

# GigaVUE-FM Installation and Upgrade Guide

**GigaVUE-FM** 

Product Version: 6.11 Document Version: 1.0

(See Change Notes for document updates.)

#### Copyright 2025 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/legaltrademarks. 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	Document	Date	Change Notes
Version	Version	Updated	
6.11	1.0	06/17/2025	The original release of this document with 6.11.00 GA.

# Contents

GigaVUE-FM Installation and Upgrade Guide	1
Change Notes	3
Contents	4
About this Guide	8
Supported Virtual Computing Requirements for GigaVU	JE-
FM	8
EULA Acceptance	9
	<b>Q</b>
	9
Dulos and Notos	01
Configuring LIEEL boot in GigaVLIE-EM	10
Installing CigoVUE-EM on VMware ESVi	12
	12
Derore you install	
VMware ESXi Hardware Requirements	12
Recommended Resource Requirements for Scaled Environments	
Rules, Notes, and Limitations	15
Reference Values for Disk Space Estimation	15
Deploy OVA file on VMware vCenter	16
Troubleshooting	19
Install GigaVUE-FM using ISO Image File on VMware ESXi Host	20
Install GigaVUE-FM using ISO Image File on VMware vCenter	20
Initial GigaVUE-FM Configuration	22
Perform Initial Configuration	
Redeploy GigaVUE-FM Instance (with VMs Already Deployed)	
Installing GigaVUE-FM on AWS	26
Before You Install	26
Install GigaVUE-FM on AWS	27
Subscribe to GigavUE-FM	27
	28
Before You Install	29
Install Glgavue-FM on Azure	

Install GigaVUE-FM Using Azure VM Dashboard	
Install GigaVUE-FM Using Azure Market Place	
Install and Upgrade GigaVUE-FM	
Cloud	
On-premise	
Installing GigaVUE-FM on GCP	
Before You Install	
Prerequisites for GigaVUE-FM	
Install GigaVUE-FM on GCP	
Installing GigaVUE-FM on OpenStack	
Before You Install	
Install GigaVUE-FM on OpenStack	
Initial GigaVUE-FM Configuration	
Installing GigaVUE-FM on Nutanix	
Before You Install	
Install GigaVUE-FM on Nutanix	
Installing GigaVUE-FM on MS Hyper-V	
Before You Install	
Windows Server Hardware Requirements	
Install GigaVUE-FM for Microsoft Hyper-V	
Install GigaVUE-FM from an ISO Image File	44
Enable UEFI Secure Boot	48
Add Additional Virtual Hard Disk and Install GigaVUE-FM	
Connect and Power On the GigaVUE-FM Virtual Machine	52
Disconnect the ISO Image File	
Initial GigaVUE-FM Configuration	54
Installing GigaVUE-FM on KVM	
Before You Install	
Limitations	57
System Requirements	57
Install GigaVUE-FM for KVM using ISO Image File	58
Initial GigaVUE-FM Configuration	65
Deploy Application Metadata Exporter (AMX) on KVM Hypervisor	67
Install GigaVUE-FM on KVM hypervisor	67
Upgrade GigaVUE-FM	
Important GigaVUE-FM Upgrade Guidance	70
Supported Upgrade Paths for GigaVUE-FM	71
Upgrade GigaVUE-FM from the GigaVUE-FM CLI	72
Upgrade GigaVUE-FM from the UI	74
Upgrade using image in External Image Server	75
Upgrade using image in Internal server	

Post-Upgrade Notes	
Upgrade GigaVUE-FM in Azure	
Upgrade Options in Azure	
Upgrade GigaVUE-FM from the UI	
Upgrade from External Image Server	
Upgrade with GigaVUE-FM as the Image Server	83
Upgrade GigaVUE-FM using Snapshot in Azure	84
Upgrade the GigaVUE-FM using the Snapshot method	
Stop GigaVUE-FM Instance	
Create Snapshot of the GigaVUE-FM Instance	
Upgrade GigaVUE-FM Instance	86
Upgrade GigaVUE-FM in AWS	
Upgrade Options in AWS	
Upgrade GigaVUE-FM	
Upgrade from External Image Server	
Upgrade with GigaVUE-FM as the Image Server	
Upgrade GigaVUE-FM using Snapshot in AWS	
At a Glance	
Stop GigaVUE-FM Instance	91
Create Snapshot of the GigaVUE-FM Instance	92
Lingrade GigaVIIE-EM Instance	97
Upgrade GigaVUE Fabric Components	94
Upgrade GigaVUE Fabric Components In GigaVUE-FM for AWS	<b>94</b>
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite	94 
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller	94 
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy	94 94 95 95 96
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure	94 94 95 95 96 98
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite	94 94 95 95 96 98 99
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller	94 95 95 95 96 98 99 99
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade UCT-V Controller	94 95 95 95 96 98 99 99 99
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy	94 94 95 95 96 98 99 99 99 99 99 90 90 91
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack Prerequisite	94 95 95 95 96 98 99 99 99 100 104
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack Prerequisite Upgrade UCT-V Controller	94 94 95 95 96 96 99 99 99 99 99 99 90 94 
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy	94 95 95 95 96 98 99 99 99 100 104 104 104 104
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE V Series Proxy Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy	94 94 95 95 96 96 99 99 99 99 99 99 99 99 90 94 94 95 95 95 95 95 95 95 95 95 95 95 95 95 95 96 96 91 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack Prerequisite Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack Prerequisite Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi Upgrade GigaVUE V Series Node for VMware NSX-T	94 95 95 95 96 98 99 99 99 100 104 104 104 104 106 108 114
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack Prerequisite Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack Prerequisite Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi Upgrade GigaVUE V Series Node for VMware NSX-T Upgrade GigaVUE V Series Node S Deployed using GigaVUE-FM	94 94 95 95 96 96 99 99 99 99 99 99 99 99 99 90 94 94 94 95 95 95 96 96 96 96 96 91 94 95 95 95 95 96 96 99 90 90 90 90 90 
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack Prerequisite Upgrade GigaVUE V Series Node and GigaVUE-FM for OpenStack Prerequisite Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi Upgrade GigaVUE V Series Node for VMware NSX-T Upgrade GigaVUE V Series Node Deployed using GigaVUE-FM	94 95 95 95 96 98 99 99 99 100 104 104 104 104 104 104 106 108 114
Upgrade GigaVUE Fabric Components Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure Prerequisite Upgrade UCT-V Controller Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack Prerequisite Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi Upgrade GigaVUE V Series Node for VMware NSX-T Upgrade GigaVUE V Series Node Deployed using GigaVUE-FM Upgrade GigaVUE V Series Node Deployed using VMware NSX-T Manager	94 94 95 95 96 98 99 99 99 99 99 99 99 99 100 104 104 106 108 114 115
<ul> <li>Upgrade GigaVUE Fabric Components</li> <li>Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS</li> <li>Prerequisite</li> <li>Upgrade UCT-V Controller</li> <li>Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy</li> <li>Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure</li> <li>Prerequisite</li> <li>Upgrade UCT-V Controller</li> <li>Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy</li> <li>Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy</li> <li>Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy</li> <li>Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack</li> <li>Prerequisite</li> <li>Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy</li> <li>Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy</li> <li>Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi</li> <li>Upgrade GigaVUE V Series Node for VMware NSX-T</li> <li>Upgrade GigaVUE V Series Node Deployed using GigaVUE-FM</li> <li>GigaVUE-FM Administrator Authentication by Platform</li> </ul>	94 95 95 95 96 98 99 99 99 100 104 104 104 104 104 104 104 104 104

Logging in to GigaVUE-FM Command Line Interface	118
Post Installation Configurations	
Install Custom Certificate	118
Pre-requisites	119
Steps	119
Install Rabbit MQ Certificate	120
Communication between GigaVUE-FM Load Balancer and Web Server .	121
Disable DNSSEC Updates	121
Configure rSyslog Server for Receiving TLS/SSL Packets	123
Reference	123
Setting the GigaVUE-FM Admin Password	124
GigaVUE-FM CLI Commands	125
fmctl	125
Backing Up Configurations	134
Additional Sources of Information	
Documentation	137
How to Download Software and Release Notes from My Gigamon	140
Documentation Feedback	140
Contact Technical Support	141
Contact Sales	142
Premium Support	142
The VÜE Community	142
Glossary	. 143

# 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 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

# Supported Virtual Computing Requirements for GigaVUE-FM

This section lists the minimum virtual computing resources required for installing GigaVUE-FM<sup>1</sup>.

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

<b>T</b>     <b>1</b> 0		e	- · ·	
Table I: Supported	Virtual (	Computina	Requirements	for GiaaVUE-FM

Minimum Virtual Computing Requirements				
Memory	Minimum 16GB memory			
Virtual CPU (vCPU)	2 vCPU			
Virtual Storage for Guest	80GB			
	• System Disk - 40GB			
	• Swap Disk - 4GB			
	• Data Disk - 40GB			
Virtual Network Interfaces	One vNIC using VMXNET3 (VMware 3rd Generation Paravirtual NIC)			

# EULA Acceptance

You can view the End User License Agreement (EULA) acceptance message only for the first time when you login after installing and upgrading the GigaVUE-FM. To use the GigaVUE-FM, you must agree with the EULA. Restoring a previous release's backup on the current GigaVUE-FM works like an upgrade. The End User License Agreement (EULA) process during this restoration is the same as during an upgrade.

# UEFI Boot

UEFI stands for Unified Extensible Firmware Interface. It stores all device initialization and start-up data in a .efi file on a special disk partition called the EFI System Partition (ESP). The ESP also holds the bootloader responsible for booting the operating system.

The primary purpose of creating UEFI is to overcome the limitations of BIOS and shorten system boot time. UEFI uses the GPT partitioning scheme and supports drive sizes that are much larger.

In addition, UEFI provides better security with the Secure Boot feature, preventing unauthorized applications from booting. However, the downside is that Secure Boot prevents dual booting because it treats other operating systems as unsigned applications.

UEFI runs in 32-bit or 64-bit mode, providing a graphical user interface.

### **UEFI Secure Boot**

Secure Boot is a Unified Extensible Firmware Interface (UEFI) feature that provides a verification mechanism for ensuring the device boots using only authorized firmware and software. It prevents running unauthorized, untrusted code. Without Secure Boot, malicious code can easily be executed, and Gigamon platforms can be easily compromised.

