



GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)

GigaVUE Cloud Suite

Product Version: 6.8

Document Version: 1.1

Last Updated: Friday, October 11, 2024

(See Change Notes for document updates.)

Copyright 2024 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.8.00	1.1	10/11/2024	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.8.00	1.0	09/10/2024	The original release of this document with 6.8.00 GA.

Contents

GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) ..	1
Change Notes	3
Contents	4
GigaVUE Cloud Suite Deployment Guide - VMware(ESXi) ..	7
Overview of GigaVUE Cloud Suite for VMware	8
Components for GigaVUE Cloud Suite for VMware	8
Cloud Overview Page	9
Overall Cloud Overview Page	9
Platform specific Cloud Overview Page	10
Top Menu	10
Viewing Charts	12
Viewing Monitoring Session Details of all Cloud Platforms	13
Viewing Monitoring Session Details of Individual Cloud Platforms	14
Architecture for GigaVUE Cloud Suite for VMware ESXi	15
Points to Note (VMware vCenter)	16
Volume-Based License	16
Base Bundles	17
Bundle Replacement Policy	17
Add-on Packages	17
How GigaVUE-FM Tracks Volume-Based License Usage	18
Manage Volume-based Licenses	18
Activate Volume-based Licenses	20
Default Trial Licenses	21
Delete Default Trial Licenses	22
Supported Hypervisors for VMware	22
Introduction to Supported Features for GigaVUE Cloud Suite for VMware ESXi	23
Rediscover	24
Analytics for Virtual Resources	24
Sharing the Same Host across Different Monitoring Domains	25
Cloud Health Monitoring	25
Selective Source Selection	25
Customer Orchestrated Source - Use Case	25

Prerequisites for Integrating V Series Nodes with VMware vCenter	26
Recommended Form Factor for VMware vCenter (Instance Types)	27
Network Firewall Requirements	27
Required VMware Virtual Center Privileges	28
Default Login Credentials	30
Install and Upgrade GigaVUE-FM	30
Deploy GigaVUE Cloud Suite for VMware (ESXi)	31
Upload GigaVUE V Series Node Image into GigaVUE-FM	31
Install Custom Certificate	32
Upload Custom Certificates using GigaVUE-FM	32
Upload Custom Certificate using Third Party Orchestration	33
Create Monitoring Domain for VMware ESXi	33
Configure GigaVUE V Series Nodes for VMware ESXi	37
Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi	44
Configure Monitoring Session	49
Create a Monitoring Session	49
Edit Monitoring Session	51
Interface Mapping	52
Create Ingress and Egress Tunnel (VMware vCenter)	52
Create Raw Endpoint (VMware vCenter)	61
Rules and Notes	62
Configure Raw Endpoint in Monitoring Session	62
Create a New Map	63
Example- Create a New Map using Inclusion and Exclusion Maps	69
Map Library	69
Deploy Monitoring Session	70
Visualize the Network Topology	71
View Monitoring Session Statistics	72
View Health Status on the Monitoring Session Page	74
Status	74
Node Health	75
Targets Source Health	75
Add Applications to Monitoring Session	75
Migrate Application Intelligence Session to Monitoring Session	76
Post Migration Notes for Application Intelligence	77
Monitor Cloud Health	79
Configuration Health Monitoring	79
Traffic Health Monitoring	80

Supported Resources and Metrics	81
Create Threshold Template	82
Apply Threshold Template	83
Edit Threshold Template	84
View Health Status	85
Configure VMware Settings	86
Analytics for Virtual Resources	87
Virtual Inventory Statistics and Cloud Applications Dashboard	88
Additional Sources of Information	93
Documentation	93
How to Download Software and Release Notes from My Gigamon	95
Documentation Feedback	96
Contact Technical Support	97
Contact Sales	97
Premium Support	98
The VUE Community	98
Glossary	99

GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)

GigaVUE Cloud Suite for VMware provides an intelligent filtering technology that allows virtual machine (VM) traffic flows of interest to be selected, forwarded, and delivered to the monitoring infrastructure centrally attached to the Gigamon Deep Observability Pipeline, thereby eliminating any traffic blind spots in the enterprise private clouds or service provider NFV deployments.

This guide describes how to install, deploy, and operate the GigaVUE V Series Nodes in VMware.

Refer to the following topics for more detailed information:

- [Overview of GigaVUE Cloud Suite for VMware](#)
- [Architecture for GigaVUE Cloud Suite for VMware ESXi](#)
- [Points to Note \(VMware vCenter\)](#)
- [Volume-Based License](#)
- [Supported Hypervisors for VMware](#)
- [Introduction to Supported Features for GigaVUE Cloud Suite for VMware ESXi](#)
- [Prerequisites for Integrating V Series Nodes with VMware vCenter](#)
- [Install and Upgrade GigaVUE-FM](#)
- [Deploy GigaVUE Cloud Suite for VMware \(ESXi\)](#)
- [Configure Monitoring Session](#)
- [Migrate Application Intelligence Session to Monitoring Session](#)
- [Monitor Cloud Health](#)
- [Configure VMware Settings](#)
- [Analytics for Virtual Resources](#)

Overview of GigaVUE Cloud Suite for VMware

GigaVUE Cloud Suite for VMware acquires, optimizes, and distributes selected traffic to your monitoring and security tools. GigaVUE Cloud Suite for VMware provides tight integration with orchestration tools to deliver intelligent network traffic visibility for workloads running in Virtual machine in VMware. GigaVUE-FM, part of the Cloud Suite, works with VMware vCenter to automatically deploy GigaVUE V Series Node to support a growing private cloud infrastructure. GigaVUE-FM leverages dynamic service chaining and workload relocation monitoring to ensure visibility and policy integrity.

GigaVUE Cloud Suite for VMware provides the following benefits:

Flexible Traffic Acquisition: Acquires traffic through port mirroring in VMware ESXi.

Automated Visibility Provisioning: Dynamically provisions and applies traffic policies as new tenants come on board or as groups scale.

Increased Tool Efficiency: Reduces load on tools by selectively filtering, de-duplicating, and load balancing traffic sent to security and performance monitoring tools.

Application Intelligence solution: You can use Application Intelligence to identify thousands of applications and utilize over 7,000 application metadata elements.

Components for GigaVUE Cloud Suite for VMware

GigaVUE Cloud Suite for VMware comprises multiple elements that enable traffic acquisition, aggregation, intelligence and distribution, along with centralized, single-pane-of-glass orchestration and management. The solution consists of these components:

Component	Description
GigaVUE-FM fabric manager (GigaVUE-FM)	<p>GigaVUE-FM is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud Suite for VMware.</p> <p>GigaVUE-FM generates an end-to-end topology view through a single-pane-of-glass GUI, which gives you insights into which cloud instances are or are not part of the deep observability pipeline. A single instance of GigaVUE-FM can manage hundreds of visibility nodes across on-premises and multi-cloud environments. GigaVUE-FM manages the configuration of the rest of the components in your cloud platform.</p>
GigaVUE® V Series Node	<p>A visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or back haul to on premise device or tools.</p>

Cloud Overview Page

The overview page is a central location to view and monitor all the monitoring sessions in a single place. You can use this overview page to spot issues which will help in troubleshooting, or perform basic actions like view, edit, clone, and delete. This page provides a quick overview of basic statistics, V Series Alarms, Connection Status and Volume Usage vs Allowance and a table to summarize the active monitoring sessions details. You can also edit the monitoring session from this page instead of navigating to the monitoring session page in each platform.

You can view cloud overview page in the following ways:

[Overall Cloud Overview Page](#)

[Platform specific Cloud Overview Page](#)

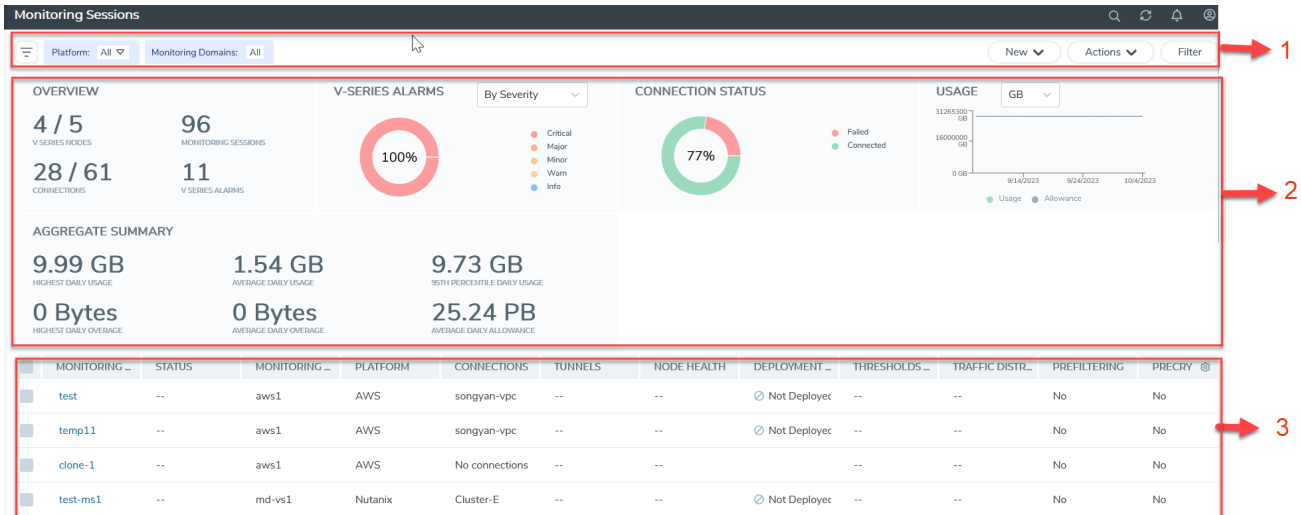
Overall Cloud Overview Page

To view the Overall Cloud Overview Page, Go to **Traffic > Virtual > Orchestrated Flows > Overview**

Platform specific Cloud Overview Page

To view Platform Specific Cloud Overview Page, Go to **Traffic > Virtual > Orchestrated Flows** > and select your cloud platform.

The **Monitoring Sessions** page appears as shown:



For easy understanding of the Monitoring Session page, the above figure is split into three major sections as described in the following table:

Number	Section	Description
1	Top Menu	Top Menu
2	Charts	Viewing Charts
3	Monitoring Session Details	<p>In Overall Cloud Overview Page, you can view the monitoring session details of all the cloud platforms.</p> <p>Refer to the section Viewing Monitoring Session Details of all Cloud Platforms</p> <p>In Platform specific Overview Page, you can view the monitoring session details of the individual cloud platforms.</p>

Top Menu

The Top menu consists of the following: options:

Options	Description
Filters	You can filter the monitoring session based on a criterion or combination of criteria such as based on the platform, monitoring session and V Series Node Id by applying filters. For more information, refer to Filters
New Drop-down list box	You create a new monitoring session and new monitoring domain. To create new monitoring session and monitoring domain refer to Create a Monitoring Session topic.
Action Drop-down list box	<p>You can do the following actions through the Action Drop down list box:</p> <ul style="list-style-type: none"> ▪ Edit - Opens the Edit page for the selected monitoring session. ▪ Delete - Deletes the selected monitoring session. ▪ Clone - Duplicates the selected monitoring session. ▪ Deploy - Deploys the selected monitoring session. ▪ Undeploy - Un-deploys the selected monitoring session. ▪ Apply Threshold - Applies the threshold template created for monitoring cloud traffic health. ▪ Apply Policy - Enables Precryption, Prefiltering, or Secure Tunnel. <p>For more information, refer to Cloud Monitoring Session topic.</p>

Filters

You can filter the monitoring session based on a criterion or combination of criteria such as based on the platform, monitoring session and V Series Node Id by applying filters.


You can apply the filters in two ways:

- [Filter on the left corner](#)
- [Filter on the right corner](#)

Filter on the left corner



You can view the monitoring sessions by filtering the monitoring domain based on the platform.

1. Select the required platform from the **Platform** drop- down list box.
2. Click  and select the monitoring domain.

The monitoring domain selected appears on the top menu bar.

Filter on the right corner

You can view the monitoring sessions by filtering the monitoring domain based on a criterion or by providing multiple criteria as follows:

- Monitoring Session
- Status
- Monitoring Domain
- Platform
- Connections
- Tunnel
- Deployment Status

Viewing Charts

You can view the following charts on the overview page:

- Overview
- V Series Alarms
- Connection Status
- Usage (VBL)
- Aggregate Summary

Overview

The overview dashboard displays the number of GigaVUE V Series Nodes active in GigaVUE-FM, the number of Monitoring sessions and connections configured in all the platforms, and the number of alarms triggered in V Series Nodes.

V Series Alarms

The V Series Alarms widget presents a pie chart that helps you to view the V Series alarms generated quickly. Each type of alarm triggered is assigned a color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of V Series alarms triggered.

Connection Status

The connection status presents a pie chart that helps you to quickly view the connection status of connections configured in the monitoring domain. The success and failed connection status is differentiated by the color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of connections.

Usage

The Usage widget displays the traffic that flows through the GigaVUE V Series Nodes. Each bar in the graph indicates the volume usage on a particular day. Hovering the mouse over a bar in the graph displays the volume allowance and volume usage on that day.

Aggregate Summary


The aggregate summary displays the highest daily volume usage, average daily volume usage, highest daily volume over usage, average daily volume over usage, 95th percentile daily volume usage and the average daily volume allowance.

Viewing Monitoring Session Details of all Cloud Platforms

You can view the following monitoring session details:

Details	Description
Monitoring Sessions	Name of the monitoring session. When you click the name of the session, you can view the following options: <ul style="list-style-type: none"> • View- When you click this option, you can view a split window displaying the details of the monitoring sessions such as Statistics, Connections, V Series Nodes, Source Health, Http2 Logging. For more information, refer to Viewing Monitoring Session Details of Individual Cloud Platforms • Edit - When you click this option, you can view the Edit Monitoring Session page.
Status	Health status of the monitoring session.
Monitoring Domain	Name of the Monitoring Domain to which the monitoring session is associated.
Platform	Cloud platform in which the session is created.
Connections	Connection details of the monitoring session.
Tunnels	Tunnel details related to the monitoring session
Node Health	Health of the node.
Deployment Status	Status of the deployment
Threshold Applied	Specifies whether the threshold is applied or not
Traffic Distribute	Specifies information about traffic distribution.
Prefiltering	Specifies whether Prefiltering is configured or not

Details	Description
Precryption	Specifies whether Precryption is configured or not.
SBI logging	Specifies whether SBI logging is configured or not.
Traffic Mirroring	Specifies whether Traffic Mirroring is configured or not.

