Azure](#)

Upgrade Options in Azure

You can upgrade the GigaVUE-FM instance using one of the following options:

- [Upgrade GigaVUE-FM from the UI](#)
- [Upgrade GigaVUE-FM using Snapshot in Azure](#)

Upgrade GigaVUE-FM from the UI

NOTE: If GigaVUE-FM is deployed in Azure, then upgrading GigaVUE-FM from the UI is supported only when upgrading GigaVUE-FM to a version greater than 6.5.00.

This section describes the steps to upgrade GigaVUE-FM from the UI. You can upgrade by using an image that is located on an external image server, or you can use GigaVUE-FM as the image server.

IMPORTANT: After upgrading GigaVUE-FM, it is recommended to clear the cache and refresh the browser to avoid any potential browser issues.

Keep in mind the following rules and notes before you upgrade GigaVUE-FM from the UI:

- When using the GigaVUE-FM UI to upgrade GigaVUE-FM, you can only upgrade to the currently available version or to the next version. You cannot downgrade.
- When using the Firefox browser, clear the cache before upgrading to prevent issues with the browser.
- When upgrading GigaVUE-FM to the latest image file, the upgrade operation will fail if GigaVUE-FM already has three image files. Delete the unused image files before proceeding to download a new image file.

NOTE: You can enable auto-purge of GigaVUE-FM images using an API. Contact Gigamon Technical Support for assistance.

- Starting from software version 5.15.00, subsequent GigaVUE-FM upgrade operation to higher versions deletes the upgraded GigaVUE-FM image file irrespective of the completion status. For example, when upgrading from 5.15.00 to 5.16.00, irrespective of whether the upgrade process fails or succeeds, GigaVUE-FM deletes the 5.16.00 image file at the end of the upgrade process.


Upgrade from External Image Server

This section provides the steps for upgrading the GigaVUE-FM from an image stored on an external server. The image can be transferred from the server to the GigaVUE-FM using SCP file protocol.

To upgrade with an image stored on an external image server, do the following:

1. Upload the image to the external image server to make it available to GigaVUE-FM.
To obtain software images, register on the [Gigamon Customer Portal](#) and download the software.
2. Add the image server to GigaVUE-FM. This stores the credentials, image file name, and IP address of the server on GigaVUE-FM.

To add the image server:

- a. On the left navigation pane, click .
- b. Select **System** on the left navigation panel and go to **Images > External Servers**.
The External Servers page appears.
- c. Click **Add**. The Add External Server page appears.
- d. On the Images Server page, specify the following:
 - An alias to help identify the image server.
 - The host IP address of the server.
 - The protocol to use for the download: SCP.
 - The user name and password.
- e. Click **Save**.

The External Server page displays the newly added external server. From the **Admin** drop-down list in the top right corner of the window, select **Upgrade** to open the FM Image Upgrade page as shown in the following figure.


Software Upgrade

Image File

Select the file server where you have uploaded the image file.

Image Server:

Image File Path:

To monitor the progress and status of the upgrade, click  "GigaVUE Administration Guide".

3. On the FM Image Upgrade page, click on the Image Server field and select the server added in [Step 2](#).
4. In the Image File Path, enter the image path and filename on the external file server.
5. Upgrade any deployed GigaVUE-FM-VMs.

After upgrading GigaVUE-FM, you must also upgrade any deployed GigaVUE-FM-VMs. Otherwise, maps may not work and the GigaVUE-FM-VMs will be unreachable. For information about upgrading GigaVUE-FM-VM, refer to the “*Bulk Upgrading GigaVUE-VM Nodes*” section in the *GigaVUE Cloud Suite Deployment Guide - VMware*.

Upgrade with GigaVUE-FM as the Image Server

This section provides the steps for upgrading GigaVUE-FM when GigaVUE-FM is used as the file server instead of an external server.


Upgrading from GigaVUE-FM 5.6.01 to 5.7.xx.00 or 5.7.01 via an internal image will not work because internal server storage does not function during the upgrade procedure. Alternatively, you can upgrade using an external image server or the GigaVUE-FM CLI or you can use the GigaVUE-FM internal storage to store the GigaVUE-FM image, and point to it as if it were an external server as follows :

1. Add the GigaVUE-FM 5.7 image under the GigaVUE-FM internal image server (/config/gigamon/imagesRepo).
2. Configure the GigaVUE-FM external server with the GigaVUE-FM IP address.
3. Initiate the upgrade process, select External Image Server, and then specify the path to the GigaVUE-FM Image file that you added in step 1 (/config/gigamon/imagesRepo/fma5700.img).

To upgrade a GigaVUE-FM using internal image files, do the following:

1. Download the images from the Gigamon website and place them where they can be available for uploading to GigaVUE-FM.

To obtain software images, register on the [Gigamon Customer Portal](#) and download the software.

2. Upload the images file to GigaVUE-FM.
 - a. On the left navigation pane, click  and select to **System > Images > Internal Image Files**.
 - b. On the Internal Image File page, click **Upload**.
 - c. Click **Browse** to locate the image file.
 - d. Click **OK** to upload the file. The page displays the progress of the upload.

After the upload completes, you can see the GigaVUE-FM image to use for the upgrade on the Internal Images Files page.

3. Click the **Admin** drop-down list on the top right of the window and select **Upgrade**.
4. On the FM Image Upgrade page, click in the **Image Server** field and select **Internal Image Server**.

Software Upgrade

Image File

Select the file server where you have uploaded the image file.

Image Server:

Version:


Image File:

5. From the **Version** drop-down list, select the version to which you are upgrading.

NOTE: You can only upgrade to another instance of the current version or the immediate next version. Downgrading to a lower version is not supported through the UI.

6. Click **Upgrade**.

NOTE: When you change the IP address of the GigaVUE-FM instance using the jump-start configuration, the internal database and the in-memory caches of the GigaVUE-FM instance are not updated. The Database continues to have the IP address of the old GigaVUE-FM, and the image upgrade using the internal server option does not work. To fix this, you must restart the GigaVUE-FM instance after upgrade.

On the left navigation pane, click  , to monitor the progress and status of the upgrade and select **Events** on the left navigation pane. Also, email notifications are sent if email notifications have been configured.

Upgrade GigaVUE-FM using Snapshot in Azure

This chapter describes how to upgrade the GigaVUE-FM instance deployed on Azure using snapshot:

- Upgrade the GigaVUE-FM using the Snapshot method
- Stop GigaVUE-FM FM Instance
- Create Snapshot of the GigaVUE-FM Instance
- Upgrade GigaVUE-FM Instance

Upgrade the GigaVUE-FM using the Snapshot method

To upgrade the GigaVUE-FM instance successfully, you must perform the following steps:

1. Stop the existing version of the GigaVUE-FM instance.
2. Create a snapshot of the data disk of the current version of the GigaVUE-FM instance.
3. Deploy the latest version of the GigaVUE-FM instance from the marketplace.
4. In the disk tab, select **Create and attach a new disk**, and attach the Snapshot.
5. Launch the GigaVUE-FM and wait for it to initialize.

Stop GigaVUE-FM FM Instance

Before upgrading the GigaVUE-FM instance, the existing version of the GigaVUE-FM instance must be stopped.

NOTE: Do not terminate the GigaVUE-FM instance.

To stop the GigaVUE-FM instance:

1. Login to the Azure portal and select the **Virtual Machines** that have the GigaVUE-FM deployed
2. Click the Stop button in the portal to shutdown GigaVUE-FM
3. Wait for few seconds for Azure to completely stop the virtual machine

Create Snapshot of the GigaVUE-FM Instance

You must create a snapshot of the blob of the existing version of the GigaVUE-FM instance. Snapshots capture data that are written to your Azure Virtual Disks at the time the snapshot is taken. This excludes any data that are cached by any applications or the operating system.

To create a snapshot:

1. Click the Data Disk link in the existing version of the GigaVUE-FM properties in the Azure portal.
2. Click Create Snapshot in the screen. The Create Snapshot (using SSD) dialog box is displayed.

3. In the Create Snapshot dialog box, enter the following information:

Table 1: Fields for Creating a Snapshot

Field	Description
Name	The name of the snapshot
Subscription	Subscription ID
Resource-group	The name of the resource group
Location	Location of the resource group
Account-type	Select the account type to use to store the snapshot.

4. Click Create. It will take several minutes for the snapshot to be created.

Upgrade GigaVUE-FM Instance

To upgrade the GigaVUE-FM instance:

1. In the Azure Marketplace, search for the GigaVUE-FM.
2. Select the latest version GigaVUE-FM of and then click **Create**.
3. On the Basic page, configure basic information for the GigaVUE-FM and then click **Next**.
4. In the disk tab, select **Create and attach a new disk**.
5. In the **Create a new disk page**, enter the name.
6. Select the **Source type** as Snapshot and then select the **Snapshot**. For more information, see [Create Snapshot of the GigaVUE-FM Instance](#)
7. Enable the option, **Delete disk with VM** and click **Ok**
8. On the **Networking Page**, configure the network settings and then click **Next**.
9. On the **Management page**, enable System assigned managed Identity and then click **Next**.
10. Configure the **Advanced page** as required and then click **Review and Create**.

NOTE: After the upgrade, there will be a total of three disks attached to GigaVUE-FM. One system disk, one data disk, and a snapshot of the old GigaVUE-FM will be attached to the upgraded GigaVUE-FM.

Upgrade GigaVUE-FM in AWS

This chapter describes how to upgrade the GigaVUE-FM instance deployed on AWS.

Refer to the following sections for details:

- [Upgrade Options in AWS](#)
- [Upgrade GigaVUE-FM from the UI](#)
- [Upgrade GigaVUE-FM using Snapshot in AWS](#)

Upgrade Options in AWS

You can upgrade the GigaVUE-FM instance using one of the following options:

- [Upgrade GigaVUE-FM from the UI](#)
- [Upgrade GigaVUE-FM using Snapshot in AWS](#)

Upgrade GigaVUE-FM from the UI

NOTE: If GigaVUE-FM is deployed in AWS, then upgrading GigaVUE-FM from the UI is supported only when upgrading GigaVUE-FM to a version greater than 6.5.00.

This section describes the steps to upgrade GigaVUE-FM from the UI. You can upgrade by using an image that is located on an external image server, or you can use GigaVUE-FM as the image server.

IMPORTANT: After upgrading GigaVUE-FM, it is recommended to clear the cache and refresh the browser to avoid any potential browser issues.

Keep in mind the following rules and notes before you upgrade GigaVUE-FM from the UI:

- When using the GigaVUE-FM UI to upgrade GigaVUE-FM, you can only upgrade to the currently available version or to the next version. You cannot downgrade.
- When using the Firefox browser, clear the cache before upgrading to prevent issues with the browser.
- When upgrading GigaVUE-FM to the latest image file, the upgrade operation will fail if GigaVUE-FM already has three image files. Delete the unused image files before proceeding to download a new image file.

NOTE: You can enable auto-purge of GigaVUE-FM images using an API. Contact Gigamon Technical Support for assistance.

- Starting from software version 5.15.00, subsequent GigaVUE-FM upgrade operation to higher versions deletes the upgraded GigaVUE-FM image file irrespective of the completion status. For example, when upgrading from 5.15.00 to 5.16.00, irrespective of whether the upgrade process fails or succeeds, GigaVUE-FM deletes the 5.16.00 image file at the end of the upgrade process.