The following table provides the details of the platforms that support UEFI boot and UEFI secure boot:

#### Supported Platforms

Platforms	UEFI Boot	UEFI Secure Boot
AWS	Yes	Yes
Azure	Yes	Yes
Microsoft Hyper-V	Yes	Yes
OpenStack	Yes	Yes
Nutanix	Yes	Yes
KVM	Yes	Yes
GCP	Yes	Yes
GigaVUE-FM Hardware Appliance (GFM-HW1- FM010, GFM-HW1-FM001-HW, and GFM-HW2- FM001-HW)	Yes	Yes
VMware ESXi	Yes	Yes

#### Rules and Notes

- Fresh installations only support UEFI boot on any platform.
- Image upgrade deployments do not change the boot mode of a GigaVUE-FM system.
  - BIOS boot systems remain as BIOS boot
  - UEFI boot systems remain as UEFI boot.
- You can change a BIOS boot installation to UEFI boot by using the snapshot upgrade method, which is recommended only on AWS, and Azure platforms.
- Disabling UEFI Secure boot after deploying GigaVUE-FM in UEFI Secure boot mode is not recommended.
- Secure Boot in VMware ESXi is supported by virtual hardware version 13 or later.
- FMHA formation with a combination of UEFI Secure Boot GigaVUE Fabric Managers and Non-UEFI Secure Boot GigaVUE Fabric Managers of the same versions is allowed. However, the FMHA cluster cannot be named as a UEFI Secure Boot cluster.

### Configuring UEFI boot in GigaVUE-FM

Refer to the sections in the table to learn about how to configure UEFI boot in GigaVUE-FM in the following platforms:

Platforms	Refer to
AWS	You should change the instance from <b>m4.xlarge</b> to <b>m5.xlarge</b> . UEFI boot supports only <b>m5.xlarge</b> . For more information, refer to Recommended Instance Types for AWS in the sectionInstalling GigaVUE-FM on AWS
Azure	No changes in the configuration procedure.
Microsoft Hyper-V	You must specify the option Generation 2 in <b>Specify Generation</b> page. UEFI boot supports only Generation 2. For more information, refer toInstall GigaVUE-FM for Microsoft Hyper-V
OpenStack	OpenStack supports UEFI from the Wallaby version and RHSOP 17.01. The train version of OpenStack does not support UEFI boot. You must specify <b>hw_firmware_type=uefi</b> in the image property for GigaVUE-FM deployment in UEFI mode. For more information, refer to Installing GigaVUE-FM on OpenStack
Nutanix	You need to switch to UEFI mode when deploying the GigaVUE-FM. For more information, refer to Installing GigaVUE-FM on Nutanix
KVM	You need to switch to UEFI mode when deploying the GigaVUE-FM. For more information, refer to Installing GigaVUE-FM on KVM.
GCP	In GCP, you must set the flag: - <b>-guest-os-features='UEFI_COMPATIBLE'</b> . For more information, refer to Install GigaVUE-FM on GCP.
VMware ESXi	Support vSphere 6.5, virtual hardware version 13 or later. For more information, refer to Installing GigaVUE-FM on VMware ESXi. For information related to troubleshooting ESXi 7.0, refer to Troubleshooting section in Deploy OVA file on VMware vCenter.

# Installing GigaVUE<mark>-</mark>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
- Deploy 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 Hardware Requirements for minimum hardware requirements.

#### VMware ESXi Hardware Requirements

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

Hardware Requirements			
VMware Hypervisor	vSphere ESXi: v7.xx and above. Refer to Supported Hypervisors for VMware for more detailed information.		
СРИ	One or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled.		

Table 1: Hardware Requirements for VMware Hypervisor

Hardware Requ	irements
	<b>Note</b> : 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)   System Disk - 40GB  Data Disk - 40GB  Note: Increase the disk space depending on the configuration load requirements for the given GigaVUE-FM instance.
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 3)
CPU				
CPU count(minimum)	2	4	12	32
CPU Min speed (per CPU)	2.30GHz	2.30GHz	2.30GHz	2.0GHz
Memory				
Memory Size	16GB	32GB	128GB	128GB
Disk Space				
OS Disk Size (min)	40GB	40GB	40GB	40GB
Config Disk Size - 15 Days Data	80GB	620GB	1100GB	1100GB
Config Disk Size - 35 Days Data	160GB	1240GB	2200GB	2200GB
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.

#### GigaVUE-FM Installation and Upgrade Guide

Configuration	Basic Configuration	Medium Configuration	Large Configuration	Large Configuration (GigaVUE-FM Hardware Appliance 3)
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
Number of Worker Pods monitored	1 Cluster with 100 Nodes and 10000 pods with 2 rules	3 Clusters, each with 100 Nodes and 10000 pods with 2 rules.	_	_

#### 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 3)
СРИ				
CPU count(minimum)	2	4	12	32
CPU Min speed (per CPU)	2.30GHz	2.30GHz	2.30GHz	2.0GHz
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 need.

Configuration	Basic Configuration	Medium Configuration	Large Configuration	Large Configuration (GigaVUE-FM Hardware Appliance 3)
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
Марѕ	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
Devices	50	500	1000	3020

### Deploy 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 6.11, and then select **Deploy OVF Template**.

The Deploy OVF Template wizard opens.

- 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.
- 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.
- 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.

- 10. Verify the OVF template details, and then click **Next**. The **Select storage** page of the **Deploy OVF Template** wizard appears.
- 11. 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.

- 12. Select the datastore where the virtual machine's files will be stored.
- 13. Click Next. The Select networks page of the Deploy OVF Template wizard appears.
- 14. Set network mapping by doing either of the following, depending on how your 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. For the **IP protocol** drop-down list, ensure to maintain the default settings intact. Do not make any changes to the **IP protocol** drop-down list, as any changes may cause problems for vCenter.
- 16. Click **Next**. The **Customize template** page of the **Deploy OVF Template** wizard appears.
- 17. 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.
- 18. 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:
  - One numerical character
  - One upper case character
  - One lower case character
  - One special character (Example- !@#\$%^&\*)

**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:

• The system displays an error message in the GigaVUE-FM UI.

- 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.
- 19. (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.
- 20. (Optional) Complete the NTP configurations such as the IP address and version of the NTP server, and then click **Next**.



Figure 1 vSphere Client: Customize Template

**Note:** You can also choose to perform the IP Networking and NTP configurations by running the **fmctI 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.

21. 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.

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

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

#### Troubleshooting

1. What should be done when GigaVUE-FM does not load on ESXi 7.0?

When GigaVUE-FM 6.8 does not load due to the missing of AVX CPU flags on ESXi 7.0, perform the following steps to bring up GigaVUE-FM:

1. Deploy GigaVUE-FM 6.8.00 on VMware vCenter 7.0 using OVA.

**Note:** After deployment, don't power on the GigaVUE-FM until the following steps are verified.

- 2. Check the **Compatibility** version in the **Summary** tab of installed GigaVUE-FM; it should be greater than 13. If it is 13 or less than 13, do the following:
  - a. Click **Actions** > **Compatibility** > **Upgrade VM Compatibility** to upgrade the VM compatibility.

The VM Compatibility Upgrade message box appears.

- b. Click Yes to view the Configure VM Compatibility dialog box.
- c. Select the compatible version as **ESXi 7.0 and later** from the drop-down list box and click **OK**.
- 3. Enable EVC mode. To enable EVC mode for GigaVUE-FM, do the following:
  - a. Go to **Configure**> **VMware EVC** > **EDIT**. You can view the **Change EVC Mode** screen.
  - b. Click the radio button to Enable EVC for Intel Hosts.
  - c. Select Intel Ivy Bridge Generation from the drop-down list in the CPU Mode field.
  - d. Press **OK**.
- 4. Power on GigaVUE-FM and verify whether GigaVUE-FM loads without any issues.

Note: Alternatively, instead of using ESXi 7.0, you can upgrade using ESXi 7.2 or 7.3.

### 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.
- 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-FM6.11, and then and 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.
  - b. From the **Disk Provisioning** 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.

- c. Select a Network Adapter.
- d. In the **CD/DVD Drive**, select **Datastore ISO file** and the **CD/DVD Media** select the ISO image uploaded in Step 3.
- e. 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.
  - 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. 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.

#### Example: fmctl set hostname <host-name>

b. Enter the required domain name.

#### Example: fmctl set domain <domain-name>

- c. Decide whether to use DHCP or STATIC for the management interface. Choose one of the following options:
  - If you want to set DHCP the IPv4 Address or IPv6 Address, CIDR, Gateway, DNS Servers, and Search Domains are dynamically set up for the management interface.

#### Example: fmctl set ip dhcp

- If you want to set static ip for GigaVUE-FM, you must provide the following:
  - i. IPv4 Address or IPv6 Address, and the respective CIDR and Gateway.

#### Example: fmctl set ip static</P address>/<mask> <gateway>

#### Example: fmctl set ip6 static</Pv6 address>/<mask> <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.

#### Example: fmctl set nameservers <IP address>

iii. In the Search Domains field, provide the required DNS domains with spaces in between.
 Example: fmctl set searchdomain <domain-name>

d. You can choose to either enable or disable NTP using fmctl command.

#### Example: fmctl set ntp enable 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org

e. 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).

**Note:** You must reboot the GigaVUE-FM, when there is a change in the IP address of the GigaVUE-FM.

#### 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.

				ADD NEW DEVIC
> CPU	2 🗸			í
> Memory		$\sim$	GB v	
> Hard disk 1	40	GB 🗸		
> Hard disk 2	4	GB 🗸		
> Hard disk 3	40	GB ∽		
> SCSI controller 0	VMware Paravirtual			
> Network adapter 1	VM Network 🗸			Connected
> New Network *	VM Network $ \sim $			Connected
> CD/DVD drive 1	Datastore ISO File	~		Connected

- 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 Deploy 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.
- Install GigaVUE-FM on AWS describes the steps to deploy GigaVUE-FM on AWS and 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.

### Install GigaVUE-FM on AWS

You can launch GigaVUE-FM in AWS by subscribing to it in the marketplace.

Refer to the following topics for instruction on installing GigaVUE-FM in AWS:

- Subscribe to GigaVUE-FM
- Initial Configuration

#### Subscribe to GigaVUE-FM

You can deploy the GigaVUE Cloud Suite for AWS from the AWS Marketplace.

**Note:** Only users with **aws-marketplace:ViewSubscriptions** permission in their IAM policy can subscribe to GigaVUE products.