NOTE: Click the settings icon  to select the columns that should appear in the monitoring session.

Viewing Monitoring Session Details of Individual Cloud Platforms

For a monitoring session, you can view the following details of the monitoring session:

Details	Description
Statistics	You can view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can view the statistics for all the V Series nodes or only for the Gigamon V Series node. You can also filter the statistics based on the elements associated with the monitoring session. For more information, refer to View Monitoring Session Statistics .
Connections	You can view the connection details of the monitoring session. You can view details such as the name of the connection, deployment status, number of targets, and targets source health.
V Series Nodes	You can view the V Series nodes associated with the monitoring session. You can also view details such as name of the V Series Node, Host VPC, MD connection, Version, and Management IP.
Source Health	You can view the health of the source connected to the monitoring session.
Http2 Logging	You can view the details of the 5G SBI logging details. For more information about 5G SBI, refer to 5G-Service Based Interface Application

To view the details, click the name of the monitoring session, and then click **View**. A split window appears displaying the details.

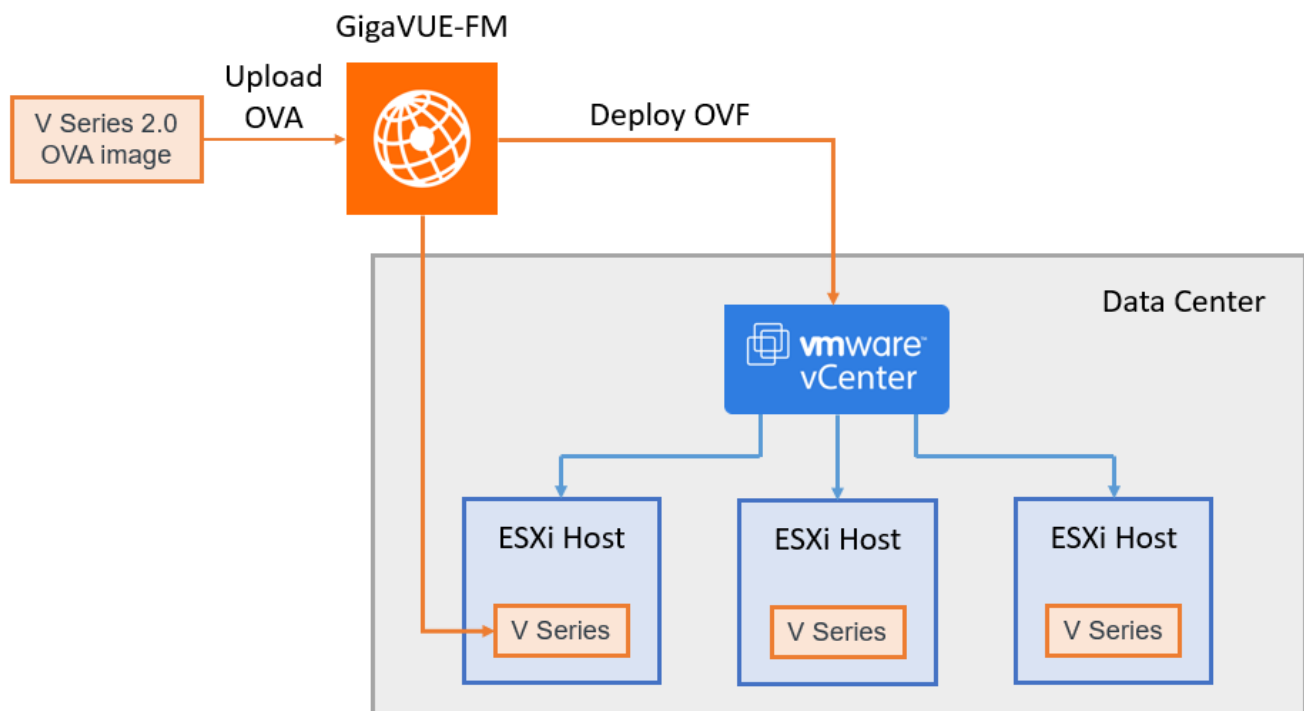
Architecture for GigaVUE Cloud Suite for VMware ESXi

This document provides an overview of the GigaVUE V Series Node deployment on the VMware ESXi platforms and describes the procedure for setting up the traffic monitoring sessions using the GigaVUE V Series Nodes. The GigaVUE V Series Nodes support traffic visibility on the following VMware networking elements:

- vSphere standard switch
- vSphere distributed switch

GigaVUE-FM creates, updates, and deletes the GigaVUE V Series Nodes in the ESXi hosts based on the configuration information provided by the user. The VMs and GigaVUE V Series Nodes are located in the same ESXi host and the traffic mirrored from VMs is sent to GigaVUE V Series Nodes. You can deploy only one GigaVUE V Series Node on a single ESXi host. GigaVUE-FM can communicate directly with the GigaVUE V Series Nodes.

The following diagram provides a high-level overview of the deployment:



Refer to the following Gigamon Validated designs for more information:

- [Deploying GigaVUE Cloud Suite on VMware vCenter in a multi-tier DC Environment](#)
- [Deploying GigaVUE Cloud Suite for VMware vCenter using V Series](#)

Points to Note (VMware vCenter)

1. These steps assume that VMware vCenter is installed and configured. Refer to [VMware Documentation](#) for configuration details.
2. Ensure the source Virtual Machine and the tool are connected to different Virtual Standard Switch. The traffic is looped, when the source Virtual Machine and the tool are connected in the same standard switch.
3. If NextGen Firewall (NGFW) with Deep Packet Inspection (DPI) is enabled to inspect your east-west traffic, expect an increase in latency due to mirrored traffic. To avoid increased latency, consider creating an exception rule for the tunneled traffic (mirrored traffic from the GigaVUE V Series Nodes to the tool) or configuring a private VDS that can bypass the NGFW rules for this traffic.
4. NSX Virtual Distributed Switch (N-VDS) based segments are not supported in **VMware vCenter** Monitoring Domain. N-VDS is supported only on NSX versions less or equal to 3.0. Refer to [VMware Documentation](#) for more detailed information.

Volume-Based License

All the GigaVUE V Series Nodes connected to GigaVUE-FM periodically report statistics on the amount of traffic that flows through the V Series Nodes. The statistics provide information on the actual data volume that flows through the V Series Nodes. All licensed applications, when running on the node, generate usage statistics.

Licensing for GigaVUE Cloud Suite is volume-based. In the Volume-Based Licensing (VBL) scheme, a license entitles specific applications on your V Series Nodes to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes becomes irrelevant for GigaVUE accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility on the actual amount of data, each licensed application is using on each node, and tracks the overuse, if any.

Volume-based licenses are available as monthly subscription licenses with a service period of one month. Service period is the period of time for which the total usage or overage is tracked. There is a grace period for each license that is encoded in the license file. The license effectively provides data allowance for this additional time after the official end time of the license.

For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales. Refer to [Contact Sales](#).

Base Bundles

In volume-based licensing scheme, licenses are offered as bundles. The following three base bundle types are available:

- CoreVUE
- NetVUE
- SecureVUEPlus

The bundles are available as SKUs¹. The number in the SKU indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE has a daily volume allowance of 250 terabytes for CoreVUE bundle.

Bundle Replacement Policy

Refer to the following notes:

- You can always upgrade to a higher bundle but you cannot move to a lower version.
- You cannot have two different base bundles at the same time however, you can have multiple base bundles of the same type.
- Once upgraded to a higher bundle, the existing lower bundles will be automatically deactivated.

Add-on Packages

GigaVUE-FM allows you to add additional packages called add-on packages to the base bundles. These add-on packages allow you to add additional applications to your base bundles. Add-on packages have their own start/end date and volume specifications.

Rules for add-on packages:

- Add-on packages can only to be added when there is an active base bundle available in GigaVUE-FM.
- The base bundle limits the total volume usage of the add-on package.
- If your add-on package has volume allowance less than the base bundle, then your add-on package can only handle volume allocated for add-on package.

¹Stock Keeping Unit. Refer to the [What is a License SKU?](#) section in the FAQs for Licenses chapter.

- When the life term of an add-on package extends beyond the base bundle, then when the base bundle expires, the volume allowance of the add-on package will be reduced to zero until a new base bundle is added.

For more information about SKUs refer to the respective Data Sheets as follows:

GigaVUE Data Sheets
GigaVUE Cloud Suite for VMware Data Sheet
GigaVUE Cloud Suite for AWS Data Sheet
GigaVUE Cloud Suite for Azure Data Sheet
GigaVUE Cloud Suite for OpenStack
GigaVUE Cloud Suite for Nutanix
GigaVUE Cloud Suite for Kubernetes

How GigaVUE-FM Tracks Volume-Based License Usage

GigaVUE-FM tracks the license usage for each V Series node as follows:

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only those applications that are licensed at that point (applicable only for ACTIVE licenses, licenses in grace period are not included).
- When a license goes into grace period, you will be notified with an audit log.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license will not be undeployed.


For releases prior to 6.4:

- The monitoring sessions using the corresponding license will be undeployed (but not deleted from the database).
- When a license is later renewed or newly imported, any undeployed monitoring sessions are redeployed.

NOTE: When the license expires, GigaVUE-FM displays a notification on the screen.

Manage Volume-based Licenses

To manage active Volume-based License:

1. On the left navigation pane, click .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.

This page lists the following information about the active Volume-based Licenses:

Field	Description
SKUs	Unique identifier associated with the license
Bundles	Bundle to which the license belongs to
Volume	Total daily allowance volume
Starts	License start date
Ends	License end date
Type	Type of license (Commercial, Trial, Lab and other license types).
Activation ID	Activation ID
Entitlement ID	Entitlement ID

NOTE: The License Type and Activation ID are displayed by default in the VBL Active page. To display the Entitlement ID field, click on the column setting configuration option to enable the Entitlement ID field.

The expired licenses are displayed in the **VBL Inactive** page, which can be found under the **FM/Cloud** drop-down in the top navigation bar. This page lists the following information about the inactive Volume-based Licenses:

Field	Description
SKUs	Unique identifier associated with the license.
Bundles	Bundle to which the license belongs to.
Ends	License end date
Grace Period	Number of days the license is in grace period
Deactivation Date	Date the license got deactivated.
Revocation Code	License revocation code.
Status	License status.

NOTE: The License Type, Activation ID and Entitlement ID fields are not displayed by default in the VBL Inactive page. To display these fields, click on the column setting configuration option and enable these fields.

Use the following buttons to manage your VBL.


Button	Description
Activate Licenses	Use this button to activate a Volume-based License. For more information, refer to the topic Activate Volume-based Licenses of the GigaVUE Licensing Guide.
Email Volume Usage	Use this button to send the volume usage details to the email recipients.
Filter	Use this button to narrow down the list of active Volume-based Licenses that are displayed on the VBL active page.
Export	Use this button to export the details in the VBL active page to a CSV or XLSX file.
Deactivate	Use this button to deactivate the licenses. You can only deactivate licenses that are in grace period or that have expired.

For more detailed information on dashboards and reports generation for Volume-based Licensing refer to the following table:

For details about:	Reference section	Guide
How to generate Volume-based License reports	Generate VBL Usage Reports	GigaVUE Administration Guide
Volume-based Licensed report details	Volume Based License Usage Report	GigaVUE Administration Guide
Fabric health analytics dashboards for Volume-based Licenses usage	Dashboards for Volume Based Licenses Usage	GigaVUE-FM User Guide

Activate Volume-based Licenses

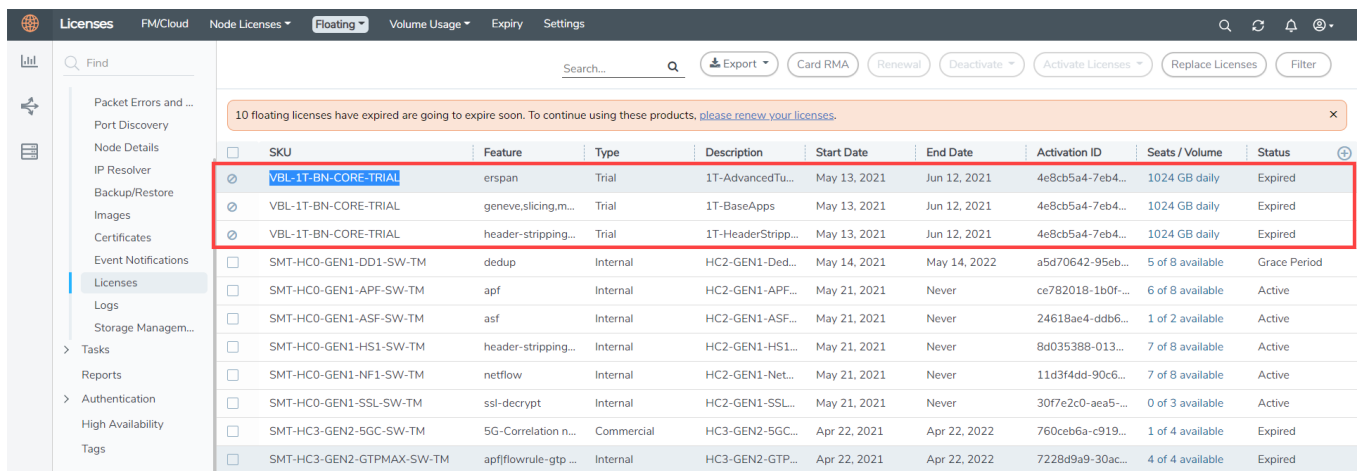
To activate Volume-based licenses:

1. On the left navigation pane, click .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.

3. Click **Activate Licenses**. The **Activate License** page appears. Perform the following steps:
 - a. Download the fabric inventory file that contains information about GigaVUE-FM. Click **Next**. Refer to the [What is a Fabric Inventory File?](#) section for more details.
 - b. Navigate to the Licensing Portal. Upload the Fabric Inventory file in the portal. Once the fabric inventory file is uploaded, select the required license and click **Activate**. A license key is provided. Record the license key or keys.
 - c. Return to GigaVUE-FM and add the additional licenses.

Default Trial Licenses

After you install GigaVUE-FM, a default free 1TB of CoreVUE trial volume-based license (VBL) is provided one-time for 30 days (from the date of installation).