Upgrade from External Image Server

This section provides the steps for upgrading the GigaVUE-FM from an image stored on an external server. The image can be transferred from the server to the GigaVUE-FM using SCP file protocol.

To upgrade with an image stored on an external image server, do the following:

1. Upload the image to the external image server to make it available to GigaVUE-FM.
To obtain software images, register on the [Gigamon Customer Portal](#) and download the software.
2. Add the image server to GigaVUE-FM. This stores the credentials, image file name, and IP address of the server on GigaVUE-FM.

To add the image server:

- a. On the left navigation pane, click .
- b. Select **System** on the left navigation panel and go to **Images > External Servers**. The External Servers page appears.
- c. Click **Add**. The Add External Server page appears.
- d. On the Images Server page, specify the following:
 - An alias to help identify the image server.
 - The host IP address of the server.
 - The protocol to use for the download: SCP.
 - The user name and password.
- e. Click **Save**.

The External Server page displays the newly added external server. From the **Admin** drop-down list in the top right corner of the window, select **Upgrade** to open the FM Image Upgrade page as shown in the following figure.

Software Upgrade

Image File

Select the file server where you have uploaded the image file.



Image Server: 

Image File Path:

To monitor the progress and status of the upgrade, click  “GigaVUE Administration Guide”.

3. On the FM Image Upgrade page, click on the Image Server field and select the server added in [Step 2](#).
4. In the Image File Path, enter the image path and filename on the external file server.
5. Upgrade any deployed GigaVUE-FM-VMs.

After upgrading GigaVUE-FM, you must also upgrade any deployed GigaVUE-FM-VMs. Otherwise, maps may not work and the GigaVUE-FM-VMs will be unreachable. For information about upgrading GigaVUE-FM-VM, refer to the “*Bulk Upgrading GigaVUE-VM Nodes*” section in the *GigaVUE Cloud Suite Deployment Guide - VMware*.

Upgrade with GigaVUE-FM as the Image Server

This section provides the steps for upgrading GigaVUE-FM when GigaVUE-FM is used as the file server instead of an external server.

Upgrading from GigaVUE-FM 5.6.01 to 5.7.xx.00 or 5.7.01 via an internal image will not work because internal server storage does not function during the upgrade procedure. Alternatively, you can upgrade using an external image server or the GigaVUE-FM CLI or you can use the GigaVUE-FM internal storage to store the GigaVUE-FM image, and point to it as if it were an external server as follows :


1. Add the GigaVUE-FM 5.7 image under the GigaVUE-FM internal image server (/config/gigamon/imagesRepo).
2. Configure the GigaVUE-FM external server with the GigaVUE-FM IP address.

3. Initiate the upgrade process, select External Image Server, and then specify the path to the GigaVUE-FM Image file that you added in step 1 (/config/gigamon/imagesRepo/fma5700.img).

To upgrade a GigaVUE-FM using internal image files, do the following:

1. Download the images from the Gigamon website and place them where they can be available for uploading to GigaVUE-FM.

To obtain software images, register on the [Gigamon Customer Portal](#) and download the software.

2. Upload the images file to GigaVUE-FM.
 - a. On the left navigation pane, click  and select to **System > Images > Internal Image Files**.
 - b. On the Internal Image File page, click **Upload**.
 - c. Click **Browse** to locate the image file.
 - d. Click **OK** to upload the file. The page displays the progress of the upload.

After the upload completes, you can see the GigaVUE-FM image to use for the upgrade on the Internal Images Files page.

3. Click the **Admin** drop-down list on the top right of the window and select **Upgrade**.
4. On the FM Image Upgrade page, click in the **Image Server** field and select **Internal Image Server**.

Software Upgrade

Image File

Select the file server where you have uploaded the image file.

Image Server:

Version:


Image File:

5. From the **Version** drop-down list, select the version to which you are upgrading.

NOTE: You can only upgrade to another instance of the current version or the immediate next version. Downgrading to a lower version is not supported through the UI.

6. Click **Upgrade**.

NOTE: When you change the IP address of the GigaVUE-FM instance using the jump-start configuration, the internal database and the in-memory caches of the GigaVUE-FM instance are not updated. The Database continues to have the IP address of the old GigaVUE-FM, and the image upgrade using the internal server option does not work. To fix this, you must restart the GigaVUE-FM instance after upgrade.

On the left navigation pane, click  , to monitor the progress and status of the upgrade and select **Events** on the left navigation pane. Also, email notifications are sent if email notifications have been configured.

Upgrade GigaVUE-FM using Snapshot in AWS

This chapter describes how to upgrade the GigaVUE-FM instance deployed on AWS using snapshot:

- [At a Glance](#)
- [Stop GigaVUE-FM FM Instance](#)
- [Create Snapshot of the GigaVUE-FM Instance](#)
- [Upgrade GigaVUE-FM Instance](#)

At a Glance

To upgrade the GigaVUE-FM instance successfully, you must perform the following steps:

Step 1: Stop the existing version of the GigaVUE-FM instance.

Step 2: Create a snapshot of the second disk (dev/sdb) of the FM instance.

Step 3: Make a note of the snapshot ID.

Step 4: Launch the latest version of the GigaVUE-FM instance. While launching the latest version, enter the snapshot ID of the old version of the GigaVUE-FM instance in **Add Storage** > **Add New Volume**.

Step 5: Complete the launch.

Step 6: Verify if the data from the previous GigaVUE-FM instance is restored in the new instance.

Step 7: Terminate the old FM instance.

Stop GigaVUE-FM Instance

Before upgrading the GigaVUE-FM instance, the existing version of the GigaVUE-FM instance must be stopped.

NOTE: Do not terminate the GigaVUE-FM instance.

To stop the GigaVUE-FM instance:

1. Login to the AWS account and select **Services > EC2**.
2. In the left navigation pane, select **Instances**.
3. In the search field, enter the name of the existing GigaVUE-FM instance and select the Instance ID.

NOTE: If the instance ID is the password for logging in to the existing GigaVUE-FM, make note of this instance ID. This instance ID will be used as the password for logging in to the upgraded GigaVUE-FM as well. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

4. Go to **Actions > Instance State > Stop**.

Create Snapshot of the GigaVUE-FM Instance

You must create a snapshot of the volume of the existing version (`dev/sdb`) of the GigaVUE-FM instance. Snapshots capture data that are written to your Amazon EBS volume at the time the snapshot is taken. This excludes any data that are cached by any applications or the operating system.

To create a snapshot:

1. Select the GigaVUE-FM instance and click the **Description** tab.
2. Scroll down and locate Block Devices.
3. Click the `/dev/sdb` link. The Block Device dialog box is displayed with the volume ID link.
4. In the Block Device dialog box, click the volume ID link. The Volumes page is displayed.
5. Click **Actions** and select **Create Snapshot**.
The Create Snapshot dialog box is displayed.
6. In the Create Snapshot dialog box, enter the following information:

Table 1: Fields for Creating a Snapshot

Field	Description
Name	The name of the snapshot.
Description	The description of the snapshot.

7. Click **Create**. It will take several minutes for the snapshot to be created.

NOTE: Make a note of the snapshot ID. This snapshot ID will be used to find the snapshot and add the volume while upgrading the GigaVUE-FM instance.

Upgrade GigaVUE-FM Instance

While upgrading the GigaVUE-FM instance, the Amazon EBS volume must be restored with the data from the snapshot that is created in [Create Snapshot of the GigaVUE-FM Instance](#).

To upgrade the GigaVUE-FM instance:

1. Select **Services > EC2**.
2. Click **Launch Instance** and go to **AWS Marketplace** or **Community AMIs**.
3. Search for **Gigamon**, locate the latest version of the GigaVUE-FM AMI, and click **Select**.
4. Choose the Instance Type. The recommended instance type is **m4.xlarge**.

NOTE: Do not select the t2 instance types as they are not supported.

5. Click **Next: Configure Instance Details**.
6. Enter the following information.
 - o **Network**— Select the VPC where you want to launch the AMI.
 - o **Subnet**— Select the management subnet that the instance will use after launch. (Required)
 - o **Auto-assign Public IP**— Select **Enable**.
 - o **IAM role**—Select an existing IAM role to associate with the instance. Refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide*.
7. Click **Configure storage** and then click **Advanced**.
8. Select **Volume 2** and then select the Snapshot that you created in [Create Snapshot of the GigaVUE-FM Instance](#).
9. Click **Next: Tag Instance**, and then add a key-value pair to identify the instance.

10. Click **Next: Add Security Group**. Click the **Select an existing security group** check box if the security group is already created. Otherwise, select the **Create a new security group** check box and click **Add Rule**. For more information on creating a security group, refer to the [Security Group](#).
11. Click **Review and Launch**. Review the instance launch details and click **Launch**.
12. Select the SSH key pair, check the acknowledgment check box, and click **Launch Instances**.
13. It will take several minutes for the instance to initialize. After the initialization is completed, verify the instance through the Web interface as follows:
 - a. Find the instance and expand the page in the **Descriptions** tab to view the instance information, if necessary.
 - b. Copy the Public DNS value and paste the value into a new browser window or tab.
 - c. Copy the Instance ID of the previous version of the GigaVUE-FM. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

NOTE: Do not have multiple versions of GigaVUE-FM instances monitoring the same AWS connection.

Launch the new version of the GigaVUE-FM instance. Verify if the data from the previous GigaVUE-FM instance is restored in the new instance. Once the data is verified, terminate the old version of the GigaVUE-FM instance.

Upgrade GigaVUE Fabric Components

This chapter describes how to upgrade different fabric components like GigaVUE V Series Node, GigaVUE V Series proxy, UCT-V Controller, and UCT-V. For more detailed information about UCT-V, UCT-V Controller, GigaVUE V Series Proxy and Node Version refer [GigaVUE-FM Version Compatibility Matrix](#).

Refer to the following topics for more detailed information on how to upgrade the fabric components using GigaVUE-FM for the respective cloud platforms:

- [Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS](#)
- [Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure](#)
- [Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack](#)
- [Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi](#)
- [Upgrade GigaVUE V Series Node in GigaVUE-FM \(NSX-T\)](#)

Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes. For more detailed information about UCT-V, UCT-V Controller, GigaVUE V Series Proxy and Node Version refer [GigaVUE-FM Version Compatibility Matrix](#).

Refer to the following topic for more information:

- [Prerequisite](#)
- [Upgrade UCT-V Controller](#)
- [Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy](#)

Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series Nodes, you must upgrade GigaVUE-FM to software version 5.13 or above.

Upgrade UCT-V Controller

NOTE: UCT-V Controllers cannot be upgraded. Only a new version that is compatible with the UCT-V's version can be added or removed in the **AWS Fabric Launch Configuration** page.

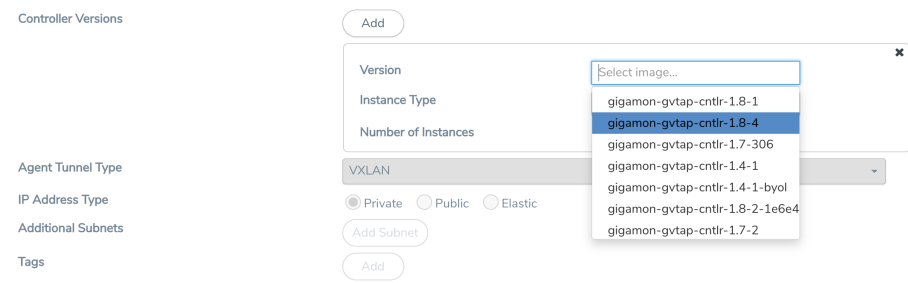
To change the UCT-V Controller version follow the steps given below:

To change UCT-V Controller version between different major versions

NOTE: You can only add UCT-V Controllers which has different major versions. For example, you can only add UCT-V Controller version 1.8-x if your existing version is 1.7-x.