To subscribe to the GigaVUE-FM, 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. Select the latest version GigaVUE Cloud Suite BYOL version. For more information on Licensing, refer to Licensing GigaVUE Cloud Suite.
- 5. Click **View Purchase Options**. The terms and condition page is displayed.
- 6. Review the Terms and Conditions and then click "Accept Terms".
- 7. Review the summary and then click "Continue to Configuration".
- 8. In the **Configure this software** page, enter the following details for your deployment:
  - a. Set **Fulfillment Option** to the default value.
  - b. Select the latest version in the **Software Version** field.
  - c. Choose your deployment **Region**.
  - d. Click Continue to Launch.

- 9. In the **Configure this software** page, select the following details. Refer to Launch an instance using defined parameters in AWS documentation.
  - a. Select the Launch from Website option in the Choose Action field.
  - b. Select the instance type from the **EC2 Instance Type** drop-down list. Refer to Recommended and Supported Instance Types for AWS.
  - c. Choose the VPC for deploying GigaVUE-FM from the **VPC Settings** drop-down list.
  - d. In the Subnet Settings, choose your desired Subnet.
  - e. Configure the security group in the **Security Group Settings** to match your access and permissions needs. Refer to Security Group for more details.
  - f. Choose your preferred **Key Pair** for secure access to the instance.
  - g. In the **Advanced details** section, select **V2 only** from the Metadata version dropdown list.
  - h. Click Launch.

GigaVUE-FM is launched in AWS. You must perform the initial configuration to view the GigaVUE-FM UI.

#### Initial Configuration

It may take several minutes for the GigaVUE-FM instance to start up. Once it is up and running, you can verify that it is working properly by following these steps:

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

#### NOTE:

=

- 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). You can get the Instance ID of GigaVUE-FM in the EC2 Instances page.
- If GigaVUE-FM is deployed outside the AWS, use admin123A!! as the default admin password.

When you first log in to GigaVUE-FM, you will be asked to change your default password.

#### What to do Next:

Configure the required permission and privileges in AWS. For detailed instructions on configuring required AWS permissions and privileges for your chosen deployment option, refer to the following topics:

Deployment Options	Reference Topics
Acquire Traffic using UCT-V	Example: Traffic Acquisition using the UCT-V
Acquire Traffic using Customer Orchestrated Source	Example: Traffic Acquisition using the Customer Orchestrated Source
Acquire Traffic using Customer Orchestrated Source when configuring Gateway Load Balancer in AWS	Example: Traffic Acquisition using the Customer Orchestrated Source with GwLB
Acquire Traffic using Customer Orchestrated Source when configuring Network Load Balancer in AWS	Example: Traffic Acquisition using the Customer Orchestrated Source with NwLB
Acquire Traffic using Traffic Mirroring	Example: Traffic Acquisition using Traffic Mirroring
Acquire Traffic using Traffic Mirroring when configuring Gateway Load Balancer in AWS	Example: Traffic Acquisition using Traffic Mirroring and GwLB
Acquire Traffic using Traffic Mirroring when configuring Network Load Balancer in AWS	Example: Traffic Acquisition using Traffic Mirroring with Network Load Balancer

# Installing GigaVUE-FM on Azure

This section describes how to install GigaVUE-FM on Azure. 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 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.
System-assigned managed identity	Use a system-assigned managed identity when a resource needs to authenticate to other services, and you want the identity to be created and deleted with the resource.
	<b>Note:</b> If you update any role it would take more than an hour to reflect in GigaVUE-FM, however, if you use APP registration it would take between 5-10 minutes to update in GigaVUE-FM.
Virtual machine name	Enter a name for the VM.
Region	Select a region for Azure VM.
Security Type	To enable UEFI secure boot, select <b>Trusted launch virtual machines</b> from the drop-down list. Click <b>Configure security features</b> and ensure that the <b>Enable secure boot check box</b> is enabled.
Image	Select the latest GigaVUE-FM images.
	<b>Note:</b> You cannot select multiple images for a VM. Refer to Configure GigaVUE

#### GigaVUE-FM Installation and Upgrade Guide

Field	Description
	Fabric Components in Azure for more details on configuring GigaVUE V Series           Node, GigaVUE V Series Proxy, and UCT-V Controller in Azure.
Size	<ul> <li>The recommended instance types are as follows:</li> <li>GigaVUE-FM - Standard_D4s_v3</li> <li>UCT-V Controller - Standard_B1ms</li> <li>V Series Node - Standard_D4s_v4</li> <li>V Series Proxy - Standard_B1ms</li> </ul>
Authentication Type	<ul> <li>We support only SSH public key authentication type</li> <li>SSH public key <ul> <li>Enter the administrator username for the VM.</li> <li>Enter the SSH public key pair name.</li> </ul> </li> <li>Password <ul> <li>Enter the administrator username for the VM.</li> <li>Enter the administrator password.</li> </ul> </li> </ul>
Disks	
Disk Size	The required disk size for GigaVUE-FM is <b>2 x 40GB</b> .
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 <b>Subnet</b> and the <b>Public IP</b> 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 <b>Network Security Groups</b> . 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.

If GigaVUE-FM is deployed in Azure, 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.

### Install and Upgrade GigaVUE-FM

You can install and upgrade the GigaVUE-FM fabric manager on cloud platforms or onpremises.

You have the flexibility of installing GigaVUE-FM across various supported platforms. Additionally, you can effectively manage deployments in any of the cloud platform as long as there exists IP connectivity for seamless operation.

#### 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 toUpgrade 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 toUpgrade 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 describe 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: • GigaVUE-FM - <b>e2-standard-4</b>		
Boot Disk: Click Change.	Boot Disk: Click Change. Select the Custom Image tab.		
Image	Select the latest GigaVUE-FM images.		
	<b>Note:</b> You cannot select multiple images for a VM.		
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			

Parameter	Description
Networking	
Network Interface	Select the Network Interface, the <b>Network</b> and the <b>Subnetwork</b> values.
SSH Keys	<ul> <li>SSH keys</li> <li>o Enter the admin under username.</li> <li>o Enter the SSH public key under key.</li> </ul>
Disks	
Disk Size	The required disk size for GigaVUE-FM is <b>40GB</b> .
	<b>Note:</b> When using UEFI secure boot, you must include an additional disk with a minimum capacity of 40GB.
Security	
Turn on Secure Boot	Enable this option to use UEFI secure boot.

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.
- 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.
- 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: Retype new password: [admin0123 ~1\$

**Note:** You can also choose to perform the IP Networking and NTP configurations by running the **fmctl set ip** 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 Prism Central.
- 2. In Prism Central, select **Dashboard > Compute & Storage > VMs**. The **VMs** page appears.

**Note:** You can view the uploaded images under **Compute & Storage > Images**. For more detailed information on how to upload fabric images refer Upload Fabric Images.

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

#### GigaVUE-FM Installation and Upgrade Guide

### 4. In the **Configuration** tab, enter the following details:

Field	Description
Name	Enter a name for the VM.
Description	Enter description for the VM. (optional)
Cluster	Select the cluster in which you wish to deploy GigaVUE-FM.
Number of VMs	Enter the number of GigaVUE-FM you wish to deploy.
VM Properties	<ul> <li>CPU(s)—number of vCPUs required. Minimum value is 1 vCPUs. However, the recommended value is 4 vCPUs.</li> </ul>
	<ul> <li>Cores Per vCPU—number of cores per vCPU. Minimum value is 2 vCPUs.</li> </ul>
	• <b>Memory</b> —memory size of the vCPU(s). Minimum value is 16GB.

5. In the **Resources** tab, enter or select the following details:

Field	Description
Disks	Click <b>Attach Disk</b> . The Attach Disk dialog box opens. Enter or select the following details:
	• Type - Select Disk from drop-down menu.
	<ul> <li>Operation - Select Clone from Image from the drop-down. This allows you to clone the GigaVUE-FM qcow2 image which you have already uploaded.</li> </ul>
	<ul> <li>Image - Select the Image uploaded in the Upload Fabric Images section.</li> </ul>
	<ul> <li>Capacity - Enter the Capacity in GB. Minimum value is 40GB.</li> <li>Bus Type - Select the Bus Type as SCSI.</li> </ul>
	Click Save.
	Add additional disk:
	Click <b>Attach Disk</b> . Enter or select the following details:
	• Type - Select Disk from drop-down menu.
	<ul> <li>Operation - Select Allocate on Storage Container from the drop-down.</li> </ul>
	<ul> <li>Storage Container - Select the Image uploaded in the Upload Fabric Images section.</li> </ul>
	• <b>Capacity</b> - Enter the Capacity in GB. Minimum value is 40GB.
	• <b>Bus Type</b> - Select the Bus Type as SCSI.
Networks	Click <b>Attach to Subnet</b> . The <b>Attach to Subnet</b> dialog box opens. Enter or select the following details:
	• <b>Subnet</b> - Select the Subnet from the drop-down menu.
	Network Connection State - Ensure the status is Connected.
	<ul> <li>Assignment Type - Select the IP assignment type from the drop- down menu.</li> </ul>
	• <b>IP Address</b> - Enter the static IP address for VLAN. This field is enabled only if Assign Static IP is selected in the Assignment Type field.
Boot Configuration	Select the boot configuration:
	UEFI Mode - To enable UEFI boot mode, select the <b>UEFI Mode</b> option.
Shield VM Security Settings	Enable the <b>Secure Boot</b> check box to use the secure boot mode.

6. In the Management tab, enter or select the following details:

7.	Field	Description
	Categories	Search for the category to be assigned to the VM. The policies associated with the category value are assigned to the VM.
	Timezone	Select the time zone from the drop-down list.

- 8. Review the details in the review tab.
- 9. Click **Save**.
- 10. The new VM appears on the VMs list with the **Power State** as **Off**.
- 11. Select the new VM and then select **Actions > Power On**. The new VM is now Active.
- 12. Copy the IP address of the newly launched GigaVUE-FM and paste it on the browser to login to the GigaVUE-FM. You can login to GigaVUE-FM using the default user name **admin** and the default password admin123A!!.

You can also launch the GigaVUE-FM console using the following steps:

- Select the new VM launched in the Prism Central and then select Actions > Launch console. The GigaVUE-FM console appears.
- 2. 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.

# Installing GigaVUE<mark>-</mark>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
СРИ	One or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled.
	<b>Note</b> : 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).	
	<b>Note:</b> 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	84GB Virtual IDE (the Hyper-V default)	
Guest	• 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-FM ISO 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 10pening the Virtual Machine Wizard.