SKU	Feature	Type	Description	Start Date	End Date	Activation ID	Seats / Volume	Status
VBL-1T-BN-CORE-TRIAL	erspan	Trial	1T-AdvancedTu...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	geneve,slicing,m...	Trial	1T-BaseApps	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	header-stripping...	Trial	1T-HeaderStripp...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
SMT-HC0-GEN1-DD1-SW-TM	dedup	Internal	HC2-GEN1-Ded...	May 14, 2021	May 14, 2022	a5d70642-95eb...	5 of 8 available	Grace Period
SMT-HC0-GEN1-APF-SW-TM	apf	Internal	HC2-GEN1-APF...	May 21, 2021	Never	ce782018-1b0f...	6 of 8 available	Active
SMT-HC0-GEN1-ASF-SW-TM	asf	Internal	HC2-GEN1-ASF...	May 21, 2021	Never	24618ae4-ddb6...	1 of 2 available	Active
SMT-HC0-GEN1-HS1-SW-TM	header-stripping...	Internal	HC2-GEN1-HS1...	May 21, 2021	Never	8d035388-013...	7 of 8 available	Active
SMT-HC0-GEN1-NF1-SW-TM	netflow	Internal	HC2-GEN1-Net...	May 21, 2021	Never	11d3f4dd-90c6...	7 of 8 available	Active
SMT-HC0-GEN1-SSL-SW-TM	ssl-decrypt	Internal	HC2-GEN1-SSL...	May 21, 2021	Never	30f7e2c0-aea5...	0 of 3 available	Active
SMT-HC3-GEN2-5GC-SW-TM	5G-Correlation n...	Commercial	HC3-GEN2-5GC...	Apr 22, 2021	Apr 22, 2022	760ceb6a-c919...	1 of 4 available	Expired
SMT-HC3-GEN2-GTPMAX-SW-TM	apfflowrule-gtp...	Internal	HC3-GEN2-GTP...	Apr 22, 2021	Apr 22, 2022	7228d9a9-30ac...	4 of 4 available	Expired

This license includes the following applications:


- ERSPAN
- Geneve
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flowmap
- Header-stripping
- Add header

NOTE: There is no grace period for the trial license. If you do not have any other Volume-based licenses installed, then after 30 days, on expiry of the trial license, any deployed monitoring sessions will be undeployed from the existing GigaVUE V Series Nodes.

To deactivate the trial VBL refer to [Delete Default Trial Licenses](#) section for details.

Delete Default Trial Licenses

GigaVUE-FM allows you to deactivate the default trial licenses from this page. To deactivate the license:

1. On the left navigation pane, click .
2. Go to **System > Licenses > Floating**. Click **Activated**.
3. Click **Deactivate > Default Trial VBL**.

The VBL trial licenses is deactivated and is no longer listed in the Activated page. However, you can view these deactivated licenses from the Deactivated page.

Supported Hypervisors for VMware

The following table lists the supported hypervisor versions for vCenter, VMware ESXi and VMware NSX-T.

GigaVUE V Series Node Supported Hypervisors	Tested Platforms			
		vCenter Server	ESXi	GigaVUE-FM
vSphere ESXi	v6.7	v6.7U3	v6.7U3	v5.10.02, v5.11.01, v5.12.00, v5.13.00, v5.13.01
	v7.0	v7.0	v7.0	v5.10.02, v5.11.01, v5.12.00, v5.13.00, v5.13.01, v5.14.00, v5.15.00, v5.16.00, v6.0.00, v6.1.00
	v7.0	v7.0U3	v7.0U3	v5.15.00, v5.16.00, v6.0.00, v6.1.00, v6.2.00, v6.3.00, v6.4.00, v6.5.00, v6.6.00, v6.7.00, v6.8.00
	v8.0	v8.0	v8.0	v6.3.00, v6.4.00, v6.5.00, v6.6.00, v6.7.00, v6.8.00

GigaVUE V Series Node Supported Hypervisors	Tested Platforms			
		vCenter Server	ESXi	GigaVUE-FM
	v8.0	v8.0U2, v8.0U3	v8.0U2, v8.0U3	v6.8.00
vSphere NSX-T	v3.1.0	v7.0	v7.0	v5.11.01, v5.12.00
	v3.1.2	v7.0	v6.7U3, v7.0U1	v5.12.00, v5.13.00, v5.13.01
	v3.1.3	v7.0	v6.7U3, v7.0U1	v5.13.01, v5.14.00, v6.0.00
	v3.2.0	v7.0, v7.0U3	v6.7U3, v7.0U1, v7.0U3	v5.14.01, v5.15.00, v5.16.00, v6.0.00
	v3.2.1	v7.0U3	v6.7U3, v7.0U1, v7.0U3	v6.0.00, v6.1.00, v6.2.00
	v3.2.2	v7.0U3	v7.0U3	v6.3.00, v6.4.00
	v3.2.3	v7.0U3	v7.0U3	v6.5.00, v6.6.00, v6.7.00, v6.8.00
	v4.0.0	v7.0U3	v7.0U3	v6.0.00, v6.1.00, v6.2.00, v6.3.00
	v4.1.0	v7.0U3	v7.0U3	v6.3.00, v6.4.00, v6.5.00
	v4.1.0	v8.0U2	v8.0U2	v6.5.00, v6.6.00, v6.7.00
	v4.1.2	v8.0U2, v8.0U3	v8.0U2, v8.0U3	v6.8.00

Introduction to Supported Features for GigaVUE Cloud Suite for VMware ESXi

GigaVUE Cloud Suite for VMware (ESXi) supports the following features:

- [Rediscover](#)
- [Analytics for Virtual Resources](#)
- [Sharing the Same Host across Different Monitoring Domains](#)
- [Cloud Health Monitoring](#)
- [Selective Source Selection](#)

Rediscover

When modifying the configurations of the GigaVUE V Series Node deployed in VMware vCenter, it may lead to configuration mismatch between the GigaVUE V Series Node and the virtual machine configuration present in GigaVUE-FM. You can use the Rediscover button in GigaVUE-FM to overcome this. The following GigaVUE V Series Node configuration can be rediscovered from GigaVUE-FM:

- GigaVUE V Series Node name
- Datastore
- Management IP address
- Tunnel IP address
- Network name for Management Interface
- Network name for Tunnel Interface

NOTE: GigaVUE-FM performs an auto-rediscovery every 24 hours. Every 24 hours GigaVUE-FM checks for the above-mentioned things and updates the GigaVUE V Series Node configuration.

You can select an individual or multiple GigaVUE V Series Node in the Monitoring Domain page and follow the instructions given below:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the **Monitoring Domain** page, click **Actions > Rediscover**.

NOTE: You can only rediscover GigaVUE V Series Nodes that are in **OK** state.

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects.

Refer to [Analytics for Virtual Resources](#) for more detailed information.

Sharing the Same Host across Different Monitoring Domains

GigaVUE-FM has the ability to share a host between VMware ESXi and VMware NSX-T monitoring domain. You can deploy multiple V Series nodes from VMware NSX-T monitoring domain and one V Series Node from VMware ESXi monitoring domain on the same host. This way the workload virtual machines connected to NSX segments can be monitored using the V Series nodes deployed in NSX-T monitoring domain and workload virtual machines connected to regular VSS / VDS networks can be monitored using the V Series node deployed in the ESXi monitoring domain.

NOTE: If a Virtual Machine has NICs attached to both VMware NSX-T segments and ESXi VDS or VSS port groups then GigaVUE-FM cannot provide visibility to those virtual machines in ESXi platform.

Cloud Health Monitoring

GigaVUE-FM allows you to monitor the traffic and configuration health status of the monitoring session and its individual components. This section provides detailed information on how to view the traffic and configuration health status of the monitoring session and its individual components.

For more information on how to configure cloud health monitoring, refer to the topic [Monitor Cloud Health](#).

Selective Source Selection

Using this feature, you can select an individual Network adapter of a virtual machine as a target when creating maps. Refer to [Create a New Map](#) topic for more detailed information.

Customer Orchestrated Source - Use Case

Customer Orchestrated Source is a traffic acquisition method that allows to tunnel traffic directly to the GigaVUE V Series Nodes. In cases where UCT-V or VPC Mirroring cannot be configured due to firewall or other restrictions, you can use this method and tunnel the traffic to GigaVUE V Series Node, where the traffic is processed.

When using Customer Orchestrated Source, you can directly configure tunnels or raw endpoints in the monitoring session, where you can use other applications like Slicing, Masking, Application Metadata, Application Filtering, etc., to process the tunneled traffic.

Refer to [Create Ingress and Egress Tunnel \(VMware vCenter\)](#) and [Create Raw Endpoint](#) for more detailed information on how to configure Tunnels and Raw End Points in the Monitoring Session.

You can configure an Ingress tunnel in the Monitoring Session with the GigaVUE V Series Node IP address as the destination IP address, then the traffic is directly tunneled to that GigaVUE V Series Node.

Prerequisites for Integrating V Series Nodes with VMware vCenter

- Refer to [Supported Hypervisors for VMware](#) for supported VMware vCenter, VMware ESXi and VMware NSX-T versions.
- ESXi hosts must have the minimum vCPU and memory resources for hosting the GigaVUE V Series Nodes. Refer to [Recommended Form Factor for VMware vCenter \(Instance Types\)](#) for more information.
- To support internationalized characters in the VMware vCenter environment, ensure that the vCenter character encoding is set to UTF-8.
- GigaVUE V Series Node device OVA image file. The GigaVUE V Series Node OVA image files can be downloaded from [Gigamon Customer Portal](#).
- All the target VMs must have VMware guest tools or Open VM tools if you use IP based filtering.
- Port 8889 must be available for GigaVUE-FM to access GigaVUE V Series Nodes.
- TCP Port 443 must be open between the GigaVUE-FM instance and the ESXi host to upload the OVA files. Refer to [Network Firewall Requirements](#) for more detailed information on ports that must be opened for configuring GigaVUE Cloud Suite for VMware vCenter.

Refer to the following topics for more detailed information:

- [Recommended Form Factor for VMware vCenter \(Instance Types\)](#)
- [Network Firewall Requirements](#)
- [Required VMware Virtual Center Privileges](#)
- [Default Login Credentials](#)

Recommended Form Factor for VMware vCenter (Instance Types)

The form factor (instance) size of the GigaVUE V Series Node is configured on the OVF file and packaged as part of the OVA image file. The following table lists the available form factors (instance types) and sizes based on memory and the number of vCPUs for a single GigaVUE V Series Node. Instance sizes can be different for GigaVUE V Series Nodes in different ESXi hosts and the default size is Small.

Type	Memory	vCPU	Disk space	vNIC
Small	4GB	2vCPU	8GB	1 Management interface, 1 Tunnel interface, and 8 vTAP interfaces
Medium	8GB	4 vCPU		
Large	16GB	8 vCPU		

NOTE: For any queries on which form factor to use, reach out to your account manager or contact Gigamon Technical Support

Network Firewall Requirements

Following are the Network Firewall Requirements for GigaVUE V Series Node deployment.

Source	Destination	Source Port	Destination Port	Protocol	Service	Purpose
GigaVUE-FM	ESXi hosts	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter and all ESXi hosts to import the V Series OVA files. OVA files require access to the host IP/URL for bulk deployment
	vCenter					
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE-FM to receive

						the traffic health updates with GigaVUE V Series Node
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	
Administrator	GigaVUE V Series Nodes	Not Applicable	22		ssh	Troubleshooting GigaVUE V Series Nodes.
Remote Source	GigaVUE V Series Nodes	Custom Port (VXLAN and UDPGRE),N/A for GRE	4789	UDP	VXLAN	Allows to UDPGRE Tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
GigaVUE V Series Nodes	Tool/ GigaVUE HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows GigaVUE V Series Node to communicate and tunnel traffic to the Tool
			Not Applicable	IP 47	GRE	
GigaVUE V Series Nodes	Tool/ GigaVUE HC Series instance	Not Applicable	Not Applicable	ICMP	Echo Request	Allows GigaVUE V Series Node to health check tunnel destination traffic (Optional)
					Echo Response	
GigaVUE V Series Nodes	GigaVUE-FM	Any (1024-65535)	Any (1024-65535)	TCP	Custom TCP	Allows GigaVUE V Series Nodes to communicate the traffic health updates with GigaVUE-FM

Required VMware Virtual Center Privileges

This section lists the minimum privileges required for the GigaVUE-FM user in Virtual Center. You assign privileges to Virtual Center users by selecting **Administration** from the left navigation pane. Then select **Roles** under the **Access Control**. Roles should be applied at the vSphere Virtual Center level and not the Data Center or Host levels.

The following table lists the minimum required permissions for GigaVUE-FM to manage the virtual center user with roles specified above.

Category	Required Privilege	Purpose
Datastore	Allocate space	V Series Node Deployment
Distributed Switch	VSPAN Operation	VDS Tapping
Folder	Create Folder	V Series Node Deployment
Host	Configuration <ul style="list-style-type: none"> Network Configuration 	VSS Tapping
	Inventory <ul style="list-style-type: none"> Modify Cluster 	Pin V Series Node to the host in cluster configurations. This prevents automatic migration.
Network	<ul style="list-style-type: none"> Assign network Configure 	<ul style="list-style-type: none"> V Series Node Deployment/VSS Tapping V Series Node Deployment
Resource	Assign virtual machine to resource pool	V Series Node Deployment
vApp	<ul style="list-style-type: none"> Import vApp instance configuration vApp application configuration 	V Series Node Deployment
Virtual machine	Configuration <ul style="list-style-type: none"> Add new disk Add or remove device Modify device settings Rename 	V Series Node Deployment V Series Node Deployment/VSS Tapping

Category	Required Privilege	Purpose
	Interaction <ul style="list-style-type: none"> • Connect devices • Power on • Power Off • Reset 	V Series Node Deployment
	Inventory <ul style="list-style-type: none"> ▪ Create from existing ▪ Remove 	V Series Node Deployment
	Provisioning <ul style="list-style-type: none"> ▪ Clone virtual machine 	V Series Node Deployment

Default Login Credentials

You can login to the GigaVUE V Series Node by using the default credentials.

Product	Login credentials
GigaVUE V Series Node	<p>You can login to the GigaVUE V Series Node by using ssh. The default username and password is:</p> <p>Username: gigamon</p> <p>Password: Enter the password provided during the fabric launch configuration. Refer Configure GigaVUE V Series Nodes for VMware ESXi for more detailed information on fabric launch configuration.</p>

Install and Upgrade GigaVUE-FM

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.

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

- Installation: Refer to GigaVUE-FM Installation and Upgrade Guide available in the [Gigamon Documentation Library](#).
- Upgrade: Refer to Upgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

Deploy GigaVUE Cloud Suite for VMware (ESXi)

To integrate GigaVUE V Series Nodes with VMware vCenter, perform the following steps:

- [Upload GigaVUE V Series Node Image into GigaVUE-FM](#)
- [Create Monitoring Domain for VMware ESXi](#)
- [Configure GigaVUE V Series Nodes for VMware ESXi](#)
- [Rediscover](#)

The below table provides step-by-step instructions on configuring GigaVUE Cloud Suite for VMware for providing visibility to physical and virtual traffic. Refer to the VMware ESXi System Requirements and [Prerequisites for Integrating V Series Nodes with VMware vCenter](#) sections for prerequisites that are required to be configured.