- Under **Controller Versions**, click **Add**.
- From the **Version** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.
- From the **Instance Type** drop-down list, select a size for the UCT-V Controller.

- d. In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.



You cannot change the IP Address Type and the Additional Subnets details, provided at the time of UCT-V Controller configuration.

After installing the new version of UCT-V Controller, follow the steps given below:

1. Install UCT-V with the version same as the UCT-V Controller.
2. Delete the UCT-V Controller with older version.

To change UCT-V Controller version with in the same major version

This is only applicable if you wish to change your UCT-V Controller version from one minor version to another within the same major version. For example, from 1.8-2 to 1.8-3.

- a. From the **Version** drop-down list, select a UCT-V Controller image with in the same major version.
- b. Specify the **Number of Instances**. The minimum number you can specify is 1.
- c. Select the **Subnet** from the drop-down.



- You cannot modify the rest of the fields.
- After installing the new version of UCT-V Controller with the same version.

Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

GigaVUE-FM lets you upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes at a time.

There are two ways to upgrade the GigaVUE V Series Proxy and Nodes. You can:

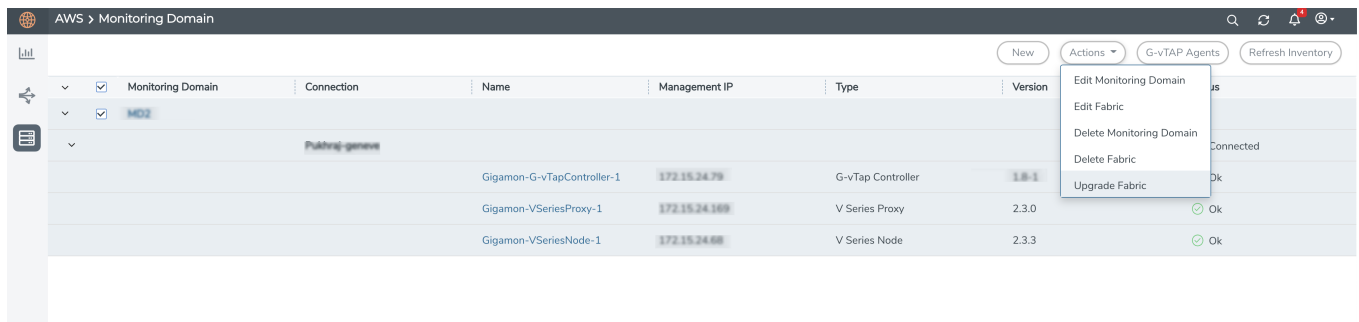
- Launch and replace the complete set of nodes and proxy at a time.
For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VPC, you can upgrade all of them at once. First, the new version of GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes are launched. Then, the old version of V Series Proxy and Nodes are deleted from the VPC.

NOTES:

- When the new version of nodes and proxy are launched, the old version is not deleted by GigaVUE-FM until the new version of node and proxy is launched and the status is changed to **Ok**. Make sure that the instance type of the node and proxy selected during the configuration can accommodate the total number of new and old fabric nodes present in the VPC. If the instance type cannot support so many Virtual Machines, you can choose to upgrade the fabric nodes in multiple batches.
- If there is an error while upgrading the complete set of proxy and nodes present in the VPC, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
- Prior to upgrading the GigaVUE V Series Proxy and Nodes, you must ensure that the required number of free addresses are available in the respective subnets. Otherwise, the upgrade will fail.
- Launch and replace the nodes and proxy in multiple batches.
For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

To upgrade the GigaVUE V Series Proxy and GigaVUE V Series Nodes:

1. Go to **Inventory > VIRTUAL > AWS**, and then click **Monitoring Domain**. The Monitoring Domain page appears.
2. On the Monitoring Domain page, select the connection name check box and click **Actions**



3. Select **Upgrade Fabric** from the drop-down list. The Fabric Nodes Upgrade page is displayed.

Fabric Nodes Upgrade

V Series Proxy

Upgrade	<input checked="" type="checkbox"/>
Current Version	2.3.0
Image	<div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px; display: inline-block;">Select an image... ▾</div>
Change Instance Type	<input type="checkbox"/>
Batch Size	<input style="width: 50px;" type="text" value="1"/>

V Series Node

Upgrade	<input checked="" type="checkbox"/>
Current Version	2.3.3
Image	<div style="border: 1px solid #ccc; border-radius: 5px; padding: 2px; display: inline-block;">Select an image... ▾</div>
Change Instance Type	<input type="checkbox"/>
Batch Size	<input style="width: 50px;" type="text" value="1"/>

4. To upgrade the GigaVUE V Series Nodes/Proxy, select the **Upgrade** checkbox.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V Series Proxy/Nodes.
6. Select the **Change Instance Type** checkbox to change the instance type of the nodes/proxy, only if required.
7. To upgrade the GigaVUE V Series Nodes/Proxy, specify the batch size in the **Batch Size** box.

For example, if there are 7 GigaVUE V Series Nodes, you can specify 7 as the batch size and upgrade all of them at once. Alternatively, you can specify 3 as the batch size, and launch and replace 3 V Series Nodes in each batch. In the last batch, the remaining 1 V Series Node is launched.

8. Click **Upgrade**.

The upgrade process takes a while depending on the number of GigaVUE V Series Proxy and Nodes upgrading in your AWS environment. First, the new version of the GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes is launched. Then, the older version of both is deleted from the project. In the V Series Proxy page, click the link under Progress to view the upgrade status.

Once the nodes are upgraded successfully, the monitoring session is re-deployed automatically.

Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V Series Node. For more detailed information about UCT-V Controller, GigaVUE V Series Proxy and Node Version refer [GigaVUE-FM Version Compatibility Matrix](#).

Refer to the following topic for more information:

- [Prerequisite](#)
- [Upgrade UCT-V Controller](#)
- [Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy](#)

Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series Node, you must upgrade GigaVUE-FM to software version 5.13.01 or above.

Upgrade UCT-V Controller

NOTE: UCT-V Controllers cannot be upgraded. Only a new version that is compatible with the UCT-V's version can be added or removed in the **Azure Fabric Launch Configuration** page.

To change the UCT-V Controller version follow the steps given below:

To change UCT-V Controller version between different major versions

NOTE: You can only add UCT-V Controllers which has different major versions. For example, you can only add UCT-V Controller version 1.8-x if your existing version is 1.7-x.

- In the **Azure Fabric Launch Configuration** page, under **Controller Versions**, click **Add**.
- From the **Image** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.
- From the **Size** drop-down list, select a size for the UCT-V Controller. The default size is Standard_B1s.
- In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.

You cannot change the IP Address Type and the Additional Subnets details, provided at the time of UCT-V Controller configuration.

After installing the new version of UCT-V Controller, follow the steps given below:

1. Install UCT-V with the version same as the UCT-V Controller.
2. Delete the UCT-V Controller with older version.

To change UCT-V Controller version with in the same major version:

NOTE: This is only applicable, if you wish to change your UCT-V Controller version from one minor version to another with in the same major version. For example, from 1.8-2 to 1.8-3.

- From the **Image** drop-down list, select a UCT-V Controller image with in the same major version.
- Specify the **Number of Instances**. The minimum number you can specify is 1.
- Select the **Subnet** from the drop-down.



- You cannot modify the rest of the fields.
- After installing the new version of UCT-V Controller, install the UCT-V with the same version.

Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy

GigaVUE-FM lets you upgrade GigaVUE V Series Proxy and GigaVUE V Series Node at a time.

There are multiple ways to upgrade the GigaVUE V Series Proxy and Node. You can:

- Launch and replace the complete set of nodes and proxys at a time.

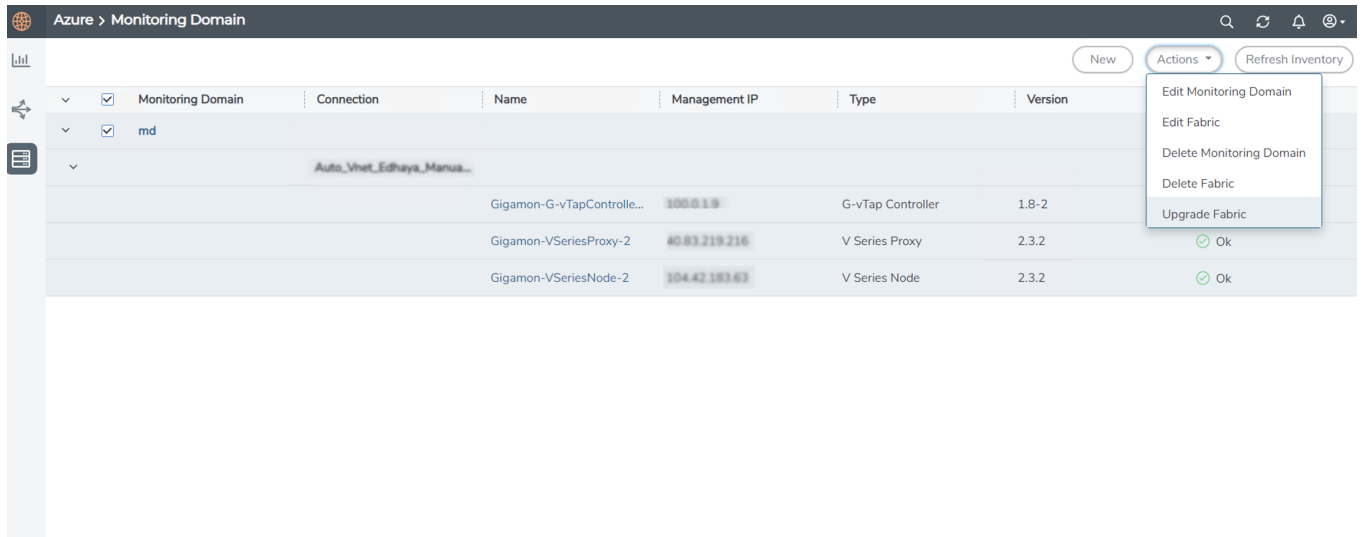
For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VNet, you can upgrade all of them at once. First, the new version of GigaVUE V Series controller is launched. Next, the new version of GigaVUE V Series nodes are launched. Then, the old version of V Series controller and nodes are deleted from the VNet.

NOTES:

- When the new version of node and proxy is launched, the old version still exists in the VNet until they are deleted. Make sure the instance type determined during the configuration can accommodate the total number of new and old instances present in the VNet. If the instance type cannot support so many instances, you can choose to upgrade in multiple batches.
- If there is an error while upgrading the complete set of proxys and nodes present in the VNet, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
- If you have deployed your nodes using Public IP address while creating the monitoring domain, then select the same number of Public IP addresses defined in your Max Instances when upgrading your nodes. Refer to [Create Monitoring Domain](#) for more detailed information.
- Launch and replace the nodes and proxy in multiple batches.
For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

To upgrade the GigaVUE V Series Proxy and GigaVUE V Series Node:

1. Go to **Inventory > VIRTUAL > Azure**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the Monitoring Domain page, select the connection name check box and click **Actions**



3. Select **Upgrade Fabric** from the drop-down list. The Fabric Nodes Upgrade page is displayed.

Fabric Nodes Upgrade

V Series Proxy

Upgrade	<input checked="" type="checkbox"/>
Current Version	2.3.0
Image	gigamon-gigavue-vseries-proxy-2.3.2-284364
Change Size	<input type="checkbox"/>
Batch Size	1

V Series Node

Upgrade	<input checked="" type="checkbox"/>
Current Version	2.3.0
Image	gigamon-gigavue-vseries-node-2.3.2-284421
Change Size	<input type="checkbox"/>
Batch Size	1
Public IPs	104.42.183.54 104.42.183.63

Upgrade Cancel

4. To upgrade the GigaVUE V Series Node/Proxy, select the **Upgrade** checkbox.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V Series Proxy/Nodes.
6. Select the **Change Size** checkbox to change the flavor of the node/proxy, only if required.
7. To upgrade the GigaVUE V Series Node/Proxy, specify the batch size in the **Batch Size** box.