The New Virtual Machine Wizard opens.

ila.	Hyper-V Manager	_ <b>_</b> ×
File Action View Help		
Hyper-V Manager Woht2.HV06PU/ Import Virtual Machine Hyper-V Settings Virtual Switch Manager Virtual SAN Manager	Ninne Virtual Machine Hard Disk Floppy Disk III	Actions W2012-HYPERV New Import Virtual Machine Hyper-V Settings Virtual Switch Manager
Edit Disk Inspect Disk Stop Service Remove Server Refresh	The selected virtual machine has no checkpoints.	Virtual SAV Vananger      Virtual SAV Vananger      Edit Disk      Impect Disk      Stop Service      Remove Server
Help	atest Created: 8/10/2015 3:27:14 PM Clustered: No Version: 5.0	View View View View View View View View
	Generation: 1 Notes: None	FM VM 3.1 latest       Image: Connect       Image: Settings       Image: Start
Displays the New Virtual Machine Wizard.	ory inversioning inveptication in its investigation in the second s	> Move v

**Figure 1** Opening the Virtual Machine Wizard

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

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

Figure 2Before 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:** You must specify the option Generation 2 for UEFI boot. UEFI boot supports only Generation 2.

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 Wizardopens.

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 3Connect Virtual Hard Disk Page.

30	New Virtual Machine Wizard	×
Connect Virt	ual Hard Disk	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.	
	< Previous Next > Finish Cance	

Figure 3 Connect Virtual Hard Disk Page

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

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 4Install Options Page.

- 10. Use this dialog box to select the ISO image file for GigaVUE-FM. As shown in the figure Figure 4Install Options Page, set the following options:
  - a. Select the **Install an operating system from a bootable CD/DVD-ROM** option.
  - 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.

8e	New Virtual Machine Wizard
	Options
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options	You can install an operating system now if you have access to the setup media, or you can install it later.  Install an operating system later  Install an operating system from a bootable CD/DVD-ROM  Media  Physical CD/DVD drive:  Image file (,iso):  Civitisers Administrator/Downloads/fmaulso  Browse
Summary	Install an operating system from a bootable floppy disk     Media     Virtual floppy disk (.vfd):     Install an operating system from a network-based installation server
	< Previous Next > Finish Cancel

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.

### Enable UEFI Secure Boot

To enable UEFI Secure boot, follow the below steps:

- 1. In Hyper-V Manager, locate the **Virtual Machines** in the results pane, right-click the GigaVUE-FM virtual machine, and click the **Settings** option.
- 2. From the left navigation pane, select **Security**.
- 3. Under the **Secure Boot** section, check the **Enable Secure Boot** option.
- 4. Click **OK**.

### 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:

Settin	igs for GigaVUE-FM-5.8 on WIN-G8HUE7498IM
GigaVUE-FM-5.8	✓ 4 ► Q
<ul> <li>Hardware</li> <li>Add Hardware</li> <li>BIOS Boot from CD</li> <li>Memory 16384 MB</li> <li>Processor 1 Virtual processor</li> <li>IDE Controller 0</li> <li>Hard Drive GigaVUE-FM-5.8.vhdx</li> <li>Hard Drive cfile&gt;</li> <li>IDE Controller 1</li> <li>DVD Drive gigamon-gigavue-fm-5.8.0</li> <li>SCSI Controller</li> <li>Vetwork Adapter Intel(R) I350 Gigabit Network</li> <li>COM 1 None</li> <li>COM 2 None</li> <li>Diskette Drive None</li> <li>Mame GigaVUE-FM-5.8</li> <li>Integration Services Some services offered</li> <li>Checkpoint File Location C: \ProgramData \Microsoft\Win</li> </ul>	<ul> <li>Hard Drive</li> <li>You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.</li> <li>Controller:</li> <li>Location:</li> <li>[IDE Controller 0 v 1 (in use) v</li> <li>Media</li> <li>You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk is editing the associated file. Specify the full path to the file.</li> <li>Virtual hard disk:</li> <li>Virtual hard disk:</li> <li>Inspect Browse</li> <li>Physical hard disk:</li> <li>If the physical hard disk, you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disk, click Remove. This disconnects the disk but does not delete the associated file.</li> </ul>
	OK Cancel Apply

**Figure 6** Navigating to the New Virtual Hard Disk Wizard

The New Virtual Hard Disk Wizard opens.

<u>گ</u>	New Virtual Hard Disk Wizard	x
Before You B	Begin	
Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location Configure Disk Summary	This wizard helps you create a new virtual hard disk. Virtual hard disks provide storage for virtual machines and are stored on physical media as .vhd or .vhdx files.	
	< Previous Next > Finish Cance	I

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:
  - Create a blank virtual hard disk of size 41GB.
  - 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.

i a				Hyper-V Ma	anager				_ 0	ı x	٢
File Action View Hel	lp										
◆ ⇒ 🖄 🖬 🖬 🖬											
Hyper-V Manager		Virtual Machine					Actions				
W2012-HTPERV		Name A	Ctate	CDITIlizade	Assigned Memory	Untime	W2012-H	IYPERV		•	Ĥ
		FM	Off	CPO Osage	Assigned Memory	optime	New				
	1		FM on W2012-H	PERV - Virtual	Machine Connection	on 🗕	□ X	Cattings			
	File	Action Media V	iew Help				_	witch Manager			
	\$	0 0 0 1						AN Manager			
								Disk			=
								vice			
								Server			
			The virtual n	achine 'F	M' is turned o	off				•	
						511					
		То	start the virtual ma	chine, select 'St	art' from the Action	menu				•	
											Π
								vint			

- 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.
- 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. 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.

#### Example: fmctl set hostname <host-name>

b. Enter the required domain name.

#### Example: fmctl set domain <domain-name>

- c. Decide whether to use DHCP or STATIC for the management interface. Choose one of the following options:
  - If you want to set DHCP the IPv4 Address or IPv6 Address, CIDR, Gateway, DNS Servers, and Search Domains are dynamically set up for the management interface.

#### Example: fmctl set ip dhcp

- If you want to set static ip for GigaVUE-FM, you must provide the following:
  - i. IPv4 Address or IPv6 Address, and the respective CIDR and Gateway.

Example: fmctl set ip static

Example: fmctl set ip6 static</Pv6 address>/<mask> <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.

#### Example: fmctl set nameservers <IP address>

iii. In the **Search Domains** field, provide the required DNS domains with spaces in between.

### Example: fmctl set searchdomain <domain-name>

d. You can choose to either enable or disable NTP using fmctl command.

#### Example: fmctl set ntp enable 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org

e. 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).

**Note:** You must reboot the GigaVUE-FM, when there is a change in the IP address of the GigaVUE-FM.

# 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 using ISO Image File 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.
- Deploy Application Metadata Exporter (AMX) on KVM Hypervisor describes the steps deploy GigaVUE-FM in the KVM environment.

# 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)					
	■ V2.0.0					
CPU	One or more 64-bit x86 CPUs with virtualization assist (Intel-VT or AMD-V) enabled.					
	<b>Note</b> : 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).					
	<b>Note:</b> 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	<ul> <li>84GB</li> <li>System Disk - 40GB</li> <li>Swap Disk - 4GB</li> <li>Data Disk - 40GB</li> </ul>			
Virtual Network Interfaces	One vNIC			

## Install GigaVUE-FM for KVM using ISO Image File

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

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

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:

Virtual Machine Manager	9 🖲 😣
File Edit View Help	
🛒 💷 Open 🕨 🔝 🙂 👻	
Name  CPU usage	
▼ QEMU/KVM	
FM-5.8.01 Shutoff	

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.

New VM 😣
Create a new virtual machine Step 2 of 5
Our of the contract of the con
No device present 👻
O Use ISO image:
/home/kvm/gigamon-gigavue-fm-5.9.00-170003  Browse
Automatically detect operating system based on install media
OS type: Unknown Version: Unknown
Cancel Back Forward

#### Click Forward to continue.

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

GigaVUE-FM Installation and Upgrade Guide

	New	VM			8
Create a r Step 3 of 5	new virte	ual m	achine		
Choose Memory an	nd CPU se	ttings			
Memory (RAM):	8192	-	+		
	Up to 1285	67 MiB	available	on the host	
CPUs:	2	-	+		
	Up to 64 av	ailable			
C	ancel	В	ack	Forward	

Click **Forward** to continue.

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

New VM 😣
Create a new virtual machine Step 4 of 5
<ul> <li>Enable storage for this virtual machine</li> <li>Create a disk image for the virtual machine</li> </ul>
40.0 - + GiB
1794.6 GiB available in the default location O Select or create custom storage
( ) ( )
Cancel Back Forward

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**.

#### GigaVUE-FM Installation and Upgrade Guide

	New VM	8
Cre Step	ate a new virtual machine	
Ready to be	egin the installation	
Name:	generic	
OS:	Generic	
Install:	Local CDROM/ISO	
Memory:	8192 MiB	
CPUs:	2	
Storage:	40.0 GiB /var/lib/libvirt/images/generic.qcow2	
	Customize configuration before insta	u
- Naturark	coloction	
• Network		
Host de	evice enpsysoro: macvcap	
Source m	node: Bridge	
In m wor com	nost configurations, macvtap does not rk for host to guest network mmunication.	
	Cancel Back Finish	

The summary screen appears as shown in the following figure:

	secoocon QEMU/XVM	2
🚽 Begin Installation	Cancel Installation	
Cverview	Details XML	
OS information CPUs Memory Boot Options VirtIO Disk 1 SATA CDROM 1 VirtIO Disk 2 VirtIO Disk 2 NIC :e8:c2:d5 MIC :e8:c2:d5	Basic Details         Name:       secboot         UUID:       4abe7ff2-31e5-4552-a223-1b9e3187f84d         Status:       Shutoff (Shut Down)         Title:	
Display Spice Sound ich9 Console Channel qemu-ga Channel spice Video QXL Controller USB 0 USB Redirector 1 USB Redirector 2 RNG /dev/urandom	Hypervisor Details Hypervisor: KVM Architecture: x86_64 Emulator: /usr/bin/qemu-system-x86_64 Chipset: Q35 • Firmware: UEFI x86_64: /usr/share/OVMF/OVMF_CODE_4M.ms.fd	•
+ Add Hardware	Cancel	net Apply 🚽

- 7. To enable UEFI Secure boot, choose the **UEFI X86\_64:** option from the **Firmware** dropdown list.
- 8. Verify the options that you have selected, and then click **Add Hardware** to add the second disk.
- 9. In the Add New Virtual Hardware screen, set the disk size to **40** GiB.