Step No	Task	Refer the following topics
1	Upload the GigaVUE V Series Node Image (OVA File) into GigaVUE-FM	Upload GigaVUE V Series Node Image into GigaVUE-FM
2	Create a Monitoring Domain	Create Monitoring Domain for VMware ESXi
3	Deploy GigaVUE V Series Nodes using GigaVUE-FM	Configure GigaVUE V Series Nodes for VMware ESXi Refer to <i>Deploy GigaVUE V Series Nodes using GigaVUE-FM</i> section.
4	Create Monitoring session	Create a Monitoring Session
5	Create a Ingress and Egress Tunnels to tunnel traffic	Create Ingress and Egress Tunnel (VMware vCenter)
6	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Upload GigaVUE V Series Node Image into GigaVUE-FM

This step is optional, you can also upload the GigaVUE V Series Node Image into GigaVUE-FM, when deploying the GigaVUE V Series Node. Refer to [Configure GigaVUE V Series Nodes for VMware ESXi](#).

To upload the V Series image into GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and then click **Settings > OVA Files**. The OVA Files page appears.
2. In the OVA Files page, click **Browse** to select the *gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova* file.
3. Click **Upload to Server** to upload the selected OVA image file to GigaVUE-FM server.

NOTE: The maximum number of OVA files that can be uploaded to GigaVUE-FM for VMware vCenter is three.

Install Custom Certificate

GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controllers have default self-signed certificates installed. The communication between GigaVUE-FM and the fabric components happens in a secure way using these default self-signed certificates, however you can also add custom certificates like SSL/TLS certificate to avoid the trust issues that occurs when the GigaVUE V Series Nodes, GigaVUE V Series Proxy, or UCT-V Controllers run through the security scanners.

You can upload the custom certificate in two ways:

- [Upload Custom Certificates using GigaVUE-FM](#)
- [Upload Custom Certificate using Third Party Orchestration](#)

Upload Custom Certificates using GigaVUE-FM

To upload the custom certificate using GigaVUE-FM follow the steps given below:

1. Go to **Inventory > Security > Custom SSL Certificate**. The **Custom Certificate Configuration** page appears.
2. On the Custom Certificate Configuration page, click **Add**. The **New Custom Certificate** page appears.
3. Enter or select the appropriate information as shown in the following table.

Field	Action
Certificate Name	Enter the custom certificate name.
Certificate	Click on the Upload Button to upload the certificate.
Private Key	Click on the Upload Button to upload the private key associated with the certificate.

4. Click **Save**.

You must also add root or the leaf CA certificate in the Trust Store. For more detailed information on how to add root CA Certificate, refer to Trust Store topic in *GigaVUE Administration Guide*.

The certificates uploaded here can be linked to the respective GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller in the Fabric Launch Configuration Page. Refer to *Configure GigaVUE Fabric Components in GigaVUE-FM* topic in the respective cloud guides for more detailed information.

NOTE: The minimum value for the authentication key encryption length provided during the key generation is 2048.

Upload Custom Certificate using Third Party Orchestration

You can also upload custom certificates to GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform at the time of deploying the fabric components. Refer to the following topics on more detailed information on how to upload custom certificates using third party orchestration in the respective platforms:

For integrated mode:

- [Configure GigaVUE Fabric Components in AWS](#)
- [Configure GigaVUE Fabric Components in Azure](#)
- [Configure GigaVUE Fabric Components in OpenStack](#)

For generic mode:

- [Configure GigaVUE Fabric Components in AWS](#)
- [Configure GigaVUE Fabric Components in Azure](#)
- [Configure GigaVUE Fabric Components in GCP](#)
- [Configure GigaVUE Fabric Components in Nutanix](#)
- [Configure GigaVUE Fabric Components in OpenStack](#)
- [Configure GigaVUE V Series Nodes using VMware ESXi](#)

Create Monitoring Domain for VMware ESXi

This chapter describes how to create a monitoring domain for deploying GigaVUE V Series Nodes in VMware vCenter environment through GigaVUE-FM. You must establish a connection between GigaVUE-FM and VMware vCenter. Creating a monitoring domain in GigaVUE-FM allows you to establish a connection between vCenter and GigaVUE-FM.

To create a monitoring domain in GigaVUE-FM for VMware vCenter:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the **Monitoring Domain** page, click **New**. The **VMware Configuration** page appears.

The screenshot shows the 'VMware Configuration' page for creating a Monitoring Domain. The page has a dark header with 'VMware vCenter', 'Monitoring Domain', and 'Settings' tabs. Below the header is a 'VMware Configuration' section with a 'Save' and 'Cancel' button. The configuration fields are:

- Monitoring Domain* (text input)
- Connection Alias* (text input)
- Virtual Center* (text input)
- Username* (text input)
- Password* (password input with eye icon)
- Traffic Acquisition Method (dropdown menu, currently 'Platform Tapping')
- Resource Allocation ⓘ (dropdown menu, currently 'Target VM Based')
- Maximum number of V Series nodes per Host (text input, value '10')

A help tooltip is displayed on the right side of the page, containing the following information:

- Target VM Based (Default) - Preferable for environments when there are workload VMs attached to less than or equal to 8 virtual switches on the same ESXI Host.
- Switch Based - Preferable for environments when there are workload VMs attached to more than 8 virtual switches on the same ESXI Host.

At the bottom left of the page, the text 'FM Instance:GigaVUE-FM - 6.7.00' is visible.

3. In the **VMware Configuration** page, enter or select the following details:

Field	Description
Monitoring Domain	Name of the monitoring domain
Connection Alias	Name of the connection
Virtual Center	IP address or FQDN of the vCenter
Username	Username of the vCenter user with minimum privileges as described in Prerequisites for Integrating V Series Nodes with VMware vCenter section.
Password	vCenter password used to connect to the vCenter

Field	Description
Traffic Acquisition Method	<p>Select a Traffic Acquisition Method.</p> <p>Platform Tapping: Platform tapping can be done in two ways.</p> <ul style="list-style-type: none"> • VSS: Platform Tapping can be used when a workload Virtual Machine is connected to a Virtual Standard Switch network. Promiscuous network will be created on VSS switch by GigaVUE-FM for tapping the traffic. • VDS: Platform Tapping can be used when a workload Virtual Machine is connected to a Virtual Distributed Switch portgroup. Port Mirroring will be created on the VDS switch by GigaVUE-FM for tapping the traffic <p>Customer Orchestrated Source: If you select Customer Orchestrated Source as the tapping method, you can use a tunnel or raw endpoint as a source where the traffic is directly tunneled to GigaVUE V Series Nodes.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: If you wish to deploy AMX application in the Monitoring Session for this Monitoring Domain, select the Traffic Acquisition Method as Customer Orchestrated Source.</p> </div>
<p>Resource Allocation</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: This field is applicable only when using Platform Tapping as the Traffic Acquisition Method.</p> </div>	<p>When deploying multiple GigaVUE V Series Node in a single host, select any one of the following options:</p> <p>Target VM Based: Choose this option if your deployment workload VMs attached to less than or equal to 8 vSwitches on the same ESXi host. This type of resource allocation will distribute the workload VMs across the multiple GigaVUE V Series Node deployed on the same ESXi host.</p> <p>Switch Based: A single GigaVUE V Series Node can tap a maximum of 8 vSwitches. Choose this option if you have traffic monitoring VMs running on ESXi hosts that are connected to more than 8 vSwitches in a single host. The vSwitches are mapped to the GigaVUE V Series Node in a round-robin manner. In this model vSwitches are evenly distributed across the available GigaVUE V Series Nodes on the same host.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: Ensure to undeploy all the Monitoring Session associated with the connection before changing the Resource Allocation type.</p> </div>
Maximum Number of V Series Nodes per Host	Enter the maximum number of GigaVUE V Series Nodes that can be deployed in a single host. The default value is 10.

4. Click **Save**. The **VMware Fabric Launch Configuration** page appears. Refer to [Configure GigaVUE V Series Nodes for VMware ESXi](#) for more detailed information on how to deploy GigaVUE V Series Nodes in the **VMware Fabric Launch Configuration** page.

The Monitoring Domain created in this section will be listed in the **Monitoring Domain** page.

You can use the following buttons in this page to perform the following actions in the Monitoring domain page:

Buttons	Description
Edit	Use to edit a monitoring domain.
Deploy Fabric	Use to deploy GigaVUE V Series Nodes.
Upgrade Fabric	Use to upgrade GigaVUE V Series Nodes. Refer to Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi for more detailed information on how to upgrade.
Delete Monitoring Domain	Use to delete a Monitoring Domain.
Delete Fabric Nodes	Use to delete a GigaVUE V Series Node.
Connect / Disconnect	<p>Disconnect- When the Monitoring Domain is in Connected state, this option appears. Use this option to stop the communication between GigaVUE-FM and the VMware vCenter.</p> <p>Connect- When the Monitoring Domain is in disconnected state, this option appears. Use this option to start the communication between GigaVUE-FM and the VMware vCenter.</p>
Rediscover	The changes made in vCenter for the GigaVUE V Series Node will be reflected in GigaVUE-FM. Refer to Rediscover topic for more detailed information.
Power On	You can select an individual GigaVUE V Series Node and power it on. The status of the GigaVUE V Series Node is changed to Ok .
Power Off	You can select an individual GigaVUE V Series Node and power it off. If the GigaVUE V Series Node is turned off from GigaVUE-FM, then it will not be considered as part of Cloud Health Monitoring and GigaVUE-FM will not try to turn it on. The status of the GigaVUE V Series Node is changed to Down .
Reboot	You can select an individual GigaVUE V Series Node and reboot it.

Configure GigaVUE V Series Nodes for VMware ESXi

This section provides step-by-step information on how to deploy GigaVUE V Series Nodes in VMware vCenter Monitoring Domain.

To deploy GigaVUE V Series Nodes using GigaVUE-FM, follow the steps given below:

1. After creating a monitoring domain, you are navigated to the **VMware Fabric Launch Configuration** page.

2. You can also open **VMware Fabric Launch Configuration** page from the **Monitoring Domain** page. To launch the **VMware Fabric Launch Configuration** from the Monitoring Domain, go to **Inventory > VIRTUAL > VMware vCenter (V Series)**. Click **Actions > Deploy Fabric**. The **VMware Fabric Launch Configuration** page appears.

VMware Fabric Launch Configuration

Datacenter*

Cluster*

V Series Node Image*

Form Factor*

Enable Custom Certificates

Host* Import Host Info from File Add Host Info Manually

Common Configuration

Datastores Datastore Clusters

Datastore

V Series Node Name Prefix

V Series Node Name Suffix

Name Server

SSL Key

No. of V Series Nodes Per Host

Management

Network*

IP Type

MTU

Tunnel

Network*

IP Type

Gateway IP

MTU

Use IPv6

Virtual Disk Format


Deployment Folder

User Password* (gigamon)

Confirm User Password*

3. On the **VMware Fabric Launch Configuration** page, enter or select the following details:

Field	Description
Datacenter	vCenter Data Center with the ESXi hosts to be provisioned with GigaVUE V Series Nodes.
Cluster	Cluster where you want to deploy the GigaVUE V Series Nodes.
V Series Node Image	<p>Select the OVA file uploaded in the Upload GigaVUE V Series Node Image into GigaVUE-FM, from the drop-down menu.</p> <p>You can also add OVA files when launching the fabric. To add OVA files:</p> <ol style="list-style-type: none"> Click on the Add button. The Upload Image dialog box opens. In the Upload Image dialog box, click Browse to select the <i>gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova</i> file. Click Upload to Server to upload the selected OVA image file to GigaVUE-FM server.
Form Factor	<p>Instance size of the GigaVUE V Series Node. Refer Prerequisites for Integrating V Series Nodes with VMware vCenter for more information.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <ul style="list-style-type: none"> Small Form Factor is not supported when using applications like Application Visualization, Application Metadata, Application Filtering. Select 80GB Disk Space, when using AMX Application. </div>
Enable Custom Certificates	<p>Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and a handshake error occurs.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: If the certificate expires after the successful deployment of the fabric components, then the fabric components move to failed state.</p> </div>
<p>Certificate</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: This field appears only when Enable Custom Certificates field is enabled.</p> </div>	<p>Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes. For more detailed information, refer to Install Custom Certificate.</p>
Hosts	<p>Select the ESXi hosts for GigaVUE V Series Node deployment. Select Import Host Info from file or Add Host Info Manually.</p> <p>Import Host Info from file:</p> <p>To import host details from a .csv file:</p> <ol style="list-style-type: none"> Download the .csv template file. Enter the required values in the Excel sheet and save the file. Click Browse and select the .csv file saved in the previous step.