For example, if there are 7 GigaVUE V Series Nodes, you can specify 7 as the batch size and upgrade all of them at once. Alternatively, you can specify 3 as the batch size, and launch and replace 3 V Series nodes in each batch. In the last batch, the remaining 1 V Series node is launched.

8. From the Public IPs drop-down list, select the IP addresses equal to the Max Instances defined when creating a monitoring domain.

NOTE: This is only applicable for nodes deployed using Public IP, when creating a monitoring domain.

9. Click **Upgrade**.

The upgrade process takes a while depending on the number of GigaVUE V Series Proxies and Nodes upgrading in your Azure environment. First, the new version of the GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes is launched. Then, the older version of both is deleted from the project. The monitoring session is deployed automatically.

To view the detailed upgrade status click **Upgrade in progress** or **Upgrade successful**, the **V Series Node Upgrade Status** dialog box appears.

Fabric Nodes Upgrade Status

Monitoring Domain: md

Start Time 2021-10-11 20:58:56

End Time 2021-10-11 21:04:03

Status Fabric upgrade completed successfully

	Proxies	Nodes
Total	1	1
Upgraded	1	1
Upgrading	0	0
Remaining	0	0
Failures	0	0

Clear
Close

- Click **Clear** to delete the monitoring domain upgrade status history of successfully upgraded nodes.

Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes. For more detailed information about UCT-V Controller, GigaVUE V Series Proxy and Node Version refer [GigaVUE-FM Version Compatibility Matrix](#).

Refer to the following topic for more information:

- [Prerequisite](#)
- [Upgrade UCT-V Controller](#)

- [Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy](#)

Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series nodes, you must upgrade GigaVUE-FM to software version 5.13. For better performance, Gigamon recommends you to upgrade to the latest version.

Upgrade UCT-V Controller

NOTE: UCT-V Controllers cannot be upgraded. Only a new version that is compatible with the UCT-V's version can be added or removed in the **OpenStack Fabric Launch Configuration** page.

To change the UCT-V Controller version follow the steps given below:

To change UCT-V Controller version between different major versions

NOTE: You can only add UCT-V Controllers which has different major versions. For example, you can only add UCT-V Controller version 1.8-x if your existing version is 1.7-x.

- a. Under **Controller Versions**, click **Add**.
- b. From the **Image** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.
- c. From the **Flavor** drop-down list, select a size for the UCT-V Controller.

- d. In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.

Controller Version(s)	Add
	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> ✕ <p>Image <input type="text" value="Select image..."/></p> <p>Flavor <input type="text" value="Select flavor..."/></p> <p>Number of Instances <input type="text" value="1"/></p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> ✕ <p>Image <input type="text" value="gigamon-gvtap-ovs-cntlr-1.8-2"/></p> <p>Flavor <input type="text" value="m1.small"/></p> <p>Number of Instances <input type="text" value="1"/></p> </div>
Management Network	<div style="border: 1px solid #ccc; padding: 5px;"> <p>IP Address Type <input type="radio"/> Private <input checked="" type="radio"/> Floating</p> <p>Network <input type="text" value="mgmt-test-network"/></p> <p>Floating IPs <input type="text" value="10.115.176.108 ✕"/></p> </div>
Additional Network(s)	Add
Tags	Add

You cannot change the IP Address Type and the Additional Networks details, provided at the time of UCT-V Controller configuration.

After installing the new version of UCT-V Controller, follow the steps given below:

1. Install UCT-V with the version same as the UCT-V Controller.
2. Delete the UCT-V Controller with older version.

To change UCT-V Controller version with in the same major version

NOTE: This is only applicable, if you wish to change your UCT-V Controller version from one minor version to another with in the same major version. For example, from 1.8-2 to 1.8-3.

- a. From the **Image** drop-down list, select a UCT-V Controller image with in the same major version.
- b. Specify the **Number of Instances**. The minimum number you can specify is 1.
- c. Select the **Network** from the drop-down.



- You cannot modify the rest of the fields.
- After installing the new version of UCT-V Controller, install the UCT-V with the same version.

Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

GigaVUE-FM lets you upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes at a time.

There are multiple ways to upgrade the GigaVUE V Series Proxy and nodes. You can:

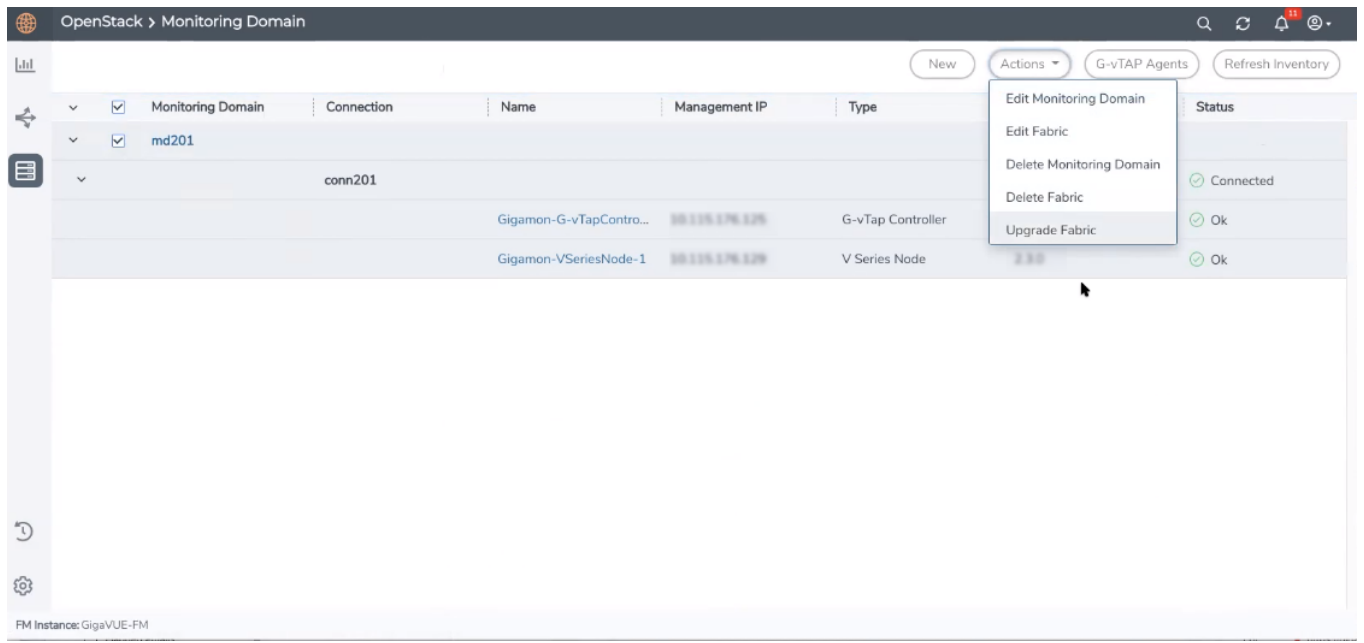
- Launch and replace the complete set of nodes and controllers at a time.
For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series nodes in your project, you can upgrade all of them at once. First, the new version of GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes are launched. Then, the old version of V Series Proxy and nodes are deleted from the project.

NOTES:

- When the new version of nodes and controllers are launched, the old version still exists in the project until they are deleted. Make sure the flavor determined during the configuration can accommodate the total number of new and old fabric nodes present in the project. If the flavor cannot support so many Virtual Machines, you can choose to upgrade in multiple batches.
- If there is an error while upgrading the complete set of controllers and nodes present in the project, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
- Prior to upgrading the GigaVUE V Series Proxy and Nodes, you must ensure that the required number of floating IP addresses are available in the respective subnets. Otherwise, the upgrade will fail.
- Launch and replace the nodes and controllers in multiple batches.
For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

To upgrade the GigaVUE V Series Proxy and GigaVUE V Series Nodes:

1. Go to **Inventory > VIRTUAL > OpenStack**, and then click **Monitoring Domain**. The Monitoring Domain page appears.
2. On the Monitoring Domain page, select the connection name check box and click **Actions**



3. Select **Upgrade Fabric** from the drop-down list. The Fabric Nodes Upgrade page is displayed.

Fabric Nodes Upgrade

V Series Proxy

Upgrade

V Series Node

Upgrade

Current Version

2.3.2

Image

Select an image...

Change Flavor

Batch Size

1

Upgrade

Cancel

4. To upgrade the GigaVUE V Series Nodes/Proxy, select the **Upgrade** checkbox.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V SeriesProxy/Nodes.

6. Select the **Change Flavor** checkbox to change the flavor of the nodes/proxy, only if required.
7. To upgrade the GigaVUE V Series Nodes/Proxy, specify the batch size in the **Batch Size** box.

For example, if there are 7 GigaVUE V Series Nodes, you can specify 7 as the batch size and upgrade all of them at once. Alternatively, you can specify 3 as the batch size, and launch and replace 3 V Series nodes in each batch. In the last batch, the remaining 1 V Series node is launched.

8. Click **Upgrade**.

The upgrade process takes a while depending on the number of GigaVUE V SeriesProxy and Nodes upgrading in your OpenStack environment. First, the new version of the GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes is launched. Then, the older version of both is deleted from the project. In the V Series Proxy page, click the link under Progress to view the upgrade status.

The monitoring session is deployed automatically.

Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi

Keep in mind the following when upgrading the GigaVUE V Series Nodes:

- You can select an entire monitoring domain and upgrade all the GigaVUE V Series Nodes in that particular monitoring domain, or you can select an individual GigaVUE V Series Node and upgrade it, or select multiple GigaVUE V Series Nodes in a monitoring domain and upgrade them.
- When upgrading GigaVUE V Series Nodes, if a host of a particular GigaVUE V Series Node is under maintenance mode, then the **Upgrade Fabric** button is disabled. Unselect the GigaVUE V Series Node whose host is under maintenance mode, and upgrade that GigaVUE V Series Node once the host is out of the maintenance mode.

NOTE: GigaVUE-FM only supports (n, n-1, n-2) GigaVUE V Series Node versions. Refer to GigaVUE-FM Version Compatibility Matrix in the *GigaVUE V Series Quick Start Guide* for detailed information on the supported versions.

To upgrade the GigaVUE V Series Node in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select an entire monitoring domain, an individual GigaVUE V Series Node, or multiple GigaVUE V Series Node and click **Actions**. From the drop-down list, select **Upgrade Fabric**, and the **V Series Node Upgrade Task** dialog box appears.