	Add New Virtual Hardware 🛛 🕺 🕺
<ul> <li>Storage</li> <li>Controller</li> <li>Network</li> <li>Input</li> <li>Graphics</li> <li>Sound</li> <li>Serial</li> <li>Parallel</li> <li>Console</li> <li>Channel</li> <li>USB Host Device</li> </ul>	Add New Virtual Hardware  Storage  Create a disk image for the virtual machine  40.0 - + GiB  1794.6 GiB available in the default location  Select or create custom storage  Manage  Device type: Disk device
<ul> <li>USB Host Device</li> <li>PCI Host Device</li> <li>Video</li> <li>Watchdog</li> <li>Filesystem</li> <li>Smartcard</li> <li>USB Redirection</li> <li>TPM</li> <li>RNG</li> <li>Panic Notifier</li> </ul>	Bus type: IDE    Advanced options Cache mode: Hypervisor default   Cancel Finish

10. 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. 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.

#### Example: fmctl set hostname <host-name>

b. Enter the required domain name.

#### Example: fmctl set domain <domain-name>

- c. Decide whether to use DHCP or STATIC for the management interface. Choose one of the following options:
  - If you want to set DHCP the IPv4 Address or IPv6 Address, CIDR, Gateway, DNS Servers, and Search Domains are dynamically set up for the management interface.

#### Example: fmctl set ip dhcp

- If you want to set static ip for GigaVUE-FM, you must provide the following:
  - i. IPv4 Address or IPv6 Address, and the respective CIDR and Gateway.

Example: fmctl set ip static</P address>/<mask> <gateway>

Example: fmctl set ip6 static</Pv6 address>/<mask> <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.

#### Example: fmctl set nameservers <IP address>

- iii. In the Search Domains field, provide the required DNS domains with spaces in between.
   Example: fmctl set searchdomain <domain-name>
- d. You can choose to either enable or disable NTP using fmctl command.

#### Example: fmctl set ntp enable 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org

e. 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).

**Note:** You must reboot the GigaVUE-FM, when there is a change in the IP address of the GigaVUE-FM.

# Deploy Application Metadata Exporter (AMX) on KVM Hypervisor

For using the KVM hypervisor on GigaVUE-FM, the following sections provide information on deploying a fresh installation of GigaVUE-FM in the KVM environment. This setup enables the deployment of the Application Metadata Exporter (AMX) on a GigaVUE-FM Hardware Appliance.

### Install GigaVUE-FM on KVM hypervisor

### **Prerequisite:**

- 1. Download the recent GigaVUE-FM image from Gigamon Customer Portal and move qcow2 file to a desired location.
- 2. Install and enable Cockpit services on the KVM hypervisor. To enable Cockpit View on the KVM hypervisor, follow these steps:
  - a. Update the system package list.

sudo apt update

b. Install Cockpit and Cockpit-Machines.

sudo apt install -y cockpit cockpit-machines

c. Enable and start the Cockpit service.

sudo systemctl enable --now cockpit.socket

Once these commands are executed, access KVM using port 9090 in your browser: http://<your-server-IP>:9090

To create a VM in KVM hypervisor for deploying the GigaVUE-FM, follow the instructions.

Parameters	Instructions	Mandatory field
Connection	Select <b>System</b> .	Yes
Installation Type	Select <b>Cloud base image</b> from the drop-down list.	Yes
Installation Source	Select the location of the qcow2 image.	Yes
Operating System	Select the latest Rocky Linux version.	Yes

Parameters	Instructions	Mandatory field
Storage	Select Create new qcow2 volume.	Yes
Storage Limit	Enter the required storage limit (ex: 40 GiB).	Yes
Memory	Enter the required memory allocation (ex: 16 GiB).	Yes

Click **Create and edit** to edit the Virtual Machine. Modify the **Firmware** to **UEFI** and click **Install**.

Edit the VM as mentioned in the following table.

Parameters	Instructions	Mandatory field
Firmware	Select <b>UEFI</b> from the drop-down list	Yes
Disks		
Add new disk		
Size	Enter the disc size as required (ex: 40 GiB).	Yes
Format	Select the format (ex: <b>qcow2</b> ).	Yes
CPU		
vCPU Maximum	Enter the maximum number of vCPU's required (ex: 10).	Yes
vCPU Count	Enter the number of CPUs to allocate (ex: 8).	Yes

**Note:** The values mentioned for CPU, size, format, storage, and memory are sample entries and can be customized as required.

Click **Run** to deploy **GigaVUE-FM**. Copy the IP address of the newly launched GigaVUE-FM and paste it on the browser to login to the GigaVUE-FM. You can login to GigaVUE-FM using the default user name **admin** and the default password admin123A!!.

# Upgrade GigaVUE-FM

This section describes how to upgrade GigaVUE-FM to the latest revision in either a VMware ESXi host or in Microsoft HyperV environment.

### NOTE:

- **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.
  - When you migrate the GigaVUE-FM from the host that does not support AVX to the host that supports AVX, the GigaVUE-FM must be power cycled so that it will choose the current host's processor flags.

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.

Always take a snapshot of GigaVUE-FM before performing a version upgrade on GigaVUE-FM to ensure quick recovery in case of upgrade failures.

### GigaVUE-FM Upgrade Guidance for GigaVUE Cloud Suite

Starting from software version 6.10.00, the Secure Communication feature in GigaVUE-FM enhances security by enabling mutual Transport Layer Security (mTLS)-based authentication across GigaVUE Fabric Components. Upon upgrading to 6.10.00, this feature will be implemented. Before upgrading GigaVUE-FM and the fabric components, ensure that the necessary ports are open as mentioned in Network Firewall Requirement for GigaVUE Cloud Suite.

### 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 GigaVUE-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 v6.10.00.

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 Upgrade Paths for GigaVUE-FM.

# 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, if you want to upgrade your GigaVUE-FM 5.8.xx to 6.11.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 > 6.7.xx > 6.9.xx > 6.11.xx.

Upgrade from version 6.10.xx to 6.11.xx is also supported.

### 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 6.11.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 software image can be downloaded using the GigaVUE-FM CLI through a local FTP server. To fetch the latest release, do the following:

- 1. Locate and download the required software image from the Gigamon Community site.
- 2. Copy the image file to your local FTP 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-6.11 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-
6.11.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-6.11.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 the image that is available on the internal server.

You can upgrade an image in GigaVUE-FM from the UI in two ways:

- Upgrade using image in External Image Server
- Upgrade using image in Internal server

Before you upgrade GigaVUE-FM from the UI, follow the given rules and notes:

- You can upgrade your GigaVUE-FM instance to any of the subsequent two versions. For example, if you want to upgrade your GigaVUE-FM 5.8.xx to 6.10.xx, your supported upgrade path is 5.8.xx > 5.10.xx > 5.12.xx > 5.16.xx > 5.16.xx > 6.3.xx > 6.5.xx > 6.7.xx > 6.9.xx > 6.10.xx. You cannot downgrade.
- 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 5.16.0.0 image file at the end of the upgrade process.
- When upgrading from any previous version to 6.10 or above, the GUI may appear stuck in the reboot state, as a new certificate is generated using the GigaVUE-FM PKI service. Reload the page to update the status. This issue will not occur in subsequent upgrades.

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

#### **BEST PRACTICES**

- Before performing an upgrade, you must take a backup of GigaVUE-FM. For more information, refer to Backup and Restore.
- You must 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.
- 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 "Upgrade Software on a GigaVUE Node or a Cluster from GigaVUE-FM" in the GigaVUE-FM User's Guide.

## Upgrade using image in 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 GigaVUE-FM with an image stored on an external image server, you must sequentially perform the tasks in the following table:

S.No	Task	Refer to
1	Upload the image to external image server	Upload image to external image server
2	Add the image from the external server to GigaVUE-FM	Add image from external server to GigaVUE-FM
3	Upgrade GigaVUE-FM using external image	Upgrade GigaVUE-FM using External image

Upload image to external image server

- Upload the image to the external image server to make it available to GigaVUE-FM. Register on the Gigamon Customer Portal to obtain software images 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.

Add image from external server to GigaVUE-FM

To add the image from the external server, perform the following steps:

- 1. On the left navigation pane, click  $^{\textcircled{1}}$
- 2. Go to System > Images > External Servers.
- 3. Click Add. The Add External Server page appears.
- 4. In the Add External Server Page enter the following details:
- 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.
- 5. Click **OK**.

The External Server page displays the newly added external server.

Upgrade GigaVUE-FM using External image

- 1. Click the Profile @• options on the top navigation bar.
- 2. Select **Upgrade** from the drop-down list box to view the **Software Upgrade** page.

The **Software Upgrade** page provides the GigaVUE-FM details such as **Host Name**, **Node Status**, **IP Address**, **Role**, **System Uptime**, and **Version**.

- 3. Select the image server type as **External Image Server** from the **Image Server Type** drop-down list box.
- 4. Select the server in which image is stored from the **Image Server** drop-down list box.

**Note:** If the image server is not available in the Image Server drop-down list box, Click **Add External Server** and enter the details provided in **Step 5** in the section Add image from external server to GigaVUE-FM

- 5. Enter the path used for storing the image in the **Image File Path**.
- 6. Click Start Upgrade.

A confirmation message appears to refrain from performing any task during the process of upgrade.

7. Click **OK**.

GigaVUE-FM notifies the various stages of theupgrade and also the completion of the upgrade process.

# Upgrade using image in Internal server

This section provides the steps for upgrading GigaVUE-FM when the image is available in the internal 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 store the image in your machine and point to it as if it were an external server as follows :

- 1. Add the GigaVUE-FM 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, you must sequentially perform the tasks in the following table:

S.No	Task	Refer to
1	Download the Image	Download Image
2	Upload the image file to GigaVUE-FM	Upload the image file to

S.No	Task	Refer to
		GigaVUE-FM
3	Upgrade GigaVUE-FM using Internal image	Upgrade GigaVUE-FM using Internal image

#### Download Image

Download the images from the Gigamon website and place them where they can be uploaded to GigaVUE-FM. To obtain software images, register on the Gigamon Customer Portal and download the software.

Upload the image file to GigaVUE-FM

To upload the images file to GigaVUE-FM, follow these steps:

- 1. On the left navigation pane, click 🕸 .
- 2. Go to **System > Images > Internal Image Files** and do the following:
  - a. On the Internal Image File page, click **Upload**.
  - b. Click **Choose** to locate the image file on the **Upload Internal Image Files** page.
  - c. Click **OK** to upload the file. The page displays the progress of the upload.

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

#### Upgrade GigaVUE-FM using Internal image

- 1. Click the Profile Or options on the top navigation bar and select **Upgrade**.
- 2. Select **Upgrade** from the drop-down list box to view the **Software Upgrade** page.

The **Software Upgrade** page provides the GigaVUE-FM details such as **Host Name**, **Node Status**, **IP Address**, **Role**, **System Uptime**, and **Version**.