Field	Description																										
	<div data-bbox="548 226 1471 447" style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">  <ul style="list-style-type: none"> To deploy more than one GigaVUE V Series Node on the same host, add more rows in the Excel sheet with the same host value for each extra GigaVUE V Series Node you want to deploy. If your GigaVUE-FM version is above 6.5 and GigaVUE V Series Nodes are on a version below 6.5, Name Server and MTU is not supported. Therefore, these fields in the .csv file must be empty. </div> <p>Add Host Info Manually:</p> <p>Select the ESXi hosts for GigaVUE V Series Node deployment.</p> <p>The Common Configuration drop-down wizard appears. Expand the Common Configuration drop-down wizard and update the following details to apply the configuration to all the selected hosts.</p> <p>You can expand the individual hosts and add or delete GigaVUE V Series Node. You can expand the individual GigaVUE V Series Node and modify the configurations that were applied in the Common Configuration.</p> <table border="1" data-bbox="526 743 1479 1770"> <thead> <tr> <th colspan="2" data-bbox="526 743 1479 785">Common Configuration</th> </tr> </thead> <tbody> <tr> <td data-bbox="526 785 854 827">Datastore</td> <td data-bbox="854 785 1479 827">Network datastore shared among all ESXi hosts.</td> </tr> <tr> <td data-bbox="526 827 854 905">V Series Node Name Prefix</td> <td data-bbox="854 827 1479 905">Enter a prefix for the GigaVUE V Series Node name.</td> </tr> <tr> <td data-bbox="526 905 854 982">V Series Node Name Suffix</td> <td data-bbox="854 905 1479 982">Enter a suffix for the GigaVUE V Series Node name.</td> </tr> <tr> <td data-bbox="526 982 854 1150">Name Server</td> <td data-bbox="854 982 1479 1150">The 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 addresses, separated by comma.</td> </tr> <tr> <td data-bbox="526 1150 854 1228">No. of V Series Nodes per Host</td> <td data-bbox="854 1150 1479 1228">Enter the number of GigaVUE V Series Nodes to be deployed in each host.</td> </tr> <tr> <th colspan="2" data-bbox="526 1228 1479 1270">Management</th> </tr> <tr> <td data-bbox="526 1270 854 1348">Network</td> <td data-bbox="854 1270 1479 1348">Management network for GigaVUE V Series Nodes.</td> </tr> <tr> <td data-bbox="526 1348 854 1425">IP Type</td> <td data-bbox="854 1348 1479 1425">Select the management network IP type as Static or DHCP.</td> </tr> <tr> <td data-bbox="526 1425 854 1640">Gateway IP</td> <td data-bbox="854 1425 1479 1640">Gateway IP address of the Management Network.</td> </tr> <tr> <td data-bbox="526 1478 841 1633" style="border: 1px solid #ccc; padding: 5px;"> NOTE: This field appears only when the Management IP type is Static. </td> <td data-bbox="854 1478 1479 1640"></td> </tr> <tr> <td data-bbox="526 1640 854 1770">Netmask Length</td> <td data-bbox="854 1640 1479 1770">Management network's subnet mask value in CIDR format. Eg. 21 for /21.</td> </tr> <tr> <td data-bbox="526 1696 841 1770" style="border: 1px solid #ccc; padding: 5px;"> NOTE: This field appears only when the </td> <td data-bbox="854 1696 1479 1770"></td> </tr> </tbody> </table>	Common Configuration		Datastore	Network datastore shared among all ESXi hosts.	V Series Node Name Prefix	Enter a prefix for the GigaVUE V Series Node name.	V Series Node Name Suffix	Enter a suffix for the GigaVUE V Series Node name.	Name Server	The 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 addresses, separated by comma.	No. of V Series Nodes per Host	Enter the number of GigaVUE V Series Nodes to be deployed in each host.	Management		Network	Management network for GigaVUE V Series Nodes.	IP Type	Select the management network IP type as Static or DHCP.	Gateway IP	Gateway IP address of the Management Network.	NOTE: This field appears only when the Management IP type is Static.		Netmask Length	Management network's subnet mask value in CIDR format. Eg. 21 for /21.	NOTE: This field appears only when the	
Common Configuration																											
Datastore	Network datastore shared among all ESXi hosts.																										
V Series Node Name Prefix	Enter a prefix for the GigaVUE V Series Node name.																										
V Series Node Name Suffix	Enter a suffix for the GigaVUE V Series Node name.																										
Name Server	The 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 addresses, separated by comma.																										
No. of V Series Nodes per Host	Enter the number of GigaVUE V Series Nodes to be deployed in each host.																										
Management																											
Network	Management network for GigaVUE V Series Nodes.																										
IP Type	Select the management network IP type as Static or DHCP.																										
Gateway IP	Gateway IP address of the Management Network.																										
NOTE: This field appears only when the Management IP type is Static.																											
Netmask Length	Management network's subnet mask value in CIDR format. Eg. 21 for /21.																										
NOTE: This field appears only when the																											

Field	Description
	Management IP type is Static.
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000.
Data Interfaces - When using Customer Orchestrated Source as the Traffic Acquisition Method, you must configure two data interfaces.	
Use IPv6	Enable to use IPv6.
	NOTE: This field appears only when Customer Orchestrated Source as the Traffic Acquisition Method.
Network	Tunnel Network for the GigaVUE V Series Nodes.
IP Type	Select the tunnel network IP address type as Static or DHCP.
Gateway IP (optional)	Gateway IP address of the Tunnel Network.
Netmask Length	Tunnel network's subnet mask value in CIDR format. Eg. 21 for /21.
	NOTE: This field appears only when the Tunnel IP type is Static.
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000.
IPv6 Prefix Length	Enter the IPv6 prefix length as 64.
	NOTE: This field appears only when the Use IPv6 toggle button is enabled.
Virtual Disk Format	Select the Virtual Disk Format from the drop-down menu
Deployment Folder	Enter the folder name in vCenter, under which the GigaVUE V Series Nodes must be deployed.
Password	Enter the password you wish to use for the GigaVUE V Series Node.

4. Click **Deploy**. After the GigaVUE V Series Node is deployed in vCenter, it appears on the **Monitoring Domain** page under the Monitoring Domain in which the GigaVUE V Series Node is deployed.

NOTE: GigaVUE-FM can process a maximum of ten GigaVUE V Series Node deployment requests in parallel on VMware vCenter. Each deployment request can have multiple GigaVUE V Series Node for deployment.

Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi

This section provides information on the different ways to upgrade the GigaVUE V Series Nodes and step-by-step instructions on how to upgrade GigaVUE V Series Nodes.

GigaVUE V Series Nodes can be upgraded using the following two ways:

1. You can upgrade all the GigaVUE V Series Node in a monitoring Domain by following the below instructions
 - a. Select the Monitoring Domain.
 - b. Click **Actions > Upgrade Fabric**.
2. You can 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.

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

- You can select an entire monitoring domain and upgrade all the GigaVUE V Series Nodes in that particular monitoring domain, or you can select an 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 once the host is out of the maintenance mode.

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

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

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

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

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

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

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

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

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

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

Monitoring Domain	Connections	Host	Name	Management IP	Tunnel IP	Type	Version	Status
md1								Upgrade Status
	con1							Connected
		10.115.81.184						
			VSeries.12310.115.81.184	10.114.82.69	10.114.84.3	V Series Node	6.6.00	upgrading
			VSeries.new10.115.81.184-1	10.114.84.88	10.114.84.93	V Series Node	6.6.00	upgrading
		10.115.81.185						
			VSeries.new10.115.81.185-1	10.114.82.143	10.114.84.86	V Series Node	6.6.00	upgrad
			VSeries.s10.115.81.185-1	10.115.80.190	10.115.80.191	V Series Node	6.6.00	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 Tasks

▼ Upgrade_GigaVUE_VSERIES_Node | SUCCESS

Clear

Summary

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

Node Statuses

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

▼ Upgrade | IN_PROGRESS

Summary

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

Node Statuses

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

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

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

Configure Monitoring Session

GigaVUE-FM collects inventory data on all V Series nodes deployed in your environment through vCenter connections. You can design your monitoring session to include or exclude the target VMs that you want to monitor. You can also choose to monitor egress, ingress, or all traffic. When a new target VM is added to your environment, GigaVUE-FM automatically detects it and based on the selection criteria, the detected target VMs are added into your monitoring session. Similarly, when a traffic monitoring target VM is removed, it updates the monitoring sessions to show the removed instance. Before deploying a monitoring session, you need to deploy a V Series node in each host where you want to monitor the traffics.

NOTE: Pre-filtering is not supported on VMware ESXi running with V Series nodes.

Refer to the following topics for details:

- [Create a Monitoring Session](#)
- [Edit Monitoring Session](#)
- [Interface Mapping](#)
- [Create Raw Endpoint](#)
- [Create a New Map](#)
- [Add Applications to Monitoring Session](#)
- [Deploy Monitoring Session](#)
- [View Monitoring Session Statistics](#)
- [Visualize the Network Topology](#)
- [Configure VMware Settings](#)

Create a Monitoring Session

GigaVUE-FM automatically collects inventory data on all target instances available in your cloud environment. You can design your monitoring session to include or exclude the instances that you want to monitor. You can also choose to monitor egress, ingress, or all traffic.

When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance into your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions to show the removed instance.

NOTE: You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows > VMware**. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page.

Create A New Monitoring Session

The screenshot shows a form titled "Create A New Monitoring Session". It contains the following fields and controls:

- Alias:** A text input field containing the value "MS1".
- Monitoring Domain:** A dropdown menu with "MD" selected.
- Connection:** Two radio buttons, "Select All" (which is checked) and "Select None". Below these is a list box containing one item, "Scope-2", with a small "x" icon to its right.

At the bottom right of the form are two buttons: "Create" and "Cancel".

3. Enter the appropriate information for the monitoring session as described in the following table.

Field	Description
Alias	The name of the monitoring session.
Monitoring Domain	The name of the monitoring domain that you want to select.
Connection	The connection(s) that are to be included as part of the monitoring domain. You can select the required connections that need to be part of the monitoring domain.

4. Click **Create**. The **Edit Monitoring Session** Canvas page appears.

NOTE: In a Monitoring Session, if a selected VM is connected to VSS and VDS, then the GigaVUE-FM can create tapping for both VSS and VDS network.

The Monitoring Session created in this section, appears in the Monitoring Session details page, displaying the specified session information and target VMs.

The Monitoring Session page also has the following buttons:

Button	Description
Edit	<p>Opens the Edit page for the selected monitoring session.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.</p> </div>
Delete	Deletes the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Deploy	Deploys the selected monitoring session.
Undeploy	Undeploys the selected monitoring session.
Apply Threshold	You can use this button to apply the threshold template created for monitoring cloud traffic health. Refer to Monitor Cloud Health for more detailed information on cloud traffic health, how to create threshold templates and how to apply threshold templates.

Edit Monitoring Session

In the edit monitoring session canvas page, you can add and configure applications, tunnel endpoints, raw endpoints, and maps.

Refer to the following topics for detailed information:

- [Create Ingress and Egress Tunnels](#)
- [Add Applications to Monitoring Session](#)
- [Create Raw Endpoint](#)
- [Create a New Map](#)

The **Edit Monitoring Session** page has the following buttons:

Button	Description
Show Targets	Use to refresh the subnets and monitored instances details that appear in the Instances dialog box.
Interface mapping	Use to change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping topic for more details.
Options	You can enable or disable User Defined Applications here. You can also create and threshold template and apply it to the monitoring session.
Dashboard	The dashboard displays the statistics for all the applications, end points and the maps available in the

Button	Description
	monitoring session.
Ok / Cancel	<p>Ok: Use to save the configurations in the monitoring session when the monitoring session is in undeployed state.</p> <p>Cancel: After the monitoring session is deployed, if you have made any changes and wish to remove them, use this option.</p>
Deploy	Deploys the selected monitoring session. Refer to Deploy Monitoring Session topic for more details.

Interface Mapping

You can change the interface of individual GigaVUE V Series Nodes deployed in a monitoring session. After deploying the monitoring session, if you wish to change the interfaces mapped to an individual GigaVUE V Series Node, you can use the **Interface Mapping** button to map the interface to the respective GigaVUE V Series Nodes. To perform interface mapping for an ingress tunnel:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select a Monitoring session from the list view and click **Actions > Edit**. The Edit Monitoring session page appears.
3. In the Edit Monitoring session canvas page, click on the **Interface Mapping** button.
4. The **Select nodes to deploy the Monitoring Session dialog box** appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.
5. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual GigaVUE V Series Nodes. Then, click **Deploy**.

Create Ingress and Egress Tunnel (VMware vCenter)

Traffic from the GigaVUE V Series Node is distributed to tunnel endpoints in a monitoring session. A tunnel endpoint can be created using a standard L2GRE, VXLAN, UDPGRE, TLS-PCAPNG, UDP, or ERSPAN tunnel.

NOTE: GigaVUE-FM allows you to configure Ingress Tunnels in the Monitoring Session, when the **Traffic Acquisition Method** is UCT-V.

To create a new tunnel endpoint:

1. After creating a new monitoring session, or click **Actions > Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.

X

Add Tunnel Spec

Save

Add To Library

Alias

Alias *

Description

Description (optional)

Type

Select a type... ▾

- Select a type...
- ERSPAN
- L2GRE**
- VXLAN

3. On the New Tunnel quick view, enter or select the required information as described in the following table.

Field	Description	
Alias	The name of the tunnel endpoint. NOTE: Do not enter spaces in the alias name.	
Description	The description of the tunnel endpoint.	
Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN, TLS-PCAPNG, UDP, or UDPGRE to create a tunnel.	
VXLAN		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
NOTE: In the scenario where secure tunnels needs to be established between GigaVUE V Series and a GigaVUE HC Series , you can utilize the Configure Physical Tunnel option provided at the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels at your physical device . Refer to Secure Tunnels section.		
In	Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose Out (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.

Field	Description	
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
UDPGRE		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.

Field	Description												
L2GRE													
Traffic Direction													
The direction of the traffic flowing through the GigaVUE V Series Node.													
<p>NOTE: In the scenario where secure tunnels needs to be established between GigaVUE V Series and a GigaVUE HC Series , you can utilize the Configure Physical Tunnel option provided at the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels at your physical device . Refer to Secure Tunnels section.</p>													
In	Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.												
	<table border="1"> <tr> <td>IP Version</td> <td>The version of the Internet Protocol. Select IPv4 or IPv6.</td> </tr> <tr> <td>Remote Tunnel IP</td> <td>For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.</td> </tr> <tr> <td>Key</td> <td>Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295.</td> </tr> </table>	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295.						
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.											
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.											
Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295.												
Out	Choose Out (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.												
	<table border="1"> <tr> <td>Remote Tunnel IP</td> <td>For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.</td> </tr> <tr> <td>MTU</td> <td>The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.</td> </tr> <tr> <td>Time to Live</td> <td>Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.</td> </tr> <tr> <td>DSCP</td> <td>Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.</td> </tr> <tr> <td>Flow Label</td> <td>Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575.</td> </tr> <tr> <td>Key</td> <td>Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value</td> </tr> </table>	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575.	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value
	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.											
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.											
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.											
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.											
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575.											
Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value												

Field	Description	
		between 0 and 4294967295.
ERSPAN		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
<p>NOTE: In the scenario where secure tunnels needs to be established between GigaVUE V Series and a GigaVUE HC Series , you can utilize the Configure Physical Tunnel option provided at the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels at your physical device . Refer to Secure Tunnels section.</p>		

Field	Description	
In	IP Version	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

Field	Description	
Out	IP Version	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.	
UDP:		

Field	Description	
Out	L4 Destination IP Address	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. Refer to Application Metadata Exporter for more detailed information on what AMX application is and how to configure it.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.

4. Click **Save**.

To delete a tunnel, select the required tunnel and click **Delete**.

To apply threshold template to Tunnel End Points, select the required tunnel end point on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold template, refer to *Monitor Cloud Health* topic.

Tunnel End Points configured can also be used to send or receive traffic from GigaVUE HC Series and GigaVUE TA Series. Provide the IP address of the GigaVUE HC Series and GigaVUE TA Series as the Source or the Destination IP address as required when configuring Tunnel End Points.