V Series Node	Form Factor	Version
VSeries.vp-esxi-	Small, 2vCPU, 4GB RAM, 8GB ...	6.4.00
VSeries.vp-esxi-	Small, 2vCPU, 4GB RAM, 8GB ...	6.4.00

3. Enter a name for the V Series Node upgrade task.
4. Select the latest GigaVUE V Series Node OVA image from the **Image** drop-down list.
5. When upgrading the GigaVUE V Series Nodes to any version equal to or greater than 6.5.00, the **Name Server** field is displayed. This field is optional. Name Server is a server that stores the mapping between the domain names and the IP address. The maximum number of name servers that can be entered is three. Enter valid IPv4 address, separated by comma.
6. If you want to modify the form factor (instance) size, click the **Change Form Factors** check box.
7. Select the form factor from the Default Form Factor drop-down menu to change the form factor of all the selected V Series Nodes. You can use the **Use Current** option to use the existing form factor of the individual GigaVUE V Series Node.

8. You can also change the form factor of a individual GigaVUE V Series Node from the **Form Factor** drop-down menu of the respective GigaVUE V Series Node. The form factor selected here overwrites the form factor selected in the **Default Form Factor**.

NOTE: All the GigaVUE V Series Node with Static IP address retain their old IP address even after the upgrade.

9. Click **Upgrade** to launch the GigaVUE V Series Node upgrade.

NOTE: Both the new and the current V Series nodes appear in the same Monitoring Domain until the new nodes replaces the current and the status changes to **Ok**.

You can view the status of the upgrade in the Status column of the **Monitoring Domain** page.

						New	Actions ▼	Refresh Inventory
Monitoring Domain	Connections	Name	Management IP	Tunnel IP	Type	Version	Status	
esxi-md-202-13							Upgrade Status	
	esxi-md-202-13						Connected	
		VSeries.vp-redscvr-10.115.208.48-renamed2	10.115.208.153	10.115.208.153	V Series Node	6.3.00	upgrading	
		VSeries.vp-redscvr-10.115.208.48	10.115.208.154	10.115.208.155	V Series Node	6.3.00	upgrading	
		VSeries.vp-redscvr-10.115.208.47	10.115.208.143	10.115.208.150	V Series Node	6.3.00	Ok	
		VSeries.vp-redscvr-10.115.208.48	10.115.208.158	10.115.208.141	V Series Node	6.3.00	Ok	
		VSeries.vp-redscvr-10.115.208.48-renamed2-c			V Series Node	6.4.00	launching	
		VSeries.vp-redscvr-10.115.208.48-upgrade			V Series Node	6.4.00	launching	

To view the detailed upgrade status click **Upgrade Status**, the **V Series Node Upgrade Status** dialog box appears.

V Series Node Upgrade Status

Monitoring Domain Name: esxi-md-202-13

Upgrade Tasks

▼ Upgrade_GigaVUE_VSERIES_Node | SUCCESS

Clear

Summary

Success: 2
 Failed: 0
 In Progress: 0
 Total: 2

Node Statuses

Node	Status
VSeries.vp-redscvr- <small>10.115.201.48</small>	OK
VSeries.vp-redscvr- <small>10.115.201.48</small> renamed2	OK

▼ Upgrade | IN_PROGRESS

Summary

Success: 0
 Failed: 0
 In Progress: 1
 Total: 1

Node Statuses

Node	Status
VSeries.vp-redscvr- <small>10.115.201.48</small> upgrade	launching

- Click **Clear** to delete the monitoring domain upgrade status history of successfully upgraded nodes.
- If the GigaVUE V Series Node upgrade fails or is interrupted for any reason, click on the **Retry** button on the **V Series Node Upgrade Status** dialog box.

NOTE: You cannot modify the node configurations when you are using **Retry** option. GigaVUE -FM uses the same values defined in the initial fabric upgrade configuration.

Upgrade GigaVUE V Series Node for VMware NSX-T

GigaVUE V Series Nodes can be deployed in two ways. You can either directly use VMware NSX-T manager to deploy your GigaVUE V Series Nodes or use GigaVUE-FM to deploy your GigaVUE V Series Nodes. Based on the method you deploy GigaVUE V Series Nodes, you can upgrade them in two ways. Refer to the following topic for more detailed information.


- [Upgrade GigaVUE V Series Nodes Deployed using GigaVUE-FM](#)
- [Upgrade GigaVUE V Series Node Deployed using VMware NSX-T Manager](#)

Upgrade GigaVUE V Series Nodes Deployed using GigaVUE-FM

Before upgrading the nodes ensure that all the current V Series nodes are of same version. To upgrade GigaVUE V Series Node in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select a deployed monitoring domain and click **Actions**. From the drop-down list, select **Upgrade Fabric**, the **V Series Node Upgrade** dialog box appears.

V Series Node Upgrade

Current Version 

Use External Image No

Change Form Factors

Select an image

- gigamon-gigavue-vseries-node-2.3.1-275864_amd64.ova>
- gigamon-gigavue-vseries-node-2.3.3-284615_amd64.ova>

- Use the **Use External Image** toggle button to choose between internal and external image.
 - Yes** to use an external image. Enter the Image URL of the latest V Series Node OVA image
 - No** to use an internal image. To use an internal image, select the uploaded OVA files from the **Select an image** drop-down menu.
- Click the **Change Form Factors** check box to modify the form factor (instance) size.

NOTE: Both the new and the current V Series nodes appears on the same monitoring domain until the new nodes replaces the current and the status changes to **Ok**.

- Click **Upgrade**.

You can view the status of the upgrade in the Status column of the **Monitoring Domain** page.

To view the detailed upgrade status click **Upgrade in progress** or **Upgrade successful**, the **V Series Node Upgrade Status** dialog box appears.

V Series Node Upgrade Status

Monitoring Domain: esxi-md

Summary

Success: 1 Failed: 0 In Progress: 0 Total: 1

Node Statuses

Node	Status
VSeries- available -node1-10-210-27-202	OK

Clear Close

Click **Clear** to delete the logs of successfully upgraded nodes.

NOTE: Monitoring Domain upgrade can be only done when there is a single service deployment in the monitoring domain.

Upgrade GigaVUE V Series Node Deployed using VMware NSX-T Manager

NOTE: When you deploy your V Series Nodes using VMware NSX-T manager, you cannot directly upgrade V Series Node in GigaVUE-FM. In this case, the upgrade button in GigaVUE-FM is disabled.

To upgrade V Series Nodes deployed using VMware NSX-T, follow the steps given below:

1. Delete the existing V Series Node in VMware NSX-T Manager.
2. Click **Actions > Edit** in the Monitoring Domain page. The **VMware Configuration** page appears.
3. Enter the new **Image URL** or select a new image if **Use External Image** toggle button is disabled.
4. Then, deploy the new V Series Nodes in the VMware NSX-T manager

GigaVUE-FM Administrator Authentication by Platform

This table describes the initial values that are used for first time log in as a GigaVUE-FM administrator via the GUI or CLI on various supported platforms. Important to know:

- The credentials used in the GigaVUE-FM GUI interface are different than those used in the GigaVUE-FM CLI interface.
- As deployments vary by platform, so do the admin authentication methods. Depending on the platform where GigaVUE-FM is installed, you may need to specify the authentication method (SSH Public Key or Password) during deployment or use a pre-defined default password and then change the password the first time you log in.
- Additionally, the default login credentials have also changed in certain software releases.

Initial Credentials for GigaVUE-FM Credentials

The following table provides the initial login credentials for GigaVUE-FM after installing or upgrading. The table displays data for Release 6.0.00 and above, and then provides CLI and GUI authentication options, rules, and notes for each supported platform.

Mode	Credential	Values by Platform and Mode (GUI/CLI)				
		AWS	Azure	VMware OVA Deployments	OpenStack	Other (non-OVA) Deployments
CLI	Username	gigamon	<i>specified during deployment.</i>	admin	admin	admin
	Password	<i>no password</i>	<i>specified during deployment.</i>	<i>specified during deployment</i>	admin123A!!	admin123A!!

	SSH Public Key	<i>specified during deployment</i>	<i>specified during deployment</i>	<i>specified during deployment</i>	<i>no initial value</i>	<i>no initial value</i>
	Rules & Notes	For AWS, initial access is only available using an SSH Public Key	During Azure deployments, you must specify one authentication method and provide the value. Either authentication method will work if configured; however, on Azure, you cannot specify both, you can only configure one method.	In VMware deployments, you may configure an SSH Public Key and/or a Password. You may configure both, but you must configure at least one of them. If you configure both, then you can use either method to access the FM CLI.	Password change is required on first login.	Password change is required on first login.
GUI	Username	admin	admin	admin	admin	admin
	Password	<AWS Instance ID> of FM virtual instance	admin123A!!	admin123A!!	<OpenStack Instance ID> of FM virtual instance, reverts to 'admin123A!!' if no metadata service is available.	admin123A!!
	Rules & Notes					

Logging in to GigaVUE-FM Command Line Interface

Users of GigaVUE Fabric Manager have access to the Linux shell of GigaVUE-FM. Log in to GigaVUE-FM through SSH and you will land on the command line prompt. Use this access to troubleshoot issues and perform certain operations. Refer to the following sections for details:

- [GigaVUE-FM CLI Commands](#)
- [Post Installation Configurations](#)
- Post Installation Configurations (Refer to GigaVUE-FM Installation and Upgrade Guide)

GigaVUE-FM has all the required software pre-installed to perform the various functions. Unless directed by Gigamon, do not install any third-party software, and Gigamon explicitly does not recommend to install such additional software.

Important: Installing Third-party software in GigaVUE-FM can have adverse effects on the operation of GigaVUE-FM. Uninstall all third-party software prior to contacting Gigamon Support for troubleshooting.

Post Installation Configurations

This section describes the processes that must be performed after GigaVUE-FM is installed. Refer to the instruction in this chapter if you wish to install custom certificate or Rabbit MQ certificate.

- How to install custom certificates instead of default Self-signed certificates loaded in GigaVUE-FM: [Install Custom Certificate](#)
- How to [Install Rabbit MQ Certificate](#)
- How to establish communication between the load balancer and web server: [Post Installation Configurations](#)

Install Custom Certificate

To install a third-party certificate on GigaVUE-FM, refer to the following sections:

- [Pre-requisites](#)
- [Steps](#)

Pre-requisites

Refer to the following pre-requisites:

- Take a backup of the default system self-signed certificate and key contents before replacing them with third-party certificate and key. The files are available in the following folders:
 - **localhost.crt:** `/etc/pki/tls/certs/localhost.crt`
 - **localhost.key:** `/etc/pki/tls/private/localhost.key`
- When replacing the certificate key and file ensure to adhere to the following naming convention:
 - For Certificate: **localhost.crt**
 - For Certificate Key: **localhost.key**
- When you copy the contents of the certificate file, do not delete the EOL characters at the end of each line. If there is no EOL character at the end of certificate file, insert one.
- In case of chain of certificates, bundle the server, intermediate, and root certificates into a single certificate file before replacing the **localhost.crt**.
- For chain of certificates, add the SSLCertificateChainFile directive to `/etc/httpd/conf.d/ssl.conf`: **sudo vim /etc/httpd/conf.d/ssl.conf**. Add the following line: **SSLCertificateChainFile /etc/pki/tls/certs/localhost.crt**.