- 3. Select the image server type as **Internal Image Server** from the **Image Server Type** drop-down list box.
- 4. From the **Version** drop-down list, select the version to which you are upgrading.
- 5. Click Start Upgrade.

**Note:** If the image server is not available in the Image Server drop-down list box, Click **Add Internal Server** and perform the actions provided in **Step 2** in the section Upload the image file to GigaVUE-FM

A confirmation message appears to refrain from performing any task during the upgrade process.

#### 6. Click **OK**.

**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.

GigaVUE-FM notifies the various stages of upgrade and also the completion of the upgrade process.

۲	Software Upgrade						Q Search	@ ~
<u>dd</u>								
N. S.	(i) After the completion of t	he process, the page will automa	tically redirect to the FM dashboard.		×			
			Upgr	rading In Progress				
			¥	fôt	C			
			Downloading (2/3)	Installation	Reboot			
	Software Upgrade In	detail					Hide	details
Ð	HOST NAME	NODE STATUS	STATUS DESCRIPTION	ROLE	APPLICATION STATUS	IP ADDRESS	6	3
	gigavue-fm-51401	Standby	Ø Downloaded	Active Eligible	Up			
£93	qiqavue-fm-51402 FM Instance: GigaVUE-FM	🐼 Standby	O Downloading	Active Eligible	αU	Last Update	<b>l:</b> Jan 26, 2022 17:4.	1:16 CST

**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.

# 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 on Azure.

Refer to the following sections for details:

- Upgrade Options in Azure
- Upgrade GigaVUE-FM from the UI
- Upgrade the GigaVUE-FM using the Snapshot method
- Stop GigaVUE-FM Instance
- Create Snapshot of the GigaVUE-FM Instance
- Upgrade GigaVUE-FM Instance

# Upgrade Options in Azure

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

- Upgrade from External Image Server
- Upgrade with GigaVUE-FM as the Image Server
- Upgrade the GigaVUE-FM using the Snapshot.

# 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.

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

- In place GigaVUE-FM upgrade is supported from GigaVUE-FM version 6.6 to a later releases.
- 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.

# 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.

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 GigaVUE-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:	NewExternalServer	~	
Image File Path:	/ <image path=""/> / <image name=""/>		

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

- 3. On the GigaVUE-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.

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

1. Download the images from the Gigamon website and store them in the instance where GigaVUE-FM is installed.

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 GigaVUE-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:	Internal 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.

**Note:** If you are using FireFox, clear the cache before upgrading to prevent issues with the browser.

# 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 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 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**.

# Upgrade GigaVUE-FM in AWS

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

Refer to the following sections for details:

- Upgrade GigaVUE-FM using Snapshot in AWS
- Upgrade from UI. For more information on upgrading from UI, refer to the Upgrade from UI topic in GigaVUE-FM Installation and Upgrade Guide.

# Upgrade Options in AWS

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

- Upgrade from External Image Server
- Upgrade with GigaVUE-FM as the Image Server
- Upgrade the GigaVUE-FM using the Snapshot.

# Upgrade GigaVUE-FM

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.

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.

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  $rac{oldsymbol{arphi}}{oldsymbol{arphi}}$ .
- 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 GigaVUE-FM Image Upgrade page as shown in the following figure.

	Software	Upgrade	
	Imag	e File	
	Select the file server where you	have uploaded the image file.	
Image Server:	NewExternalServer	~	
Image File Path:	/ <image path=""/> / <image name=""/>		

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

- 3. On the GigaVUE-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.

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

1. Download the images from the Gigamon website and store them in the instance where GigaVUE-FM is installed.

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 GigaVUE-FM Image Upgrade page, click in the **Image Server** field and select **Internal Image Server**.

	Software Upgra	ade
	Image File	9
Select the fi	ile server where you have u	ploaded the image file.
Image Server:	Internal 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.

After upgrading GigaVUE-FM, you must also upgrade any deployed GigaVUE-VMs. Otherwise, maps may not work and the GigaVUE-VMs 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*.

**Note:** If you are using FireFox, clear the cache before upgrading to prevent issues with the browser.

# 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 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 GigaVUE-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 GigaVUE-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.
  - **Network** Select the VPC where you want to launch the AMI.
  - **Subnet** Select the management subnet that the instance will use after launch. (Required)
  - Auto-assign Public IP— Select Enable.
  - **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.
- 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 section in GigaVUE Cloud Suite Deployment Guide - AWS.
- 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 for VMware NSX-T

# Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V SeriesNodes. 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.

- a. Under Controller Versions, click Add.
- b. 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.
- c. 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 components present in the VPC. If the instance type cannot support so many Virtual Machines, you can choose to upgrade the fabric components 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**

۲	AWS > Monitoring Domain						ର <i>ଅ</i> ମ୍ <sup>4</sup> ®•
<u>lad</u>						New	Actions  G-vTAP Agents Refresh Inventory
2	<ul> <li>Monitoring Domain</li> </ul>	Connection	Name	Management IP	Туре	Version	Edit Monitoring Domain
<i>.</i>	× 🖌 M02						Edit Fabric
	~	Publical menora					Delete Monitoring Domain
-		Count Annual					Delete Fabric
			Gigamon-G-vTapController-1	172.15.24.79	G-vTap Controller	1.8-1	Upgrade Fabric Dk
			Gigamon-VSeriesProxy-1	172.15.24.169	V Series Proxy	2.3.0	Ok
			Gigamon-VSeriesNode-1	172.15.24.68	V Series Node	2.3.3	⊘ Ok

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

Upgrade		
Current Version	2.3.0	
Image	Select an image	
Change Instance Type		
Batch Size	1	
Series Node		
Current Version	222	
Image	Select an image	
Change Instance Type		
Batch Size	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 to the *GigaVUE-FM Version Compatibility* section in the **Prerequisites for GigaVUE Cloud Suite for Azure**.

#### **IMPORTANT NOTE:**

=

Before upgrading the Fabric Components to version 6.10.00 or above, ensure the following actions are performed:

- Create Token in GigaVUE-FM for UCT-V Installation and update it in the configuration file. Refer to UCT-V-VSN.html for more details.
- Create Tokens for deploying the Fabric Components using Third Party Orchestration. Refer to Token-based Authentication for more details.
- Open the required ports in the cloud platform. Refer to Network Firewall Requirement for GigaVUE Cloud Suite for more details.

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.

- a. In the Azure Fabric Launch Configuration page, 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 **Size** drop-down list, select a size for the UCT-V Controller. The default size is Standard\_Bls.
- 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		
			×
	Image	Select image	
	Size	Standard_B1s 👻	
	Number of Instances	1	
			×
	Image	gigamon-inc-g-tap-cnttr-1.8-2	
	Size	Standard_B1s +	
	Number of Instances	1	
Management Culturat			
Management Subnet	IP Address Type	Private Public	
	Subnet	mgmt -	
Additional Subnets			
	Subnet 1	traffic1 -	
	Security Groups	[Initia Milli, Editorya Marcul, 31303]	
Tags			

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.

- 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 **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* in GigaVUE Cloud Suite Deployment Guide - Azure 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**

	Azure > Monitoring Domain					୯ <i>ପ</i> ଼ ⊜∙			
<u></u>								New	Actions  Refresh Inventory
2	~	$\checkmark$	Monitoring Domain	Connection	Name	Management IP	Туре	Version	Edit Monitoring Domain
. K.	~	$\checkmark$	md						Edit Fabric
	~			Auto_Vnet_Edhaya_Manua_					Delete Monitoring Domain
					Circura C . Tes Centrelle	100.010	C . The Controller	10.2	Delete Fabric
					Gigamon-G-v rapcontrolle	1000.19	G-viap Controller	1.8-2	Upgrade Fabric
					Gigamon-VSeriesProxy-2	40.83.219.216	V Series Proxy	2.3.2	⊘ Ok
					Gigamon-VSeriesNode-2	104.42.183.63	V Series Node	2.3.2	⊘ Ok

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

#### Fabric Nodes Upgrade

Series Proxy	
Upgrade	
Current Version	2.3.0
Image	gigamon-gigavue-vseries-proxy-2.3.2-284364
Change Size	
Batch Size	1
Series Node	
Current Version	2.3.0
Image	gigamon-gigavue-vseries-node-2.3.2-284421
Change Size	
Batch Size	1
0.111.10	



- 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 SeriesProxy/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 addressess 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 Proxys 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 Statu	S		
Monitoring Domain: md			
Start Time	2021-10-1	1 20:58:56	
End Time	2021-10-1	121:04:03	
Status	Fabric upgra successfully	ade completed	
	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 upgradeGigaVUE 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.

#### **IMPORTANT NOTE:**

Before upgrading the Fabric Components to version 6.10.00 or above, ensure the following actions are performed:

- Create Token in GigaVUE-FM for UCT-V Installation and update it in the configuration file. Refer to Install UCT-Vfor more details.
- Create Tokens for deploying the Fabric Components using Third Party Orchestration. Refer to Configure Tokens for more details.
- Open the required ports in the cloud platform. Refer to Network Firewall Requirement for Cloud Suite] for more details.
- When using FMHA configuration, follow the steps given provided in the Configure Secure Communication between Fabric Components in FMHA section.

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		
			×
	Image	Select image	•
	Flavor	Select flavor	-
	Number of Instances	1	
			×
	Image	gigamon-gvtap-ovs-cntlr-1.8-2	•
	Flavor	m1.small	-
	Number of Instances	1	
Management Network	IP Address Type	Private Floating	
	Network	mgmt-test-network	-
	Floating IPs	10.115.176.108 ×	•
Additional Network(s)			
Tags			

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:

- 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**

۲	Oper	nStack	> Monitoring Domain						ର <i>ପ</i> ଠ଼ <sup>™</sup> ®⁺
<u>lad</u>							New	Actions  G-vTAP Agen	ts (Refresh Inventory)
4	~	$\checkmark$	Monitoring Domain	Connection	Name	Management IP	Туре	Edit Monitoring Domain	Status
~	~		md201					Edit Fabric	
	~			conn201				Delete Monitoring Domain	Connected
					Gigamon-G-vTapContro	10115176125	G-vTap Controller	Delete Fabric	⊘ Ok
					Gigamon-VSeriesNode-1	10115176129	V Series Node	Opgrade Pablic	⊘ Ok
								•	
Ð									
\$									
FM Inst	ance: Gig	aVUE-F	М						

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	
		Lingrade Cancel
		opgrade Cancer

- 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

This section explains the available methods to upgrade the GigaVUE V Series Nodes and provides instructions on how to upgrade GigaVUE V Series Nodes.