After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When multiple egress tunnels are configured for a monitoring session, then the Egress Tunnel column displays the number of egress tunnels configured in that monitoring session. Hover over the number of egress tunnels to display the names of the egress tunnels used in that particular monitoring session.

Tunnel End Points created here can also be viewed in the Tunnel Specifications page. Refer to [Create Tunnel Specifications](#) for more detailed information.

Create Raw Endpoint (VMware vCenter)

This section provides step-by-step instructions on configuring a RAW Endpoint (REP) in the Monitoring Session.

Rules and Notes

- Ingress REP is supported only when the Traffic Acquisition Method is selected as **Customer Orchestrated Source** when configuring the Monitoring Domain. Refer to [Create Monitoring Domain for VMware ESXi](#) for more detailed information on how to select the traffic acquisition method.
- GigaVUE-FM expects the IP address to be configured on the GigaVUE V Series Node interface which will be used for creating RAW Endpoint (REP).

Points to Note:

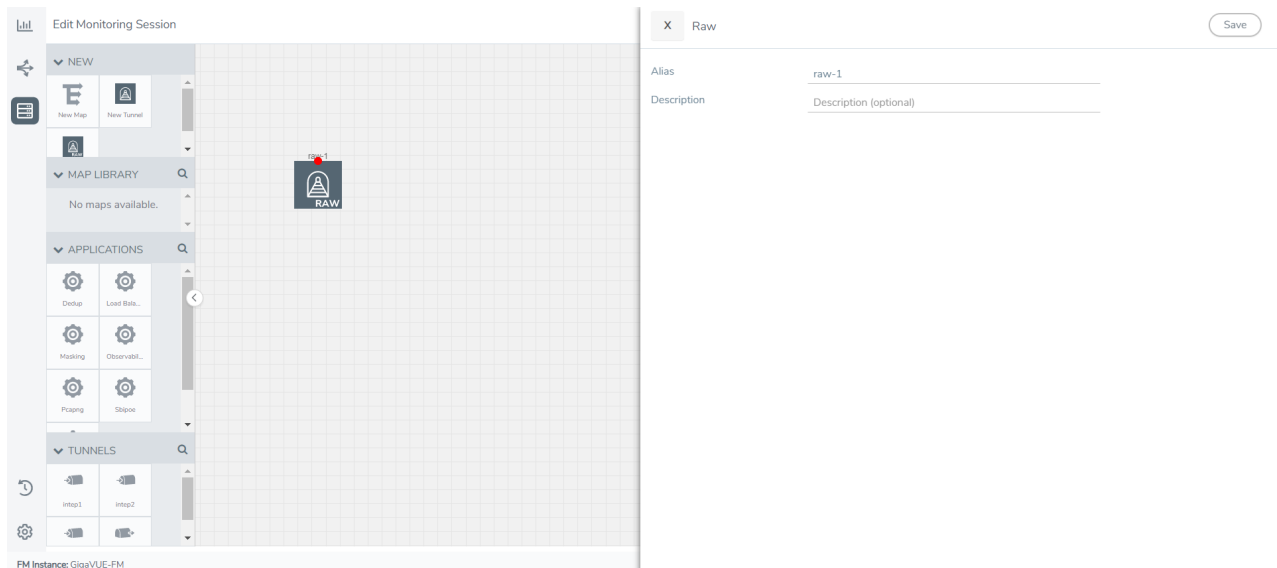
When deploying GigaVUE V Series Nodes in the Monitoring Domain, the number of interfaces varies based on the Traffic Acquisition Method. Refer below for more detailed information:

Traffic Acquisition Method	Display Name	Interface Name	Role	Comments
Customer Orchestrated Source	Network Adapter 1	ens160	Management	
	Network Adapter 2	ens192	Data	Supports Tunnel and RAW endpoint. Can be used for Ingress and Egress REP
	Network Adapter 3	ens224	Data	Supports Tunnel and RAW endpoint. Can be used for Ingress and Egress REP
Platform Tapping	Network Adapter 1	ens160	Management	
	Network Adapter 2	ens192	Data	Supports Tunnel and Egress RAW endpoint.
	Network Adapter 3 - 10	-	Data	Reserved and used for platform tapping (Port Mirroring)

Configure Raw Endpoint in Monitoring Session

To add Raw Endpoint to the monitoring session:

1. Drag and drop **New Raw EndPoint** from **NEW** to the graphical workspace.
2. Click the **RAW** icon and select **Details**. The **RAW** quick view page appears.
3. Enter the alias and description. In the **Alias** field, enter a name for the Raw Endpoint and click **Save**.



4. To deploy the monitoring session after adding the Raw Endpoint click the **Deploy** button on the edit monitoring session page.
5. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Nodes for which you wish to deploy the monitoring session.
6. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual V Series Nodes.
 - a. When using **Customer Orchestrated Source** as the **Traffic Acquisition Method**, data interfaces ens192 and ens224 can be used for ingress and egress REP.
 - b. When using **Platform Tapping** as the **Traffic Acquisition Method**, data interface ens192 should be used for the ingress REP.
7. Click **Deploy**.

Create a New Map


You must have the flow map license to deploy a map in monitoring session.

For new users, the free trial bundle will expire after 30 days and the GigaVUE-FM prompts you to buy a new license. For licensing information refer to *GigaVUE Licensing Guide*.

A map is used to filter the traffic flowing through the GigaVUE V Series Nodes. It is a collection of one or more rules (R). The traffic passing through a map can match one or more rules defined in the map.

Keep in mind the following when creating a map:

Parameter	Description
Rules	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and the (egress or ingress) direction of tapping the network traffic.
Priority	A priority determines the order in which the rules are executed. The priority value can range from 1 to 5, with 1 being the highest and 5 is the lowest priority.
Pass	The traffic from the virtual machine will be passed to the destination.
Drop	The traffic from the virtual machine is dropped when passing through the map.
Traffic Filter Maps	A set of maps that are used to match traffic and perform various actions on the matched traffic.
Inclusion Map	An inclusion map determines the instances to be included for monitoring. This map is used only for target selection.

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	<p>A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the monitoring session.</p> <p>The below formula describes how ATS works:</p> <p>Selected Targets = Traffic Filter Maps \cap Inclusion Maps - Exclusion Maps</p> <p>Below are the filter rule types that work in ATS:</p> <ul style="list-style-type: none"> • mac Source • mac Destination • ipv4 Source • ipv4 Destination • ipv6 Source • ipv6 Destination • VM Name Destination • VM Name Source • VM Tag Destination • VM Tag Source • Host Name <p>The traffic direction is as follow:</p> <ul style="list-style-type: none"> • For any rule type as Source - the traffic direction is egress. • For Destination rule type - the traffic direction is ingress. • For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Points to Note:</p> <ul style="list-style-type: none"> • If no ATS rule filters listed above are used, all VMs and vNICs are selected as targets. When any ATS rule results in a null set, no target is selected and GigaVUE V Series Node does not receive traffic from any VM or vNIC. • When using VM Name filter for selecting the Virtual Machines using Inclusion and Exclusion Maps, wild-cards in VM names are not supported. You must use the prefix of the Virtual Machine name. • When using Inclusion and Exclusion Maps, the following network filters are not supported: <ul style="list-style-type: none"> • VLAN ID • Subnet • Netmask Length </div>
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

To create a new map:

1. After creating a new monitoring session, or click **Actions > Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Map**, drag and drop a new map template to the workspace. The New Map quick view appears.

The screenshot displays the GigaVUE-FM interface. On the left, there is a sidebar with navigation options: NEW, MAP LIBRARY, APPLICATIONS, and TUNNELS. The main workspace is a grid with a blue 'E' icon. On the right, the 'Map: Map1' configuration panel is open, showing the following details:

Name: Map1
Description: [Empty field]

Selected Virtual Machines:

VM Name	Data Center	Cluster	Host	Network Adapter	Port Group
ubuntu-target-rk-2	Datacenter	ClusterDeux	10.115.201.46	00:50:56:9d:ba:89	VM Network
ubuntu-target-rk-3	Datacenter	ClusterDeux	10.115.201.45	00:50:56:9d:7fa:7	VM Network
ubuntu-target-201-46	Datacenter	ClusterDeux	10.115.201.46	00:50:56:9d:43:d3	VDS-ClusterDeux-M...

Rules:

Priority 1 Application Endpoint ID 2

Add a Rule

Rule 1 Condition search... Pass Drop


IP Version
 Version v4 Position 0

3. On the New Map quick view, enter or select the required information as described in the following table.

Field	Description
Name	Name of the new map
Description	Description of the map
Selected Virtual Machines	
Using this option, you can select an individual Network adapter of a virtual machine as a target. You can also view and filter the list of virtual machines available. When using this option, you cannot use Automatic Target Selection (ATS).	
Virtual Machine List	<p>Click on the Virtual Machine List button. The Virtual Machine List quick view opens. Select the virtual machines you wish to use as the target and click on the Apply button in the Virtual Machine List quick view to save your changes.</p> <p>You can also use the filter button to filter the virtual machines. To filter the list of virtual machines:</p> <p>Click on the Filter button to filter the virtual machines based on any of the following criteria:</p> <ul style="list-style-type: none"> • Data Center • Cluster • Host Name • VM Name • VM Tag Category • VM Tag Name <p>After selecting the details, click on the Apply button in the filter dialog box to apply the filters. The list of virtual machines appears based on the filter criteria. Select the virtual machines you wish to use as the target and click on the Apply button in the Virtual Machine List quick view to save your changes.</p>



- VMware tools are not required to discover targets, since GigaVUE-FM can discover targets with ATS using the tags attached to the VMs.
- Targets can be selected by providing the VM's node name or the hostname as selection criteria. A host is selected when the hostname matches all the active targets.
- Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:
 - Traffic Map—Only Pass rules for ATS
 - Inclusion Map—Only Pass rules for ATS
 - Exclusion Map—Only Drop rules for ATS


4. Click on **Rule Sets** tab. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. Refer to [Example-Create a New Map using Inclusion and Exclusion Maps](#) for more detailed information on how to configure Inclusion and Exclusion maps using ATS.
 - a. **To create a new rule set:**
 - i. Click **Actions > New Rule Set**.
 - ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
 - iii. Enter the Application Endpoint in the Application EndPoint ID field.
 - iv. Select a required condition from the drop-down list.
 - v. Select the rule to **Pass** or **Drop** through the map.
 - b. **To create a new rule:**
 - i. Click **Actions > New Rule**.
 - ii. Select a required condition from the drop-down list. Click  and select **Add Condition** to add more conditions.
 - iii. Select the rule to **Pass** or **Drop** through the map.
5. Click **Save**.

NOTE: If a packet is fragmented then all the fragments will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Map Statistics" section in *GigaVUE Fabric Management Guide* for detailed information.

To edit a map, select the map and click **Details**, or click **Delete** to delete the map.

To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold templates, refer to [Monitor Cloud Health](#).

You can also perform the following action in the Monitoring session canvas.

- Click a map and select **Details** to edit the map
- Click a map and select **Delete** to delete the map.
- Click the **Show Targets** button to refresh the subnets and monitored instances details that appear in the **Instances** dialog box.
- Click  to expand the **Targets** dialog box. To view details about a GigaVUE V Series

Node, click the arrow next to the VM.

- In the Instances window, click  to filter the list of instances.

Example- Create a New Map using Inclusion and Exclusion Maps

Consider a monitoring session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

1. Drag and drop a new map template to the workspace. The New map quick view appears.
2. In the **General** tab, enter the name as Map 1 and enter the description. In the **Rule sets** tab, enter the priority and Application Endpoint ID.
3. Select the condition as VM Name and enter the **target**. This includes the instances target-1-1, target-1-2, target-1-3, target-2-1, and target-2-2.
4. Click on the Expand icon at the bottom of the Monitoring session canvas. The Inclusion Maps and Exclusion Maps section appears.
5. Drag and drop a new map template to the Inclusion Maps region. The New Map quick view appears. Enter the Name and Description of the map.
 - a. In the **General** tab, enter the name as Inclusionmap1 and enter the description. In the **Rule Sets**, enter the priority and Application Endpoint ID.
 - b. Select the condition as VM Name and enter the VM Name as **target-1**. Then the instance with VM name **target-1-1**, **target-1-2**, and **target-1-3** will be included.
6. Drag and drop a new map template to the Exclusion Maps region. The New Map quick view appears. Enter the details as mentioned in the above section.
 - a. In the **General** tab, enter the name as Exclusionmap1 and enter the description. In the **Rule Sets** tab, enter the priority and Application Endpoint ID.
 - b. Select the condition as VM Name and enter the VM Name as **target-1-3**. Then the instance **target-1-3** will be excluded.

Based on this configuration, the Automatic Target Selection will select the instances target-1-1 and target-1-2 as target.

Map Library

To reuse a map,

1. In the Monitoring Session page, Click **Actions > Edit**. The Edit Monitoring Session page opens.
2. Click the map you wish to save as a template. Click **Details**. The Application quick view appears.
3. Click **Add to Library**. Save the map using one of the following ways:
4. Select an existing group from the **Select Group** list or create a **New Group** with a

name.

5. Enter a description in the **Description** field, and click **Save**.

The Map is saved to the **Map Library** in the Edit Monitoring Session Canvas page. This map can be used from any of the monitoring session. To reuse the map, drag and drop the saved map from the Map Library.

Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop the following items to the canvas as required:
 - Maps from the **MAP LIBRARY** section
 - Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
 - GigaSMART apps from the **APPLICATIONS** section
 - Egress tunnels from the **TUNNELS** section
2. After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

NOTE: You can drag multiple arrows from a single map and connect them to different maps.

3. (Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method) Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.