Steps

Generate the certificate and a private key file in pem format. Use the following command on Linux or a Linux app (such as Cygwin) for generating the files:

```
sudo openssl req -new -newkey ec -pkeyopt ec_paramgen_curve:secp384r1 -x509 -nodes -keyout privatekey.pem -days 365 -out certificate.pem
```

NOTE: Until software version 6.4.00, GigaVUE-FM supported RSA based certificates. Starting from software version 6.5.00, GigaVUE-FM supports ECDHE based certificates. However, you can configure the certificate as per your need.

Copy the contents of the certificate file.

To install the certificates:

1. Log in to the GigaVUE-FM CLI.
2. Execute the following steps from the shell prompt as a root user (**sudo**):
 - Replace SSLCertificateFile: `/etc/pki/tls/certs/localhost.crt`
 - Replace SSLCertificateKeyFile: `/etc/pki/tls/private/localhost.key`
 - Provide access to certificate file: `chmod 644 /etc/pki/tls/certs/localhost.crt`
 - Provide access to key file: `chmod 600 /etc/pki/tls/private/localhost.key`

- Configure GigaVUE-FM load balancer functionality:

```
cat /etc/pki/tls/certs/localhost.crt  
/etc/pki/tls/private/localhost.key > /etc/pki/tls/certs/localhost.pem  
systemctl reload haproxy.service
```

- Restart apache as root: **systemctl restart httpd.service**
- After restarting, ensure tomcat is up and running: **sudo systemctl status tomcat@cms.service**

The system will now start using the newly installed certificate.

GigaVUE-FM uses a public key (cms.p12 file) to encrypt the Security Assertion Markup Language (SAML) messages. You can either use the default public key available in GigaVUE-FM or generate a new public key using the following command:

```
sudo openssl pkcs12 -export -name CMS -out /etc/gigamon/cms.p12 -inkey  
/etc/pki/tls/private/localhost.key -in /etc/pki/tls/certs/localhost.crt -  
passout pass:cms123
```

You will be prompted for a pass phrase for the **localhost.crt**.

After the public key (cms.p12 file) is generated, place the file in the `/etc/gigamon` directory. Change the access rights to **chmod 644**.

Install Rabbit MQ Certificate

To update the Rabbit MQ certificate, generate the certificate and a private key file in pem format. Use the following command on Linux or a Linux app (such as Cygwin) for generating the files:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout privatekey.pem -out  
certificate.pem
```

Copy the contents of the certificate file.

To update the RabbitMQ files:

1. Log in to the GigaVUE-FM CLI.
2. Execute the following steps from the shell prompt as a root user (sudo):

Replace the existing certificate: `/var/lib/gigamon/rabbitmq/server/cert.pem`

Example: `cp certificate.pem /var/lib/gigamon/rabbitmq/server/cert.pem`

Replace the existing private key: `/var/lib/gigamon/rabbitmq/server/key.pem`

Example: `cp privatekey.pem /var/lib/gigamon/rabbitmq/server/key.pem`

Provide access to certificate and key: **chmod 644**

NOTE: It is not required to reload the RMQ service.

Syslog and AFI Monitoring Stats Collection

By default, GigaVUE-FM collects the system logs and AFI monitoring statistics only if GigaVUE-FM is configured in Dual Stack or IPv6 environment. If your GigaVUE-FM instance is running in IPv4 only environment, execute the following command from the GigaVUE-FM command line interface to enable syslog and AFI monitoring stats collection:

```
curl -XPOST "http://localhost:4466/fmcs/fm/network?pretty" -H
"Content-Type:
application/json" -d '{"logstash":{"enable_ipv6" : "false"}}'
```

To revert back to IPv6 / Dual Stack environment, execute the following command:

```
curl -XPOST "http://localhost:4466/fmcs/fm/network?pretty" -H
"Content-Type:
application/json" -d '{"logstash":{"enable_ipv6" : "true"}}'
```

Communication between GigaVUE-FM Load Balancer and Web Server

After GigaVUE-FM is installed, communication is established between GigaVUE-FM Load Balancer (HA-proxy service) and the apache web server. By default, Load Balancer uses the IPv4 loopback address to communicate with the webserver present locally.

Refer to the following notes:

To change from IPv4 to IPv6 loopback address use the following command:

```
curl -XPOST "http://localhost:4466/fmcs/fm/network?pretty" -H "Content-Type:
application/json" -d '{"haproxy":{"enable_ipv6" : "true"} '
```

To change from IPv6 to IPv4 loopback address use the following command:

```
curl -XPOST "http://localhost:4466/fmcs/fm/network?pretty" -H "Content-Type:
application/json" -d '{"haproxy":{"enable_ipv6" : "false"} '
```

Configure rSyslog Server for Receiving TLS/SSL Packets

This section describes the steps to configure the rSyslog server if you want to enable TLS logging for audit logs and syslogs from GigaVUE-FM.

Prerequisite: Install the required packages on the rSyslog server:

```
rsyslog-gnutls-5.8.10-10.0.1.el6_6.x86_64
rsyslog-5.8.10-10.0.1.el6_6.x86_64
gnutls-utils-2.8.5-19.el6_7.x86_64
gnutls-2.8.5-19.el6_7.x86_64
```

The steps are described in the following table:

	Steps	Details
1	Add the following parameter <code>s</code> in <code>/etc/rsyslog.conf</code> in remote server and restart rsyslog services.	<pre>\$ModLoad imtcp \$InputTCPServerRun 514 \$DefaultNetstreamDriver gtls \$DefaultNetstreamDriverCAFile /etc/pki/tls/private/ca.pem \$DefaultNetstreamDriverCertFile /etc/pki/tls/private/rservtls-cert.pem \$DefaultNetstreamDriverKeyFile /etc/pki/tls/private/rservtls-key.pem \$ActionSendStreamDriverPermittedPeer <10.115.48.54> ==> Replace with remote server IP/DNS Name \$ActionSendStreamDriverMode 1 \$ActionSendStreamDriverAuthMode x509/name</pre>

	Steps	Details
2	Generate CA key on the remote server.	<pre> fmtaf@fmreg26:/tmp/rsysconf\$ certtool --generate-privkey --outfile ca-key.pem Generating a 3072 bit RSA private key... fmtaf@fmreg26:/tmp/rsysconf\$ chmod 400 ca-key.pem </pre>
3	Generate CA per on the remote server	<pre> fmtaf@fmreg26:/tmp/rsysconf\$ certtool --generate-self-signed --load-privkey ca-key.pem -- outfile ca.pem Generating a self signed certificate... Please enter the details of the certificate's distinguished name. Just press enter to ignore a field. Common name: 10.210.22.114 UID: Organizational unit name: Organization name: Locality name: State or province name: Country name (2 chars): Enter the subject's domain component (DC): This field should not be used in new certificates. E-mail: Enter the certificate's serial number in decimal (123) or hex (0xabcd) (default is 0x3fdea4af40da84d2580d59f9770ae288732c3421) value: Activation/Expiration time. The certificate will expire in (days): 3650 Extensions. Does the certificate belong to an authority? (y/N): y Path length constraint (decimal, -1 for no constraint): Is this a TLS web client certificate? (y/N): Will the certificate be used for IPsec IKE operations? (y/N): Is this a TLS web server certificate? (y/N): </pre>

Steps	Details
	<pre> Enter a dnsName of the subject of the certificate: Enter a URI of the subject of the certificate: Enter the IP address of the subject of the certificate: Enter the e-mail of the subject of the certificate: Will the certificate be used for signing (required for TLS)? (Y/n): Will the certificate be used for data encryption? (y/N): Will the certificate be used to sign OCSP requests? (y/N): Will the certificate be used to sign code? (y/N): Will the certificate be used for time stamping? (y/N): Will the certificate be used for email protection? (y/N): Will the certificate be used to sign other certificates? (Y/n): Y Will the certificate be used to sign CRLs? (y/N): y Enter the URI of the CRL distribution point: X.509 Certificate Information: Version: 3 Serial Number (hex): 3fdea4af40da84d2580d59f9770ae288732c3421 Validity: Not Before: Thu Mar 09 14:41:22 UTC 2023 Not After: Sun Mar 06 14:41:29 UTC 2033 Subject: CN=10.210.22.114 Subject Public Key Algorithm: RSA Algorithm Security Level: High (3072 bits) Modulus (bits 3072): 00:e4:09:d2:d0:b4:eb:a3:49:da:53:3f:34:78:8c:36 46:76:f8:23:43:ab:59:51:b9:28:ff:c7:01:9c:b3:65 02:fc:4f:f1:9d:a7:5e:f7:60:f7:e7:90:58:4d:3c:86 85:ac:f7:d6:dd:85:3f:ef:55:88:2d:4b:f5:ec:ba:f2 76:01:04:e4:83:5d:40:c8:57:87:f5:06:40:0d:be:30 a4:2a:2f:8f:e9:6a:9e:4a:2a:53:e4:40:ef:ec:f6:a9 17:cd:e5:58:41:fd:9a:82:2b:7c:b3:33:64:b3:5d:74 31:e0:9a:47:b6:b5:42:bc:9f:89:82:50:08:36:b2:ca e8:c6:3a:ac:ad:47:d3:4f:f7:a6:6e:e1:33:bc:b8:d1 </pre>

Steps	Details
	<pre> 32:10:f3:cb:29:ef:28:cd:9b:40:57:c3:4e:45:f9:fe 33:eb:5f:6f:72:db:52:2f:e7:99:eb:61:ea:66:ee:e9 c2:79:c9:d0:cd:fc:18:7a:01:98:39:4e:f0:12:97:d1 c7:68:ba:cd:08:b1:30:cb:22:17:0b:c5:a2:f7:55:7d 37:5f:21:d1:10:d9:1d:2b:cf:d6:c8:a0:d7:e0:64:57 9a:f6:7a:57:17:ef:bb:4f:16:5e:4c:17:f1:cd:53:cc da:b1:8e:32:3c:eb:1e:6b:83:20:c5:a7:5a:24:8f:96 b3:03:04:b0:16:8a:95:44:1c:7b:42:70:2f:30:87:23 8d:13:69:a9:b2:ed:8f:4f:11:f1:42:b9:11:a6:35:35 ef:30:b7:5c:82:d9:b3:90:91:65:20:cf:e4:46:3d:3a 05:d6:72:85:26:42:e7:ea:a1:8b:94:81:ab:9e:ed:83 79:f7:7f:8a:07:8c:0f:17:b0:6c:7d:78:a5:16:9d:cc 5f:48:0c:b1:40:3c:bf:94:4d:f7:a4:b4:e5:d0:bd:62 4b:ba:a6:2e:57:0f:87:50:f1:98:79:1e:ac:d2:47:b0 e0:3b:41:a2:0e:cd:2a:8e:15:34:cf:ad:a6:c6:1b:27 4d Exponent (bits 24): 01:00:01 Extensions: Basic Constraints (critical): Certificate Authority (CA): TRUE Key Usage (critical): Digital signature. Certificate signing. CRL signing. Subject Key Identifier (not critical): c61e0b508686f9701616f57f1e49e3448b06f98d Other Information: Public Key ID: sha1:c61e0b508686f9701616f57f1e49e3448b06f98d sha256:e01a89569cfb732403af0e5e2c0bd9606f69fa7b66c3a8beea69970569eb51fd Public Key PIN: </pre>

	Steps	Details
		<pre>pin-sha256:4BqJVpz7cyQDrw5eLAvZYG9p+ntmw6i+6mmXBWnrUf0= Is the above information ok? (y/N): y Signing certificate... fmtaf@fmreg26:/tmp/rsysconf\$</pre>
4	Generate remote server tls key	<pre>fmtaf@fmreg26:/tmp/rsysconf\$ certtool --generate-privkey --outfile rservtls-key.pem --bits 2048 ** Note: You may use '--sec-param Medium' instead of '--bits 2048' Generating a 2048 bit RSA private key... fmtaf@fmreg26:/tmp/rsysconf\$</pre>
5	Generate remote server tls pem	<pre>fmtaf@fmreg26:/tmp/rsysconf\$ certtool --generate-request --load-privkey rservtls-key.pem --outfile request.pem Generating a PKCS #10 certificate request... Common name: 10.210.22.114 Organizational unit name: Organization name: Locality name: State or province name: Country name (2 chars): Enter the subject's domain component (DC): UID: Enter a dnsName of the subject of the certificate: Enter a URI of the subject of the certificate: Enter the IP address of the subject of the certificate: Enter the e-mail of the subject of the certificate: Enter a challenge password: Does the certificate belong to an authority? (y/N): Will the certificate be used for signing (DHE ciphersuites)? (Y/n):</pre>

	Steps	Details
		<pre> Will the certificate be used for encryption (RSA ciphersuites)? (Y/n): Will the certificate be used to sign code? (y/N): Will the certificate be used for time stamping? (y/N): Will the certificate be used for email protection? (y/N): Will the certificate be used for IPsec IKE operations? (y/N): Will the certificate be used to sign OCSP requests? (y/N): Is this a TLS web client certificate? (y/N): Is this a TLS web server certificate? (y/N): fmtaf@fmreg26:/tmp/rsysconf\$ </pre>
6	Generate remote server tls cert	<pre> fmtaf@fmreg26:/tmp/rsysconf\$ certtool --generate-certificate --load-request request.pem -- outfile rservtls-cert.pem --load-ca-certificate ca.pem --load-ca-privkey ca-key.pem Generating a signed certificate... Enter the certificate's serial number in decimal (123) or hex (0xabcd) (default is 0x5df5369b91556a947c9f33ba41defd7ad6cdaf23) value: Activation/Expiration time. The certificate will expire in (days): 1000 Extensions. Do you want to honour all the extensions from the request? (y/N): Does the certificate belong to an authority? (y/N): Is this a TLS web client certificate? (y/N): y Will the certificate be used for IPsec IKE operations? (y/N): Is this a TLS web server certificate? (y/N): y Enter a dnsName of the subject of the certificate: 10.210.22.114. <Remote server IP /DNS NAmE> Enter an additional dnsName of the subject of the certificate: Enter a URI of the subject of the certificate: Enter the IP address of the subject of the certificate: Will the certificate be used for signing (DHE ciphersuites)? (Y/n): </pre>

Steps	Details
	<pre> Will the certificate be used for encryption (RSA ciphersuites)? (Y/n): Will the certificate be used for data encryption? (y/N): Will the certificate be used to sign OCSP requests? (y/N): Will the certificate be used to sign code? (y/N): Will the certificate be used for time stamping? (y/N): Will the certificate be used for email protection? (y/N): X.509 Certificate Information: Version: 3 Serial Number (hex): 5df5369b91556a947c9f33ba41defd7ad6cdaf23 Validity: Not Before: Thu Mar 09 15:03:54 UTC 2023 Not After: Wed Dec 03 15:03:57 UTC 2025 Subject: CN=10.210.22.114 Subject Public Key Algorithm: RSA Algorithm Security Level: Medium (2048 bits) Modulus (bits 2048): 00:a7:f3:c9:05:27:f3:bc:d9:81:e4:67:9e:7c:44:2f d3:c8:8f:66:21:cd:d3:e3:2b:91:b9:36:bf:2b:bf:b4 cf:2e:37:31:a0:ed:a9:8d:a2:e2:e5:f9:7a:c3:10:2c 08:7e:ea:66:7e:d6:48:5a:c0:4b:2e:5e:94:c8:19:61 12:66:53:f0:df:cd:cc:e9:40:f3:9a:ed:96:e5:3b:ba a6:19:df:ef:6f:d9:f2:62:64:9a:80:5f:6b:4c:bc:6b 85:fb:70:c9:8d:d7:ff:40:32:4b:c2:92:82:e1:e3:ae 51:e5:fa:70:1f:cd:3f:d2:da:f7:6b:c7:9b:20:df:d8 54:9a:2e:88:4e:9f:f1:17:bd:63:e4:ee:f1:2d:73:86 c8:7f:a8:e7:13:7f:20:5b:e7:47:52:ec:f5:55:ee:d3 13:63:93:bf:d8:2e:43:d8:17:a8:9f:c3:3f:5b:5d:c9 20:58:a5:26:fe:c4:8d:75:cf:d6:d8:7b:72:f1:ca:60 fb:b6:11:0e:c1:da:62:e9:28:dc:ed:43:18:66:13:2e 6e:54:a4:f8:72:82:4f:43:f6:9a:72:b9:ec:c4:15:cc 65:9a:8d:78:e3:ab:99:c5:da:d4:28:40:e7:b0:53:b3 a1:8d:71:2d:8d:0d:3c:cb:59:2e:de:6f:1d:ac:96:fd </pre>

	Steps	Details
		<pre> 95 Exponent (bits 24): 01:00:01 Extensions: Basic Constraints (critical): Certificate Authority (CA): FALSE Key Purpose (not critical): TLS WWW Client. TLS WWW Server. Subject Alternative Name (not critical): DNSname: 10.210.22.114 Key Usage (critical): Digital signature. Key encipherment. Subject Key Identifier (not critical): 068d2ac695b2b89eb631e8abc9441c9054c6b5e2 Authority Key Identifier (not critical): c61e0b508686f9701616f57f1e49e3448b06f98d Other Information: Public Key ID: sha1:068d2ac695b2b89eb631e8abc9441c9054c6b5e2 sha256:f81482f583c4e6a464ffcc2c05ddfdb00ef9b7255eb6d344006b116ebe28cd29 Public Key PIN: pin-sha256:+BSC9YPE5qRk/8wsBd39sA75tyVettNEAGsRbr4ozSk= Is the above information ok? (y/N): y Signing certificate... fmtaf@fmreg26:/tmp/rsysconf\$ </pre>
7	Copy the following	<pre> # rsync -aP rslserver-* root@<GigaVUE-FM IP address>:/etc/pki/tls/private/ # rsync -aP ca.pem root@<GigaVUE-FM IP address>:/etc/pki/tls/private/ </pre>

	Steps	Details
	<p>three files generated in the remote server to GigaVUE-FM at path /etc/pki/tls/private.</p> <ul style="list-style-type: none"> • ca.pem • rservtls-key.pem • rservtls-cert.pem 	
8	<p>Run the command in GigaVUE-FM to enable IP rules.</p>	<pre># sudo iptables -A INPUT -p tcp --dport 514 -j ACCEPT</pre>
9	<p>Run the fmctl command. Verify that</p>	<pre># fmctl logging 10.115.48.54:514 tls</pre>

Steps	Details
tls logging is configured by running the sudo TCPdump command at the remote server.	

Reference

This section provides additional information useful for GigaVUE-FM installation and upgrade.

Topics:

- [Setting the GigaVUE-FM Admin Password](#)
- [GigaVUE-FM CLI Commands](#)

Setting the GigaVUE-FM Admin Password

You can set the admin password for GigaVUE-FM from the GigaVUE-FM Command-line Interface (CLI) or from the GigaVUE-FM GUI. This topic describes the requirements for the password.

The characters in the admin password must include, at least:

- At least 8 characters and up to a maximum of 64 characters in length
- One numerical character
- One upper case character
- One lower case character
- One special character from -!@#\$%^&*()+

If the password does not meet the complexity requirements:

- The system does not display any error message.
- The parameters configured above are not passed on to the GigaVUE-FM except the host name parameter.
- The static IP addresses that were configured originally will be unavailable after GigaVUE-FM is deployed.

Setting the Admin Password from the GigaVUE-FM CLI

The password can be a minimum of 14 characters and a maximum of 255 characters, and must comply with the character requirements specified above.

NOTE: The password that you set from the GigaVUE-FM CLI is applicable only to the GigaVUE-FM CLI.

Setting the Admin Password from the GigaVUE-FM GUI

You must change the default admin password when you first login to the GigaVUE-FM UI. The default username and password for a admin user in GigaVUE-FM GUI is *admin* and *admin123A!!*, respectively. If GigaVUE-FM is deployed inside AWS or OpenStack, then the default password is the **Instance ID**. You can change the default admin password from GUI. The password

can be a minimum of 8 characters and a maximum of 64 characters, and must comply with the character requirements specified above.

NOTE: The password that you set from the GigaVUE-FM GUI is applicable only to the GigaVUE-FM GUI.

GigaVUE-FM CLI Commands

This section describes the commands for the GigaVUE-FM Command-Line Interface (CLI) related to installation and upgrade processes.

fmctl

Use the **fmctl** command to manage GigaVUE-FM-related configurations.

The **fmctl** command has the following syntax:

```
fmctl  
  configuration [backup|restore][<absolute pathname of backup file>]  
  image  
    fetch <download URI> [<filename>]  
    list [details] [<filename>]  
    install <filename> [next|location {1|2}]  
    boot [next|location {1|2}]  
    delete [force] <filename>  
    {move|rename} <old filename> <new filename>  
    show  
  jump-start
```

```

logging [<fqdn>[:<port>]] [facility <facility>] [priority <priority>] [udp|tcp|tls]
no logging <fqdn>[:<port>]
reset factory halt
set UI admin password <new password>