#### **IMPORTANT NOTE:**

=

Before upgrading the Fabric Components to version 6.10.00 or above, ensure the following actions are performed:

- Open the required ports in the cloud platform. For details, refer to .
- When using FMHA configuration, follow the steps provided in the Configure Secure Communication between Fabric Components in FMHA section.

#### Update GigaVUE V Series Nodes

Use one the following two options:

- 1. Upgrade all the GigaVUE V Series Node in a monitoring Domain:
  - a. Select the Monitoring Domain.
  - b. Select Actions > Upgrade Fabric.
2. Upgrade a single or a group of GigaVUE V Series Node. When upgrading a group of GigaVUE V Series Nodes, ensure all the GigaVUE V Series Nodes deployed on the same ESXi hosts are selected.

#### **Upgrade Considerations**

•

- 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 entire host and upgrade all the GigaVUE V Series Node deployed in that particular host.
- When multiple GigaVUE V Series Nodes are deployed on the same ESXi host and only if a part of GigaVUE V Series Nodes are selected in that particular host, then the **Upgrade Fabric** button is disabled.
- 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 when the host is out of the maintenance mode.
- **Note:** GigaVUE-FMsupports only (n, n-1, n-2) GigaVUE V Series Node versions.

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 or an entire host and select Actions.

3. From the drop-down list, select **Upgrade Fabric.** The **V Series Node Upgrade Task** dialog box appears.

eries Nodes Upgrade Task		
Name*	Enter a name	
lmage*	gigamon-gigavue-vseries-nod	•
Name Server	Use Comma to seperate values	
Change Form Factors		*
Default Form Factor ①	Use Current	•
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
	Upgra	de Cancel

- 4. Enter a name for the V Series Node upgrade task.
- 5. Select the latest GigaVUE V Series Node OVA image from the **Image** drop-down list.**Note:** 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. (Optional) If you want to modify the form factor (instance) size, select 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.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.

8. Select **Upgrade** to launch the GigaVUE V Series Node upgrade.

**Note:** Both the new and the current GigaVUE 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.

#### GigaVUE-FM Installation and Upgrade Guide

htt							New	v Actions V	Refr	resh Inventory
A.		Monitoring Domain	Connections	Host	Name	Management IP	Tunnel IP	Туре	Version	Status 🕲
<b>₩</b>	$\sim$	md1								Upgrade Status
	$\sim$		con1							⊘ Connected
	$\sim$			10.115.81.184						
					VSeries	10.114.82.69	10.114.84.3	V Series Node	6.6.00	Ø upgrading
					VSeries.new	10.114.84.88	10.114.84.93	V Series Node	6.6.00	Ø upgrading
	$\sim$			10.115.81.185						
					VSeries.new	10.114.82.143	10.114.84.86	V Series Node	6.6.00	Ø upgrad
					VSeries.s	10.115.80.190	10.115.80.191	V Series Node	6.6.00	Ø upgrading

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_GigaVUE_VSERIES_Node   SUCCESS	
Clear	
Summary Success: 2 Failed: 0 In Progress: 0 Total: 2	
Node Statuses	
Node Status	
VSeries.vp-redscvr- OK VSeries.vp-redscvr- renamed2 OK	
✓	
✓ Upgrade   IN_PROGRESS	
Summary	
Success: 0 Failed: 0 In Progress: 1 Total: 1	
Node Statuses	
Node Status	
VSeries.vp-redscvr- upgrade launching	

- Select **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, select **Retry** on the **V Series Node Upgrade Status** dialog box.

V Casta Nada Unanda

**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.

Current Version	2.3.2
Use External Image	No No
	Select an image
Change Form	gigamon-gigavue-vseries-node-2.3.1-275864_amd64.ova>
Factors	gigamon-gigavue-vseries-node-2.3.3-284615_amd64.ova>

- 3. 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.
- 4. 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**.

5. 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	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 predefined 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.

		Values by Platform and Mode (GUI/CLI)				
Mod e	Credenti al	AWS	Azure	VMware OVA Deployments	OpenStac k	Other (non- OVA) Deploymen ts
CLI	Usernam e	gigamon	specified during deployment.	admin	admin	admin
	Passwor d	no password	specified during deployment.	specified during deployment	admin123A!!	admin123A!!

	SSH Public Key	specified during deploymen t	specified during deployment	specified during deployment	no initial value	no initial value
	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 authenticat ion 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 configu re both, but you must config ure at least one of them. If you configure both, then you can use either method to access the GigaVUE-FM CLI.	Password change is required on first login.	Password change is required on first login.
GUI	Usernam e	admin	admin	admin	admin	admin
	Passwor d	<aws Instance ID&gt; of GigaVUE-F M virtual instance</aws 	admin123A!!	admin123A!!	<pre><openstack id="" instance=""> of GigaVUE-FM virtual instance, reverts to 'admin123A!! ' if no metadata service is available.</openstack></pre>	admin123A!!
	Rules & Notes					

# Logging in to GigaVUE-FM Command Line Interface

Users of GigaVUE-FM 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

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
- If the private key is encrypted, you must decrypt it before replacing the localhost.key file. You can use the following **openssi** command to decrypt the private key:

```
openssl rsa -in [original.key] -out [new.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.
- You must bundle the certificates in the following order without any space:
  - Server certificate (at the top)
  - Intermediate certificates
  - Root certificate (at the bottom)
- 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
```

 When using GigaVUE Cloud Suite, run the following commands to ensure that GigaVUE-FM continues to communicate securely with all the fabric components after certificate replacement.

**Note:** Ensure that you run the following commands before restarting the Apache server.

```
curl --location 'https://<FM-
IP>/api/v1.3/cloud/nodes/certificate/clientCa' \
--header 'Authorization: Bearer <YOUR_TOKEN>' \
--form 'caCertificate=@</path/to/localhost.crt>'
```

- 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 <code>/etc/gigamon</code> directory. Change the access rights to <code>chmod 644</code>.

### 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.

### Communication between GigaVUE-FM Load Balancer and Web Server

After GigaVUE-FM is installed, communication is established between GigaVUE-FMLoad 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"} '
```

### Disable DNSSEC Updates

You may observe that GigaVUE-FM connects to the root DNS servers to update the DNSSEC signatures. This process is managed by the unbound-anchor.service, which, along with unbound-anchor.timer, automates the unbound's root trust anchor updates for DNSSEC.

You can disable these services if you prefer that GigaVUE-FM should not connect to the root DNS servers. This prevents automatic root anchor updates, but it may weaken DNSSEC validation. In such cases, you must manually update the root anchor.

**Note:** These changes will not persist after a GigaVUE-FM upgrade. This procedure serves as a temporary workaround if the actions of the **unbound-anchor.service** are not desirable.

To disable the DNSSEC updates:

- 1. Log in to the GigaVUE-FM CLI.
- 2. Run the following commands:

```
sudo systemctl disable --now unbound-anchor.service
sudo systemctl stop unbound-anchor.timer
sudo systemctl disable unbound-anchor.timer
```

After completing these steps, GigaVUE-FM will no longer attempt to connect to the root DNS servers for DNSSEC updates. Ensure that you manually update the root anchor as needed to maintain DNSSEC validation.

# 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.

The steps are described in the following table:

	Steps	Details
1	Copy the generated certificates in to the path.	<pre>sudo cp ca.pem rservtls-cert.pem rservtls-key.pem /etc/pki/tls/private/</pre>
2	Run the <i>fmctl</i> command to configure syslog server.	fmctl logging <rsyslog server-ip="">:514 tls</rsyslog>

# 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.

**Note:** If you enter an incorrect password three times, your account will be locked for 10 minutes as a security measure. After this 10-minute lockout period, you can attempt to log in again using the correct password.

### 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>]

CHAPTER 10 | (Undefined variable: General.UserGuideTitle)

list [details] [<filename>]
install <filename> [next|location {1|2}]
boot [next|location {1|2}]
delete [force] <filename>
{move|rename} <old filename> <new filename>
show

logging [<fqdn>[:<port>]] [facility <facility>] [priority <priority>] [udp|tcp|tls]

logging <ipaddress> [port <port number>] [facility <facility>] [priority <priority>] [udp|tcp|tls]

no logging <fqdn>[:<port>]

no logging <ipaddress> [port <port number>]

reset factory halt

set crypto enable

get crypto

set audit network enable

set audit network disable

get audit network

set crl enable

get crl

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 [<server1>[,<server2>[,...]]]
set ntp enable [version <version_number>] [<server>[:<key_id>:<key_type>:<key_value>[,...]]]
set ntp update [version <version_number>] [<server>[:<key_id>:<key_type>:<key_value>]]
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>
```

**Note:** You must reboot the GigaVUE-FM, when there is a change in the IP address of the GigaVUE-FM.

Argument	Description
configuration [backup restore]	Backs up and restores the configurations such as management interface, hostname, domain, IP, search domains, and NTP.
	For example, use the following command to back up the system configurations:
	fmctl configuration backup <absolute backup="" file="" name="" of="" path=""></absolute>
	Use the following command to restore the system configurations from the backup:
	fmctl configuration restore <absolute backup="" file="" name="" of="" path=""></absolute>
image fetch <download uri=""> [<filename>]</filename></download>	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:
	[protocol]://username[:password]@hostname:/path/filename
	For example, the following command retrieves the image file named myimage from the FTP server at 192.168.1.10 using the <b>robh</b> account with the <b>xray</b> password:
	fmctl image fetch ftp://robh:xray@xxx.xxx.x.x/myimage

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

Argument	Description
	You can also use the <b><filename></filename></b> argument to give the retrieved file a new name on GigaVUE-FM. For example, the following command retrieves <b>myimage</b> and names it <b>newconfig</b> :
	fmctl image fetch scp://bbochy:catchl@xxx.xxx.x.x/myconfig newconfig
	<b>Note:</b> You cannot retrieve a file with the same name as an existing configuration file.
image list	Provides the list of image file names available in GigaVUE-FM.
	For example:
	fmctl image list
image install <filename></filename>	Installs the image file.
[next location {1 2}]	For example, use the following command to install the image file on the next partition:
	fmctl image install gigamon-gigavue-fm-5.8.00-160194-trial.img next
	Use the following command to install the image file on the specified partition:
	fmctl image install gigamon-gigavue-fm-5.8.00-160194-trial.img location 1
	<b>Note:</b> Ensure that your current partition is not the same as the partition you specified for installation. Else, an error is displayed.
image boot [next location {1 2}]	Boots the image file on the specified partition. Ensure that the partition has the installed image file.
	For example, use the following command to boot the image file on the next partition:
	fmctl image boot next
	Use the folloaing command to boot the image file on the specified partition:
	fmctl image boot location 1
	Note: GigaVUE-FM reboots immediately.
image delete [force] <filename></filename>	Deletes the named image file.