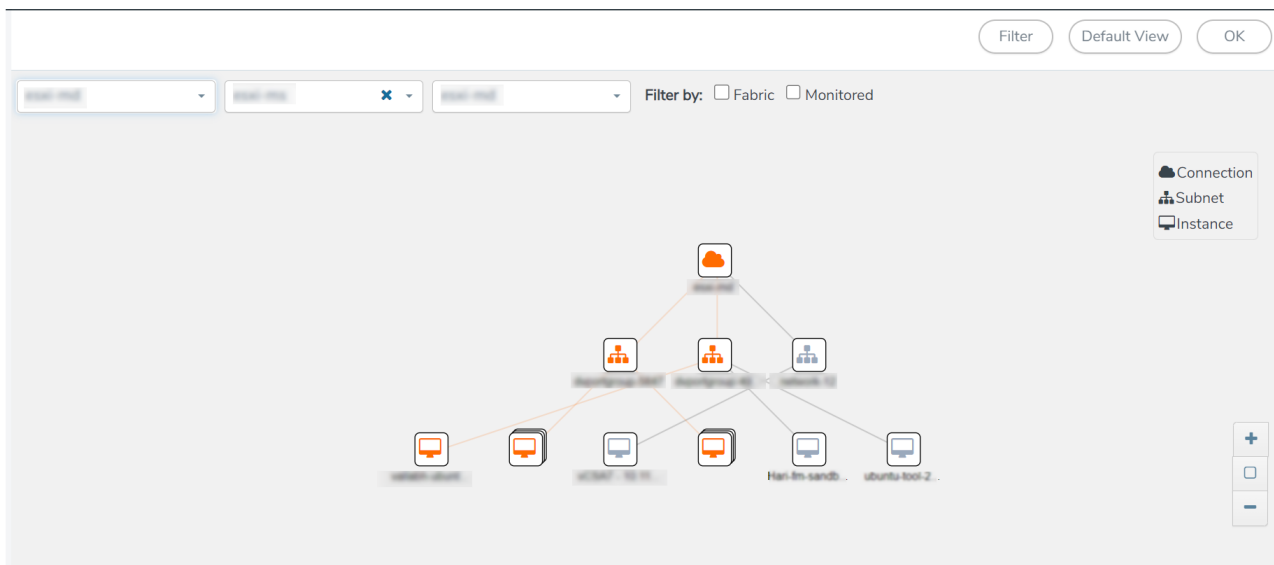
4. Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series nodes. Click on the status link in the Status column on the Monitoring Session page to view the Monitoring Session Deployment Report. When you click on the Status link, the Deployment Report is displayed. If the monitoring session is not deployed properly, then one of the following errors is displayed in the Status column.
 - Partial Success—The session is not deployed on one or more instances due to V Series node failure.
 - Failure—The session is not deployed on any of the V Series nodes.The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

Visualize the Network Topology

You can have multiple connections in GigaVUE-FM. Each connection can have multiple monitoring sessions configured within them. You can select the connection and the monitoring session to view the selected subnets and instances in the topology view.

To view the topology diagram in GigaVUE-FM:

1. On the Monitoring Session page, select **Topology** tab. The Topology page appears.
2. Select a monitoring domain from the **Select monitoring domain...** list.
3. Select a connection from the **Select monitoring session...**list.
4. Select a monitoring session from the **Select connection...** list. The topology view of the monitored subnets and instances in the selected session are displayed.



5. (Optional) Hover over or click the subnet or VM Group icons to view the subnets or instances present within the group.

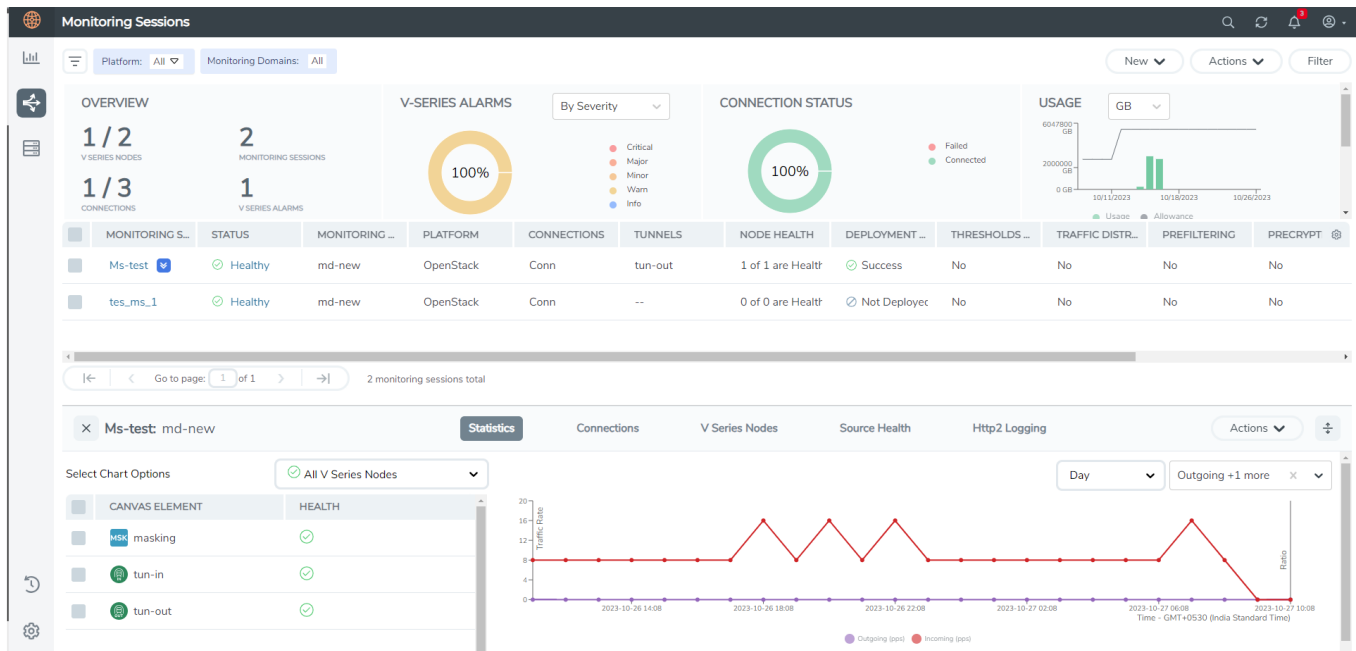
In the topology page, you can also do the following:

- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitoring instances.
- Use the arrows at the right-bottom corner to move the topology page up, down, left, or right. Click the **Fit-to-Width** icon to fit the topology diagram according to the width of the page.
- Use **+** or **-** icons to zoom in and zoom out the topology view.

View Monitoring Session Statistics

The Monitoring Session Statistics page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.

On the Monitoring Sessions page, click the name of the monitoring session, and then click **View**. A split window appears displaying the **Statistics**, **Connections**, **V Series Nodes**, **Source Health** and **Http2 Logging** of the monitoring session as shown:



To know more about the statistics of the session, click **Statistics**.

You can view the statistics by applying different filters as per the requirements of analysing the data. GigaVUE-FM allows you to perform the following actions on the Monitoring Session Statistics page:

- You can view the **Statistics** in full screen. To view in full screen, click the **Actions** drop-down list at the right corner of the window, and select **Full Screen. Statistics** appear in full screen.
- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can select the options from the drop-down list box.
 - For the hourly statistics, the data points are plotted every five minutes.
 - For the daily statistics, the data points are plotted every one hour.
 - For the weekly statistics, the data points are plotted every six hours.
 - For the monthly statistics, the data points are plotted every day.
 - The data points in graph are plotted every five minutes, one hour, six hours, or a day based on the option selected in the drop-down menu.

NOTE: The latest data point displayed in the graph for any particular time will be less than five minutes, one hour, six hours, or day from the time at which the statistics are checked based on the option selected from the drop-down menu. For example, if you are viewing the hourly statistics at 11.30, the latest data point in the graph would be 11.25.

- The statistical data between two data points is displayed at the first data point. For example, the data between 11.30 and 12.30 is displayed at the data point 11.30 when viewing the daily statistics.

- You can filter the traffic and view the statistics based on factors such as **Incoming, Outgoing, Ratio (Out/In), Incoming Packets, Outgoing Packets, Ratio (Out/In) Packets**. You can select the options from the drop-down list box.
- You can also view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual GigaVUE V Series Node, select the name of the **V Series Node** from the drop-down list for which you want to view the statistics from the GigaVUE V Series Node drop-down menu on the top left corner of the Monitoring Session Statistics page.
- You can view the statistics of the elements involved in the monitoring session. To view the statistics, click on the **Select Chart Options** page and select the elements associated with the session.
- Directly on the graph, you can click on **Incoming(Mbps), Outgoing (Mbps), or Ratio (Out/In) (Mbps)** to view the statistics individually.



Raw EndPoint (REP) is a part of the monitoring session but can also receive the bypassed traffic that is not filtered by the map, so it is recording more packets than expected. For example, if the map has a rule as IPv4, but the REP can receive the bypassed (non-ipv4) traffic. The recorded number of packets from the V Series node can be more than expected.

View Health Status on the Monitoring Session Page

You can view the health status of the monitoring session and the components deployed, in the monitoring session page. Refer to [Monitor Cloud Health](#) for more detailed information on how to configure cloud health and view health status.

To view the health status on the Monitoring Session page:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. The Monitoring Session page appears. The list view in the Monitoring Domain page displays the details of the Monitoring Session.

The following columns in the monitoring session page are used to convey the health status:

Status

This column displays the health status (both traffic and configuration) of the entire monitoring session. The status is marked healthy only if both the traffic and configuration health status is healthy, even if either of them is unhealthy, then the health status is moved to unhealthy.

Node Health

This column displays the configuration and traffic health status of the monitoring session deployed in V Series Nodes. This column provides information on the number of GigaVUE V Series Nodes that have healthy traffic flow and monitoring session successfully deployed to the total number of V Series Nodes that have monitoring session deployed.

NOTE: Node Health only displays the health status, so if the V Series Node is down it will not be reflected in the monitoring session page.

Targets Source Health

1. On the Monitoring Session page, click the name of the monitoring session and click **View**.
2. Select the **Connections** tab.

This column displays the configuration health status of the monitoring session deployed in targets. This column provides information on the number of monitoring sessions successfully deployed on a particular target to the total number of monitoring session deployed on that particular target.

You can view the health status of the individual targets and also the error message associated with them, by clicking on the Target Source Health column.

Add Applications to Monitoring Session

GigaVUE Cloud Suite with GigaVUE V Series Node supports the following GigaSMART applications in the GigaVUE-FM canvas:

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- Header Stripping
- 5G-Service Based Interface Application

- 5G Cloud CASA VTAP Support
- Application Metadata Exporter
- SSL Decrypt

For more detailed information on how to configure these application, refer to *GigaVUE V Series Applications Guide*.

Migrate Application Intelligence Session to Monitoring Session

Starting from Software version 6.5.00, Application Intelligence solution can be configured from Monitoring Session Page. After upgrading to 6.5.00, you cannot create a new Application Intelligence Session or edit an existing Application Intelligence Session for virtual environment from the **Application Intelligence** page. The following operations can only be performed using the existing Application Intelligence Session:

- View Details
- Delete
- Forced Delete

It is highly recommended to migrate the existing sessions to Monitoring Session for full functionality. GigaVUE-FM will migrate all your virtual Application Intelligence sessions and their connections seamlessly. All sessions will be rolled back to their original states if the migration fails.



Points to Note:

- You must be a user with write access for the **Traffic Control Management** Resource in GigaVUE-FM to perform this migration. Refer to [Create Roles](#) section for more detailed information on how to configure roles with write access for the Traffic Control Management resource.
- If any of the existing Application Intelligence Session is in PENDING or SUSPENDED, then the migration will not be triggered. Resolve the issue and start the migration process.
- If any of the existing Application Intelligence Session is in FAILED state due to incorrect configuration, then the migration will not be triggered. Resolve the issue and start the migration process.
- If an existing Monitoring Session has a same name as the Application Intelligence Session, then the migration will not be triggered. Change the existing Monitoring Session name to continue with the migration process.



- If any of the existing Application Intelligence Session has Application Filtering configured with Advanced Rules as Drop Rule and No Rule Match Pass All in the 5th rule set, you cannot continue with the migration. In the Monitoring Session either only Pass All or Advanced Rules as Drop is supported in the fifth Rule Set. Please delete this session and start the migration.
- When migrating the Application Intelligence Session, in rare scenarios, the migration process might fail after the pre-validation. In such cases, all the Application Intelligence Session roll back to the Application Intelligence page. Contact Technical Support for migrating the Application Intelligence Session in these scenarios.

To migrate your existing Application Intelligence Session to Monitoring Session Page, follow the steps given below:

1. On the left navigation pane, select **Traffic > Solutions > Application Intelligence**. You cannot create a new Application Intelligence Session from this page.
2. When you have an existing virtual Application Intelligence Session in the above page, the **Migrate Virtual Application Intelligence** dialog box appears.
3. Review the message and click **Migrate**.
4. The **Confirm Migration** dialog box appears. The list Application Intelligence Session that will be migrated appears here.
5. Review the message and click **Migrate**.
6. GigaVUE-FM checks for the requirements and then migrates the Application Intelligence Sessions to the Monitoring Session Page.
7. Click on the **Go to Monitoring Session Page** button to view the Application Intelligence Session that are migrated to the monitoring session page.

All the virtual Application Intelligence Sessions in the Application Intelligence page is migrated to the Monitoring Session Page.

Post Migration Notes for Application Intelligence

After migrating Application Intelligence session to Monitoring Session page, you must consider the following things:

1. If you wish to enable Secure tunnels after migrating the Application Intelligence Session, follow the steps given below.
 - a. Enable Secure Tunnels in the **Options** page. Refer to [Enable Prefiltering, Precryption, and Secure Tunnel](#) topic more detailed information on how to enable secure tunnel for a monitoring Session.
 - b. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Undeploy**. The monitoring session is undeployed.
 - c. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Edit**. The **Edit Monitoring Session** Canvas page appears.
 - d. Add the Application Intelligence applications.
 - e. Modify the Number of Flows as per the below table:

Cloud Platform	Instance Size	Maximum Number of Flows
VMware	Large (8 vCPU and 16 GB RAM)	200k
AWS	AMD - Large (c5n.2xlarge)	300k
	AMD - Medium (t3a.xlarge)	100k
	ARM - Large (c7gn.2xlarge)	100k
	ARM - Medium (m7g.xlarge)	200k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16 GB RAM)	200k

NOTE: Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.

- f. Click **Deploy**. Refer to [Application Intelligence](#) topic for more detailed information on how to deploy the Application Intelligence applications.
2. When GigaVUE-FM version is 6.5.00, and the GigaVUE V Series Node version is below 6.5.00, after migrating the Application Intelligence Session to the Monitoring Session and redeploying the monitoring session, a momentary loss in the statistical data of the Application Visualization application will be seen while redeploying the monitoring session.
3. After migrating the Application Intelligence Session to monitoring session, if you wish to make any configuration changes, then the GigaVUE V Series Node version must be greater than or equal to 6.3.00.

Monitor Cloud Health

GigaVUE-FM allows you to monitor the traffic and configuration health status of the monitoring session and its individual components. This section provides detailed information on how to view the traffic and configuration health status of the monitoring session and its individual components. Refer to the following topics for more detailed information on configuration health, traffic health and how to view the health status:

- [Configuration Health Monitoring](#)
- [Traffic Health Monitoring](#)
- [View Health Status](#)

Configuration Health Monitoring

The configuration health status provides us detailed information about the configuration and deployment status of the deployed monitoring session.