{get|show} interface [{mgmt|management}]
set interface {mgmt|management} <interface name>
[options{--help|--interface <interface name>}]
    set mapping <fqdn> <IP address>
    {get|show} {ip|ntp|hostname|domain|fqdn}
    set [ip|ip6] dhcp
    set [ip|ip6] [static] <address/cidr> [<gateway> [<dns1>[,<dns2>[,...]]]
    set {ip|ip6} route {add|remove} address/cidr gateway
    set ntp {disable|[enable] <server1>[,<server2>[,...]}
    set hostname <hostname>
    set domain <domain>
    set fqdn <hostname> <domain>
    set/get/show searchdomains [<domain1>[,<domain2>[,...]]]
    set/get/show nameservers [<dns1>[,<dns2>[,...]]]
    show backup [<absolute pathname of backup file>]
unlock UI <username>

```

The following table describes the arguments for the **fmctl** command:

Argument	Description
configuration [backup restore]	<p>Backs up and restores the configurations such as management interface, hostname, domain, IP, search domains, and NTP.</p> <p>For example, use the following command to back up the system configurations:</p> <p style="text-align: center;">fmctl configuration backup <absolute path name of backup file></p> <p>Use the following command to restore the system configurations from the backup:</p> <p style="text-align: center;">fmctl configuration restore <absolute path name of backup file></p>
image fetch <download URI> [<filename>]	<p>Retrieves an image file from a remote host. Use HTTP(S), FTP, or SCP to retrieve the file. The format for the download URL is as follows:</p> <p style="text-align: center;">[protocol]://username[:password]@hostname:/path/filename</p> <p>For example, the following command retrieves the image file named myimage from the FTP server at 192.168.1.10 using the robh account with the xray password:</p> <p style="text-align: center;">fmctl image fetch ftp://robh:xray@192.168.1.10/myimage</p> <p>You can also use the <filename> argument to give the retrieved file a new name on GigaVUE-FM. For example, the following command retrieves myimage and names it newconfig:</p> <p style="text-align: center;">fmctl image fetch scp://bbochy:catch1@192.168.1.75:/myconfig newconfig</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: You cannot retrieve a file with the same name as an existing configuration file.</p> </div>
image list	<p>Provides the list of image file names available in GigaVUE-FM.</p> <p>For example:</p> <p style="text-align: center;">fmctl image list</p>
image install <filename> [next location {1 2}]	<p>Installs the image file.</p> <p>For example, use the following command to install the image file on the next partition:</p> <p style="text-align: center;">fmctl image install gigamon-gigavue-fm-5.8.00-160194-trial.img next</p> <p>Use the following command to install the image file on the specified partition:</p> <p style="text-align: center;">fmctl image install gigamon-gigavue-fm-5.8.00-160194-trial.img location</p>

Argument	Description
	<p>1</p> <p>NOTE: Ensure that your current partition is not the same as the partition you specified for installation. Else, an error is displayed.</p>
image boot [next location {1 2}]	<p>Boots the image file on the specified partition. Ensure that the partition has the installed image file.</p> <p>For example, use the following command to boot the image file on the next partition:</p> <p>fmctl image boot next</p> <p>Use the following command to boot the image file on the specified partition:</p> <p>fmctl image boot location 1</p> <p>NOTE: GigaVUE-FM reboots immediately.</p>
image delete [force] <filename>	<p>Deletes the named image file.</p> <p>For example:</p> <p>fmctl image delete myimage</p>
image {move rename} <old filename> <new filename>	<p>Moves or renames the specified image file. For example, the following command renames myimage as newimage:</p> <p>fmctl image rename myimage newimage</p>
image show	<p>Displays the last boot partition.</p> <p>For example:</p> <p>fmctl image show</p>
jump-start	<p>Runs the configuration wizard for the initial setup of GigaVUE-FM. Refer to Perform Initial Configuration.</p> <p>NOTE: When you change the IP address of the GigaVUE-FM instance using the jump-start</p>

Argument	Description
	<p>configuration, the internal database and the in-memory caches of the GigaVUE-FM instance are not updated. The Database continues to have the IP address of the old GigaVUE-FM, and the image upgrade using the internal server option does not work. To fix this, you must restart the GigaVUE-FM instance after upgrade.</p>
<p>logging [<fqdn>[:<port>]] [facility <facility>] [priority <priority>] [udp tcp tls]</p>	<p>Configures the logging server for sending events and audit logs to the remote server. For example:</p> <p style="text-align: center;">fmctl logging 1.2.3.4:9514 facility * priority debug tcp</p> <p>Until software version 6.2.00, you can only use the UDP and TCP protocols for logging the audit logs and Syslogs to a remote server. Starting from software version 6.3.00, GigaVUE-FM allows you to configure the logging of audit logs and syslogs using tls. You must perform specific configurations in the remote server to enable logging using TLS. Refer to the Configure rSyslog Server for Receiving TLS/SSL Packets section for more details.</p>
<p>no logging <fqdn>[:<port>]</p>	<p>Removes the logging server configuration. For example:</p> <p style="text-align: center;">fmctl no logging 1.2.3.4:9514</p>
<p>reset factory halt</p>	<p>Resets the GigaVUE-FM instance to the default configuration and shuts down the system. For example:</p> <p style="text-align: center;">fmctl reset factory halt</p>
<p>set UI admin password <new password></p>	<p>Configures a new admin password for the GigaVUE-FM UI only. For information on setting the GigaVUE-FM password, refer to Setting the GigaVUE-FM Admin Password.</p>
<p>{get show} interface [{mgmt management}]</p>	<p>Displays the management interface configured for the GigaVUE-FM instance. For example:</p> <p style="text-align: center;">fmctl get show interface management</p>

Argument	Description
set interface {mgmt management} <interface name>	<p>Configures the management interface for the GigaVUE-FM instance, which has more than one ethernet interface.</p> <p>For example:</p> <pre>fmctl set interface management eth1</pre> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: You cannot use the --interface syntax with the set interface management argument.</p> </div>
--interface <interface name>	<p>Allows various configurations that can be set for the management interface. This is an optional argument.</p> <p>For example, use the following command to ensure that eth1 management interface uses DHCP:</p> <pre>fmctl --interface eth1 set ip dhcp</pre>
[options{--help --interface <interface name>}] set mapping <fqdn> <IP address>	<p>Maps the FQDN with the IP address of GigaVUE-FM.</p> <p>For example:</p> <pre>fmctl --interface eth1 set mapping fm 10.10.10.1</pre> <p>Use the following command to remove the mapping:</p> <pre>fmctl --interface eth1 set mapping fm</pre>
[options{--help --interface <interface name>}] {get show} {ip ntp hostname domain fqdn}	<p>Use to either fetch or display the IP address, NTP configurations, host name, domain name, or FQDN .</p> <p>For example:</p> <pre>fmctl --interface eth1 get {ip ntp hostname domain fqdn} fmctl --help show {ip ntp hostname domain fqdn}</pre>
[options{--help --interface <interface name>}] set [ip ip6] dhcp	<p>Configures the management interface to use DHCP.</p> <p>For example:</p> <pre>fmctl --interface eth1 set ip dhcp</pre>

Argument	Description
<code>[options{--help --interface <interface name>}] set [ip ip6] [static] <address/cidr> [<gateway> [<dns1> [,<dns2>[,...]]]</code>	Configures the static IP address and gateway on the management interface. You can also choose to configure DNS. For example: fmctl --interface eth1 set ip static 10.115.46.72/21 10.115.40.1 10.10.1.20
<code>[options{--help --interface <interface name>}] set {ip ip6} route {add remove} address/cidr gateway</code>	Adds or removes the IP address and gateway for the management interface.
<code>[options{--help --interface <interface name>}] set ntp {disable [enable] <server1>[,<server2>[,...]]}</code>	Use to enable or disable NTP for synchronization of the system's clock. For example, the following command disables NTP: fmctl --interface eth1 set ntp disable You choose to enable NTP and add NTP servers. For example, the following command enables NTP and adds a NTP server: fmctl --interface eth1 set ntp enable 192.168.1.10
<code>[options{--help --interface <interface name>}] set hostname <hostname></code>	Configures the hostname. For example: fmctl --interface eth1 set hostname myfm NOTE: Ensure that you log out and re-login to the GigaVUE-FM to view the changes.
<code>[options{--help --interface <interface name>}] set domain <domain></code>	Configures the domain for GigaVUE-FM. For example: fmctl --interface eth1 set domain gigamon.com
<code>[options{--help --interface <interface name>}] set fqdn <hostname> <domain></code>	Configures the Fully Qualified Domain Name (FQDN) for the current GigaVUE-FM. fmctl --interface eth1 set fqdn myfm gigamon.com
<code>[options{--help --interface <interface name>}] set/get/show searchdomains</code>	Displays a list of domains for the current GigaVUE-FM For example:

Argument	Description
<code>[<domain1>[,<domain2>[,...]]]</code>	<p>fmctl --interface eth1 set searchdomains</p> <p>fmctl --help get show searchdomains</p>
<code>[options{--help --interface <interface name>}] set/get/show nameservers [<dns1>[,<dns2>[,...]]]</code>	<p>Displays a list of name servers for the current GigaVUE-FM</p> <p>For example:</p> <p>fmctl --interface eth1 set nameservers</p> <p>fmctl --help get show nameservers</p>
<code>[options{--help --interface <interface name>}] show backup</code>	<p>Displays the configurations that were backed up.</p> <p>For example:</p> <p>fmctl --help show backup <absolute path name of backup file></p>
<code>unlock UI <username></code>	<p>Unlocks the admin user whose account is locked after the maximum attempt to login is reached.</p> <p>fmctl --unlock UI <username></p>

Rules, Notes and Limitations

Refer to the following rules and notes:

- To include special characters in the `fmctl` command line, enclose the string containing the special characters within single quotes. For example, to include the bang (!) special character in a password string, you must enclose the password string within single quotes, as shown in the following example:
fmctl set UI admin password 'admin!!'
- When you manually restart the rsyslog service or change any fmctl logging configuration parameters, a few GigaVUE-FM audit log messages will not be captured in the syslog. This occurs as a result of limitations of the library used for pushing GigaVUE-FM's audit logs to syslog.

This page intentionally left blank to ensure new chapters start on right (odd number) pages.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- [Documentation](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VÜE Community](#)

Documentation

This table lists all the guides provided for GigaVUE-FM software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view [What's New](#) to access quick links to topics for each of the new features in this Release; view [Documentation Downloads](#) to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE-FM 6.5 Hardware and Software Guides
<p>DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing Edit > Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p>
<p>Hardware</p> <p>how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE-FM devices; reference information and specifications for the respective GigaVUE-FM devices</p>
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide

GigaVUE-FM 6.5 Hardware and Software Guides

GigaVUE-TA200 Hardware Installation Guide

GigaVUE-TA200E Hardware Installation Guide

GigaVUE-TA400 Hardware Installation Guide

GigaVUE-OS Installation Guide for DELL S4112F-ON

G-TAP A Series 2 Installation Guide

GigaVUE M Series Hardware Installation Guide

GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW

Software Installation and Upgrade Guides

GigaVUE-FM Installation, Migration, and Upgrade Guide

GigaVUE-OS Upgrade Guide

GigaVUE V Series Migration Guide

Fabric Management and Administration Guides

GigaVUE Administration Guide

covers both GigaVUE-OS and GigaVUE-FM

GigaVUE Fabric Management Guide

how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features

Cloud Guides

how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms

GigaVUE V Series Applications Guide

GigaVUE V Series Quick Start Guide

GigaVUE Cloud Suite Deployment Guide - AWS

GigaVUE Cloud Suite Deployment Guide - Azure

GigaVUE Cloud Suite Deployment Guide - OpenStack

GigaVUE Cloud Suite Deployment Guide - Nutanix

GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)

GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

Universal Cloud Tap - Container Deployment Guide

GigaVUE-FM 6.5 Hardware and Software Guides

Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide

GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions

Reference Guides

GigaVUE-OS CLI Reference Guide

library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices

GigaVUE-OS Security Hardening Guide

GigaVUE Firewall and Security Guide

GigaVUE Licensing Guide

GigaVUE-OS Cabling Quick Reference Guide

guidelines for the different types of cables used to connect Gigamon devices

GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide

samples uses of the GigaVUE-FM Application Program Interfaces (APIs)

Release Notes

GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes

new features, resolved issues, and known issues in this release ;
important notes regarding installing and upgrading to this release

NOTE: Release Notes are not included in the online documentation.

NOTE: Registered Customers can log in to [My Gigamon](#) to download the Software and Release Notes from the Software & Docs page on to [My Gigamon](#). Refer to [How to Download Software and Release Notes from My Gigamon](#).

In-Product Help

GigaVUE-FM Online Help

how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to [My Gigamon](#). Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to [My Gigamon](#)
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to: documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	
For Online Topics	Online doc link	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>

For PDF Topics	Document Title	<i>(shown on the cover page or in page header)</i>
	Product Version	<i>(shown on the cover page)</i>
	Document Version	<i>(shown on the cover page)</i>
	Chapter Heading	<i>(shown in footer)</i>
	PDF page #	<i>(shown in footer)</i>
How can we improve?	Describe the issue	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings**  > **Support** > **Contact Support** in GigaVUE-FM.

You can also refer to <https://www.gigamon.com/support-and-services/contact-support> for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives:

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The **VÜE Community** is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)