Argument	Description
	For example:
	fmctl image delete myimage
image {move rename} <old filename&gt; <new filename=""></new></old 	Moves or renames the specified image file. For example, the following command renames myimage as newimage:
	fmctl image rename myimage newimage
image show	Displays the last boot partition.
	For example:
	fmctl image show
show securebootstatus	Displays whether UEFI secure boot is enabled or not.
	For example:
	fmctl show securebootstatus
logging [ <fqdn>[:<port>]] [facility</port></fqdn>	Configures the logging server for sending events and audit logs to the remote server.
<facility>] [priority <priority>]</priority></facility>	For Example 1:
[uapitcpitis]	fmctl logging 1.2.3.4:6514 facility auth priority debug tcp
	Example 2:
	fmctl logging 1.2.3.4:6514 tcp
	Note: Don't use '*' in the command. It is the default one for facility and priority .
	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 <b>tls</b> . 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.
logging <ipaddress> [port <port number&gt;] [facility <facility>] [priority <priority>] [udp tcp tls]</priority></facility></port </ipaddress>	Configure the Syslog server with an IPv4 and IPv6 address. You must use only this command when you configure the IPv6 address.

Argument	Description
	For example:
	fmctl logging <ipv4 address="" ipv6="" or=""> port 6514 tls</ipv4>
	<b>Note:</b> If IPv6 syslog server is configured in 6.9 version and then upgraded to 6.11, you must reconfigure the IPv6 syslog server using the new fmctl command.
no logging <ipaddress> [port <port< th=""><th>Removes the logging server configuration when you use IPv4 or IPv6 address.</th></port<></ipaddress>	Removes the logging server configuration when you use IPv4 or IPv6 address.
number>]	For example: fmctl no logging <ipv4 address="" ipv6="" or=""> port 6514</ipv4>
no logging <fqdn>[:<port>]</port></fqdn>	Removes the logging server configuration.
	For example:
	fmctl no logging 1.2.3.4:6514
reset factory halt	Resets the GigaVUE-FM instance to the default configuration and shuts down the system.
	For example:
	fmctl reset factory halt
set crypto enable	Enables the crypto mode in GigaVUE-FM.
get crypto	Returns the response for API.
set audit network enable	Enables the network audit logs in GigaVUE-FM.
set audit network disable	Disables the network audit logs in GigaVUE-FM.
get audit network	Returns the response for API.
set crl enable	Enables the CRL validation in GigaVUE-FM.
set crl disable	Disables the CRL validation in GigaVUE-FM.
get crl	Returns the Response for API.
set UI admin password <new password&gt;</new 	Configures a new admin password for the GigaVUE-FM UI only.

Argument	Description	
	For information on setting the GigaVUE-FM password, refer to Setting the GigaVUE-FM Admin Password .	
{get show} interface	Displays the management interface configured for the GigaVUE-FMinstance.	
[{mgmt management}]	For example:	
	fmctl get show interface management	
set interface {mgmt management} <interface name=""></interface>	Configures the management interface for the GigaVUE-FM instance, which has more than one ethernet interface.	
	For example:	
	fmctl set interface management eth1	
	<b>Note:</b> You cannot use the <b>interface</b> syntax with the <b>set interface management</b> argument.	
interface <interface name=""></interface>	Allows various configurations that can be set for the management interface. This is an optional	
	argument.	
	For example, use the following command to ensure that eth1 management interface uses DHCP:	
	fmctlinterface eth1 set ip dhcp	
[options{help interface	Maps the FQDN with the IP address of GigaVUE-FM.	
<interface name="">}] set mapping <fqdn> <ip address=""></ip></fqdn></interface>	For example:	
	fmctlinterface eth1 set mapping fm 10.10.10.1	
	Use the following command to remove the mapping:	
	fmctlinterface eth1 set mapping fm	
[options{help interface <interface name="">}] {get show}</interface>	Use to either fetch or display the IP address, NTP configurations, host name, domain name, or FQDN .	
{ip ntp hostname domain fqdn}	For example:	
	fmctlinterface eth1 get {ip ntp hostname domain fqdn}	
	fmctlhelp show {ip ntp hostname domain fqdn}	

Argument	Description		
[options{help interface <interface name="">}] set [ip ip6]</interface>	Configures the management interface to use DHCP.		
	For example:		
ancp	fmctlinterface eth1 set ip dhcp		
[options{help interface <interface name="">}] set [ip ip6]</interface>	Configures the static IP address and gateway on the management interface. You can also choose to configure DNS.		
[static] <address cidr=""> [<gateway></gateway></address>	For example:		
[ <dns1>[,<dns2>[,]]]</dns2></dns1>	fmctlinterface eth1 set ip static 10.115.46.72/21 10.115.40.1 10.10.1.20		
[options{help interface <interface name="">}] set {ip ip6} route {add remove} address/cidr gateway</interface>	Adds or removes the IP address and gateway for the management interface.		
[options{help interface <interface name="">}] set ntp {disable <server1>[,<server2>[,]}</server2></server1></interface>	Use to disable NTP for synchronization of the system's clock or delete a NTP server.		
	For example, the following command disables NTP:		
	fmctlinterface eth1 set ntp disable		
	For example, the following command deletes NTP server:		
	fmctlinterface eth1 set ntp disable 1.2.3.4		
[options{help interface <interface name="">}] set ntp [enable]</interface>	You choose to enable NTP and add NTP servers. For example, the following command enables NTP and adds a NTP server:		
[version <version_number>]</version_number>	fmctlinterface eth1 set ntp enable 192.168.1.10		
<pre>[<server>[:<key_id>:<key_ type="">:<key_yalue>[ 1]]}</key_yalue></key_></key_id></server></pre>	For example, the following command enables NTP and adds a NTP server with Authentication:		
	fmctlinterface eth1 set ntp enable		
	192.168.1.10:50:SHA1:HEX:0EAB2E8193262AA0DA64C96A63E9221A20395313		
[options{help interface <interface name="">}] set ntp update</interface>	Use to update the Auth-details (keys) of the NTP server or to remove the Auth-details.		
[version <version_ number="">] <server>[:<key_ id="">:<key_< th=""><td>For example, the following command updates the Auth-details (keys) of a NTP server:</td></key_<></key_></server></version_>	For example, the following command updates the Auth-details (keys) of a NTP server:		

Argument	Description	
type>: <key_value>]</key_value>	fmctl –interface eth1 set ntp update 1.2.3.4:54:SHA1:HEX:0EAB2E8193262AA0DA64C96A63E9221A20395313	
	For example, the following command removes the Auth-details (keys) of a NTP server if configured already:	
	fmctlinterface eth1 set ntp update 1.2.3.4	
[options{help interface	Configures the hostname.	
<interface name="">}] set hostname <hostname></hostname></interface>	For example:	
	fmctlinterface eth1 set hostname myfm	
	<b>Note:</b> Ensure that you log out and re-login to the GigaVUE-FM to view the changes.	
[options{help interface <interface name="">}] set domain <domain></domain></interface>	Configures the domain for GigaVUE-FM.	
	For example:	
	fmctlinterface eth1 set domain gigamon.com	
[options{help interface	Configures the Fully Qualified Domain Name (FQDN) for the current GigaVUE-FM.	
<interface name="">}] set fqdn <hostname> <domain></domain></hostname></interface>	fmctlinterface eth1 set fqdn myfm gigamon.com	
[options{help interface	Displays a list of domains for the current GigaVUE-FM	
<interface name="">}] set/get/show</interface>	For example:	
searcnoomains [ <omaini> [.<domain2>[]]]</domain2></omaini>	fmctlinterface eth1 set searchdomains	
[,	fmctlhelp get   show searchdomains	

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

**NOTE:** The command **fmctl jump-start** is deprecated.

### Backing Up Configurations

Configurations that can backed up using **fmctl** commands are as follows:

- **BackupVersion**
- fmMgmtPort
- fmHostname
- fmDomain
- fmNtpEnabled
- fmNtpServers
- fmDevice
- fmIp4Connection
- fmDhcpEnabled
- fmlp4Address

fmlp4Gateway	
fmlp4DNS	
fmlp4Routes	
fmlp6Connection	
fmDhcp6Enabled	
fmlp6Address	
fmlp6Gateway	
fmlp6DNS	
fmlp6Routes	
fmNameServers	
fmSearchDomains	
fmExtraPortCount	

**Note:** When there are multiple interfaces in GigaVUE-FM, back up files provide the configurations of all the interfaces.

#### 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 Ul 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 6.11 Hardware and Software Guides

**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.

#### Hardware

how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE-FM devices; reference information and specifications for the respective GigaVUE-FM devices

GigaVUE-HC1 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-TA200 Hardware Installation Guide

GigaVUE-TA200E Hardware Installation Guide

**GigaVUE-TA400 Hardware Installation Guide** 

GigaVUE-TA400E 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 Appliances Guide** 

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

#### **GigaVUE Application Intelligence Solutions Guide**

#### **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 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 6.11 Hardware and Software Guides

Gigamon Containerized Broker Deployment Guide

#### GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions

GigaVUE Cloud Suite Deployment Guide - Azure 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 GigaVUE 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)

#### Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices

Sanitization guidelines for GigaVUE Fabric Management Guide and GigavUE-OS devices.

#### **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 and 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		

#### GigaVUE-FM Installation and Upgrade Guide

For Online Topics	Online doc link	(URL for where the issue is)
	Topic Heading	(if it's a long topic, please provide the heading of the section where the issue is)
For PDF Topics	Document Title	(shown on the cover page or in page header )
	Product Version	(shown on the cover page)
	Document Version	(shown on the cover page)
	Chapter Heading	(shown in footer)
	PDF page #	(shown in footer)
How can we improve?	Describe the issue	Describe the error or issue in the documentation.
		(If it helps, attach an image to show the issue.)
	How can we improve the content?	
	Be as specific as possible.	
	Any other comments?	
		1

### **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 Community 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, usecase, 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 VÜECommunity 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)

#### Μ

#### member node

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

#### Ν

#### no-decrypt list

no need to decrypt (formerly whitelist)

#### nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

#### primary source

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

R

Ρ

#### receiver

follower in a bidirectional clock relationship (formerly slave)

#### S

#### source

leader in a bidirectional clock relationship (formerly master)