This feature is supported for the following fabric components and features on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Nutanix

For UCT-Vs:

- AWS
- Azure
- OpenStack

For VPC Mirroring:

- AWS

For OVS Mirroring and VLAN Trunk Port:

- OpenStack

To view the configuration health status, refer to the [View Health Status](#) section.

Traffic Health Monitoring

GigaVUE-FM allows you to monitor the traffic health status of the entire monitoring session and also the individual V Series Nodes for which the monitoring session is configured. Traffic health monitoring focuses on identifying any discrepancies (packet drop or overflow etc) in the traffic flow. When any such discrepancies are identified, GigaVUE-FM propagates the health status to corresponding monitoring session. GigaVUE-FM monitors the traffic health status in near real-time. GigaVUE V Series Node monitors the traffic, when the traffic limit goes beyond the upper or lower threshold values that is configured, it notifies GigaVUE-FM, based on which traffic health is computed.

NOTE: When GigaVUE-FM and GigaVUE V Series Nodes are deployed in different cloud platforms, then the GigaVUE-FM public IP address must be added to the **Data Notification Interface** as the Target Address in the Event Notifications page. Refer to section in the *GigaVUE Administration Guide* for configuration details.

This feature is supported for GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Third Party Orchestration

The following section gives step-by-step instructions on creating, applying, and editing threshold templates across a monitoring session or an application, and viewing the traffic health status. Refer to the following section for more detailed information:

- [Supported Resources and Metrics](#)
- [Create Threshold Template](#)
- [Apply Threshold Template](#)
- [Edit Threshold Template](#)
- [Clear Thresholds](#)

Keep in mind the following points when configuring a threshold template:

- By default Threshold Template is not configured to any monitoring session. If you wish to monitor the traffic health status, then create and apply threshold template to the monitoring session.
- Editing or redeploying the monitoring session will reapply all the threshold policies associated with that monitoring session.

- Deleting or undeploying the monitoring session will clear all the threshold policies associated with that monitoring session.
- After applying threshold template to a particular application, you need not deploy the monitoring session again.

Supported Resources and Metrics

The following table lists the resources and the respective metrics supported for traffic health monitoring

Resource	Metrics	Threshold types	Trigger Condition
Tunnel End Point	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
RawEnd Point	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
Map	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
Slicing	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
Masking	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under

Dedup	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
HeaderStripping	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
TunnelEncapsulation	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
LoadBalancing	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
SSLDecryption	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
Application Metadata	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
AMI Exporter	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
Geneve	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under
5G-SBI	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under

Create Threshold Template

To create threshold templates:

1. There are two ways to navigate to the Threshold Template page, they are:
 - a. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Then, click on the **Threshold Template** tab in the top navigation bar.
 - b. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Select a Monitoring Session and click **Actions > Edit**. In the Edit Monitoring Session page, click **Options > Threshold**.
2. The **Threshold Template** page appears. Click **Create** to open the **New Threshold Template** page.
3. Enter the appropriate information for the threshold template as described in the following table.

Field	Description
Threshold Template Name	The name of the threshold template.
Thresholds	
Monitored Objects	Select the resource for which you wish to apply the threshold template. Eg: TEP, REP, Maps, Applications like Slicing, Dedup etc
Time Interval	Frequency at which the traffic flow needs to be monitored.
Metric	Metrics that need to be monitored. For example: Tx Packets, Rx Packets.
Type	Difference: The difference between the stats counter at the start and end time of an interval, for a given metric. Derivative: Average value of the statistics counter in a time interval, for a given metric.
Condition	Over: Checks if the statistics counter value is greater than the 'Set Trigger Value'. Under: Checks if the statistics counter value is lower than the 'Set Trigger Value'.
Set Trigger Value	Value at which a traffic health event is raised, if the statistics counter goes below or above this value, based on the condition configured.
Clear Trigger Value	Value at which a traffic health event is cleared, if the statistics counter goes below or above this value, based on the condition configured.

4. Click **Save**. The newly created threshold template is saved, and it appears on the **Threshold Template** page.

Apply Threshold Template

You can apply your threshold template across the entire monitoring session and also to a particular application.

Apply Threshold Template to Monitoring Session

To apply the threshold template across a monitoring session, follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds** page appears. To apply a threshold template across a Monitoring Session, select the template you wish to apply across the Monitoring Session from the Threshold Template drop-down menu.
4. Click **Done**.

Apply Threshold Template to Applications

To apply the threshold template to a particular application in the Monitoring Session follow the steps given below:

NOTE: Applying the threshold template across Monitoring Session will not over write the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it over writes the existing threshold value for that particular application.

1. On the **Monitoring Session** page. Click **Actions > Edit**. The Edit Monitoring Session page with the canvas page appears.
2. Click on the application for which you wish to apply or change a threshold template and click **Details**. The **Application** quick view opens.
3. Click on the **Thresholds** tab. Select the template you wish to apply from the Threshold Template drop-down menu or enter the threshold values manually.
4. Click **Save**.

NOTE: Threshold Template is not supported for pcapng and sbipoe applications. The Threshold configuration for these applications will not be applied.

Edit Threshold Template

To edit a particular threshold template follow the steps given below:

1. On the Threshold Template page, Click **Edit**. The **Edit Threshold Template** page appears.
2. The existing threshold templates will be listed here. Edit the templates you wish to modify.
3. Click **Save**.

NOTE: Editing a threshold template does not automatically apply the template to Monitoring Session. You must apply the edited template to Monitoring Session for the changes to take effect.

Clear Thresholds

You can clear the thresholds across the entire Monitoring Session and also to a particular application.

Clear Thresholds for Applications

To clear the thresholds of a particular application in the Monitoring Session follow the steps given below:

1. On the **Monitoring Session** page. Click **Actions > Edit**. The Edit Monitoring Session page with canvas page appears.
2. Click on the application for which you wish to clear the thresholds and click **Details**. The **Application** quick view opens.
3. Click on the **Thresholds** tab. Click **Clear All** and then Click **Save**.

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a Monitoring Session follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select the Monitoring Session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds** page appears. Click **Clear**.

NOTE: Clearing thresholds at Monitoring Session level does not clear the thresholds that were applied specifically at the application level. To clear thresholds for a particular application refer to [Clear Thresholds for Applications](#)

View Health Status

You can view the health status of the monitoring session on the Monitoring Session details page. The health status of the monitoring session is healthy only if both the configuration health and traffic health are healthy.

View Health Status of an Application

To view the health status of an application across an entire monitoring session:

1. After creating a Monitoring Session, go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Select a monitoring session, click **Actions > Edit**. The Edit Monitoring Session Page appears.
2. Click on the application for which you wish to see the health status and select **Details**. The quick view page appears.
3. Click on the **HEALTH STATUS** tab.

This displays the configuration health and traffic health of the application and also the thresholds applied to that particular application.

NOTE: The secure tunnel status is refreshed for every 5 minutes, and the GigaVUE-FM does not display UCT-V secure tunnel status that is older than 7 minutes. If the secure tunnel in the UCT-V is removed, it takes up to 7 minutes to reset the status on the GigaVUE-FM.

View Health Status for Individual GigaVUE V Series Nodes

You can also view the health status of the view the health status of an individual GigaVUE V Series Node. To view the configuration health status and traffic health status of the V Series Nodes:

1. On the Monitoring Session page, click the name of the monitoring session and click **View**.
2. Select the **Statistics** tab.
3. Select the GigaVUE V Series Node from the **All V Series Nodes** drop-down menu.

View Application Health Status for Individual V Series Nodes

To view the application configuration and traffic health status of the GigaVUE V Series Nodes:

1. On the Monitoring Session page, click the name of the monitoring session and click **View**.
2. Select the **Statistics** tab.
3. Select the GigaVUE V Series Node from the **All V Series Nodes** drop-down menu.
4. The list view displays the list of applications for the selected GigaVUE V Series Node and the health status of each application.

You can also view the cloud health Status in the Monitoring Session Page, refer to [View Health Status on the Monitoring Session Page](#) topic for more detailed information on how to view cloud health status in the Monitoring Session page.

Configure VMware Settings

This section provides information on how to configure the maximum number of connections, refresh intervals for instance and non-instance inventory, and maximum batch size for monitoring session updates.

To configure the VMware Settings:

Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and then click **Settings > Advanced Settings** to edit the VMware vCenter settings.

Advanced Settings

Edit

Maximum number of vCenter connections allowed	20
Refresh interval for VM target selection inventory (secs)	300
Refresh interval for fabric deployment inventory (secs)	86400
Traffic distribution tunnel range start	8000
Traffic distribution tunnel range end	8512

Refer to the following table for details:

Settings	Description
Maximum number of vCenter connections allowed	Specifies the maximum number of vCenter connections you can establish in GigaVUE-FM
Refresh interval for VM target selection inventory (secs)	Specifies the frequency for updating the state of target VMs in VMware vCenter
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for updating the state of GigaVUE-FM fabrics deployed in VMware vCenter
Traffic distribution tunnel range start	Specifies the start range value of the tunnel ID.
Traffic distribution tunnel range end	Specifies the closing range value of the tunnel ID.

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics¹ you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects. Refer to Analytics topic in *GigaVUE Fabric Management Guide* for more detailed information on Analytics.

Rules and Notes:

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations. Refer to the Clone Dashboard section in GigaVUE-FM Installation and Upgrade Guide for more details.


¹Analytics uses the OpenSearch front-end application to visualize and analyze the data in the OpenSearch database of GigaVUE-FM.

- Use the Time Filter option to select the required time interval for which you need to view the visualization.

Virtual Inventory Statistics and Cloud Applications Dashboard

Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly. Refer to the [Analytics](#) section in *GigaVUE Fabric Management Guide* for details on how to create a new dashboard, clone a dashboard, create a new visualization, and other information about the Discover page and Reports page.

To access the dashboards:

1. Go to  -> **Analytics -> Dashboards.**
2. Click on the required dashboard to view the visualizations.

The following table lists the various virtual dashboards:

Dashboard	Displays	Visualizations	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: <ul style="list-style-type: none"> • Number of Monitoring Sessions • Number of V Series Nodes • Number of Connections • Number of GCB Nodes You can filter the visualizations based on the following control filters: <ul style="list-style-type: none"> • Platform • Health Status 	<i>V Series Node Status by Platform</i>	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		<i>Monitoring Session Status by Platform</i>	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		<i>Connection Status by Platform</i>	Number of healthy and unhealthy connections for each of the supported cloud platforms
		<i>GCB Node Status by Platform</i>	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node.	<i>V Series Node Maximum CPU Usage Trend</i>	Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval,

Dashboard	Displays	Visualizations	Displays
	<p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> Platform Connection V Series Node 		<p>for the past one hour.</p> <p>NOTE: The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V Series nodes do not have service cores, therefore the CPU usage is reported as 0.</p>
		<i>V Series Node with Most CPU Usage For Past 5 minutes</i>	<p>Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes.</p> <p>NOTE: You cannot use the time based filter options to filter and visualize the data.</p>
		<i>V Series Node Rx Trend</i>	<p>Receiving trend of the V Series node in 5 minutes interval, for the past one hour.</p>
		<i>V Series Network Interfaces with Most Rx for Past 5 mins</i>	<p>Total packets received by each of the V Series network interface for the past 5 minutes.</p> <p>NOTE: You cannot use the time based filter options to filter and visualize the data.</p>
		<i>V Series Node Tunnel Rx Packets/Errors</i>	<p>Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising</p>

Dashboard	Displays	Visualizations	Displays
			{monDomain, conn, VSN, tunnelName}, before aggregation.
		<i>V Series Node Tunnel Tx Packets/Errors</i>	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	<p>Displays visualizations related to Dedup application.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> • Platform • Connection • V Series Node 	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload.
		<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the de-duplicated packets received against the de-duplication application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	<p>Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V Series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. • V Series node: Management IP of the V Series node. Choose the required V Series node from the drop-down. 	<i>Tunnel Bytes</i>	<p>Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.</p> <ul style="list-style-type: none"> • For input tunnel, transmitted traffic is displayed as zero. • For output tunnel, received traffic is displayed as zero.

Dashboard	Displays	Visualizations	Displays
	<ul style="list-style-type: none"> • Tunnel: Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. <p>The following statistics are displayed for the tunnel:</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets 		
		<i>Tunnel Packets</i>	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
App (Virtual)	<p>Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V Series node.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session • V Series node • Application: Select the required application. By default, the visualizations displayed includes all the applications. <p>By default, the following statistics are displayed:</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Errored Packets • Dropped Packets 	<i>App Bytes</i>	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	Visualizations	Displays
		<i>App Packets</i>	Displays received traffic vs transmitted traffic, as the number of packets.
End Point (Virtual)	<p>Displays Byte and packet level statistics for the un-tunneled traffic deployed on the V Series nodes.</p> <p>The following statistics that are shown for Endpoint (Virtual):</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets <p>The endpoint drop-down shows <i><V Series Node Management IP address : Network Interface></i> for each endpoint.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session • V Series node • Endpoint: Management IP of the V Series node followed by the Network Interface (NIC) 	<i>Endpoint Bytes</i>	Displays received traffic vs transmitted traffic, in Bytes.
		<i>Endpoint Packets</i>	Displays received traffic vs transmitted traffic, as the number of packets.

NOTE: The Tunnel (Virtual), App (Virtual) and Endpoint (Virtual) dashboards do not show data from the previous releases if the *Monitoring Session [Platform : Domain : Connection]* dashboard filter is applied. This is because, this filter relies on the new attributes in the OpenSearch database, which are available only from software version 5.14.00 and beyond.

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 VUE Community](#)

Documentation

This table lists all the guides provided for GigaVUE Cloud Suite 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 Cloud Suite 6.8 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 Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite 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 Cloud Suite 6.8 Hardware and Software Guides

GigaVUE-TA200 Hardware Installation Guide

GigaVUE-TA200E Hardware Installation Guide

GigaVUE-TA400 Hardware Installation Guide

GigaVUE-OS Installation Guide for DELL S4112F-ON

G-TAP A Series 2 Installation Guide

GigaVUE M Series Hardware Installation Guide

GigaVUE-FM Hardware 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

Cloud Guides

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

GigaVUE V Series Applications Guide

GigaVUE V Series Quick Start Guide

GigaVUE Cloud Suite Deployment Guide - AWS

GigaVUE Cloud Suite Deployment Guide - Azure

GigaVUE Cloud Suite Deployment Guide - OpenStack

GigaVUE Cloud Suite Deployment Guide - Nutanix

GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)

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

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

Universal Cloud TAP - Container Deployment Guide

GigaVUE Cloud Suite 6.8 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)
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	
For Online Topics	Online doc link	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to 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, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)