



# GigaVUE Cloud Suite for Nutanix - Deployment Guide

**GigaVUE Cloud Suite**

Product Version: 6.6

Document Version: 1.0

Last Updated: Friday, April 12, 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](http://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
6.6.00	1.0	3/22/2024	The original release of this document with 6.6.00 GA.

# Contents

<b>GigaVUE Cloud Suite for Nutanix - Deployment Guide</b> .....	<b>1</b>
Change Notes .....	3
Contents .....	4
<b>GigaVUE Cloud Suite Deployment Guide - Nutanix (GigaVUE V Series)</b> .....	<b>7</b>
<b>Overview of GigaVUE Cloud Suite for Nutanix</b> .....	<b>7</b>
Components of GigaVUE Cloud Suite for Nutanix .....	8
Cloud Overview Page .....	9
Overall Cloud Overview Page .....	10
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 .....	13
<b>Points to Note (Nutanix)</b> .....	<b>14</b>
<b>Prerequisites for GigaVUE Cloud Suite for Nutanix Deployment</b> ....	<b>14</b>
Minimum Compute Requirements .....	15
Network Firewall Requirements .....	15
Default Login Credentials .....	16
<b>License Information</b> .....	<b>17</b>
Volume Based License (VBL) .....	17
Base Bundles .....	18
Bundle Replacement Policy .....	18
Add-on Packages .....	18
How GigaVUE-FM Tracks Volume-Based License Usage .....	19
Manage and Activate Volume-based Licenses .....	19
Apply License .....	23
<b>Install and Upgrade GigaVUE-FM</b> .....	<b>23</b>
<b>Upload Fabric Images</b> .....	<b>23</b>
<b>Deploy GigaVUE Cloud Suite for Nutanix</b> .....	<b>24</b>
Install Custom Certificate .....	24
Upload Custom Certificates using GigaVUE-FM .....	24
Adding Certificate Authority .....	25

CA List .....	25
Create a Monitoring Domain .....	26
Configure GigaVUE Fabric Components in GigaVUE-FM .....	27
Nutanix Fabric Launch Configuration .....	27
<b>Secure Tunnels .....</b>	<b>30</b>
Supported Platforms .....	31
Configure Secure Tunnel .....	32
Prerequisites .....	32
Notes .....	32
Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2 .....	32
<b>Configure Monitoring Session .....</b>	<b>37</b>
Create a Monitoring Session .....	37
Edit Monitoring Session .....	39
Monitoring Session Options .....	40
Interface Mapping .....	40
Create Ingress and Egress Tunnel .....	41
Create a New Map .....	46
Example- Create a New Map using Inclusion and Exclusion Maps .....	51
Map Library .....	51
Add Applications to Monitoring Session .....	52
View Monitoring Session Statistics .....	54
Visualize the Network Topology .....	55
<b>Cloud Health Monitoring - Configuration Health Monitoring .....</b>	<b>56</b>
View Monitoring Session Configuration Health .....	57
Health .....	57
V Series Node Health .....	57
Target Source Health .....	58
View Monitoring Session Statistics .....	58
View Monitoring Session Diagram .....	58
<b>Analytics for Virtual Resources .....</b>	<b>59</b>
Virtual Inventory Statistics and Cloud Applications Dashboard .....	59
<b>Administer GigaVUE Cloud Suite for Nutanix .....</b>	<b>64</b>
Configure Nutanix Settings .....	64
Role Based Access Control .....	64
About Events .....	65
About Audit Logs .....	67
<b>Additional Sources of Information .....</b>	<b>69</b>
Documentation .....	69
How to Download Software and Release Notes from My Gigamon .....	71
Documentation Feedback .....	72

Contact Technical Support .....	73
Contact Sales .....	73
Premium Support .....	73
The VUE Community .....	74
<b>Glossary .....</b>	<b>75</b>

# GigaVUE Cloud Suite Deployment Guide - Nutanix (GigaVUE V Series)

This guide describes how to install, configure, and deploy the GigaVUE Cloud Suite for Nutanix- (GigaVUE V Series) in the Prism Central environment. Use this document for instructions on configuring the GigaVUE Cloud Suite Cloud components and setting up the traffic monitoring sessions for the Nutanix.

Topics:

- [Overview of GigaVUE Cloud Suite for Nutanix](#)
- [Points to Note \(Nutanix\)](#)
- [Prerequisites for GigaVUE Cloud Suite for Nutanix Deployment](#)
- [License Information](#)
- [Install and Upgrade GigaVUE-FM](#)
- [Upload Fabric Images](#)
- [Deploy GigaVUE Cloud Suite for Nutanix](#)
- [Cloud Health Monitoring - Configuration Health Monitoring](#)
- [Analytics for Virtual Resources](#)
- [Administer GigaVUE Cloud Suite for Nutanix](#)

## Overview of GigaVUE Cloud Suite for Nutanix

GigaVUE Cloud Suite™ for Nutanix provides in-depth visibility to enhance tool effectiveness, optimize performance, and accelerate troubleshooting of private cloud environments. You can aggregate and optimize traffic from your Nutanix deployments with the Gigamon Deep Observability Pipeline. This provides centralized control, allowing the right traffic to be forwarded to the right tools.

Nutanix Prism can instantiate Gigamon GigaVUE® Cloud Suite with GigaVUE Universal Cloud Tap (UCT) instances to monitor and control operations. Compute VMs can also be directed to copy micro-segment traffic and send to GigaVUE visibility nodes.

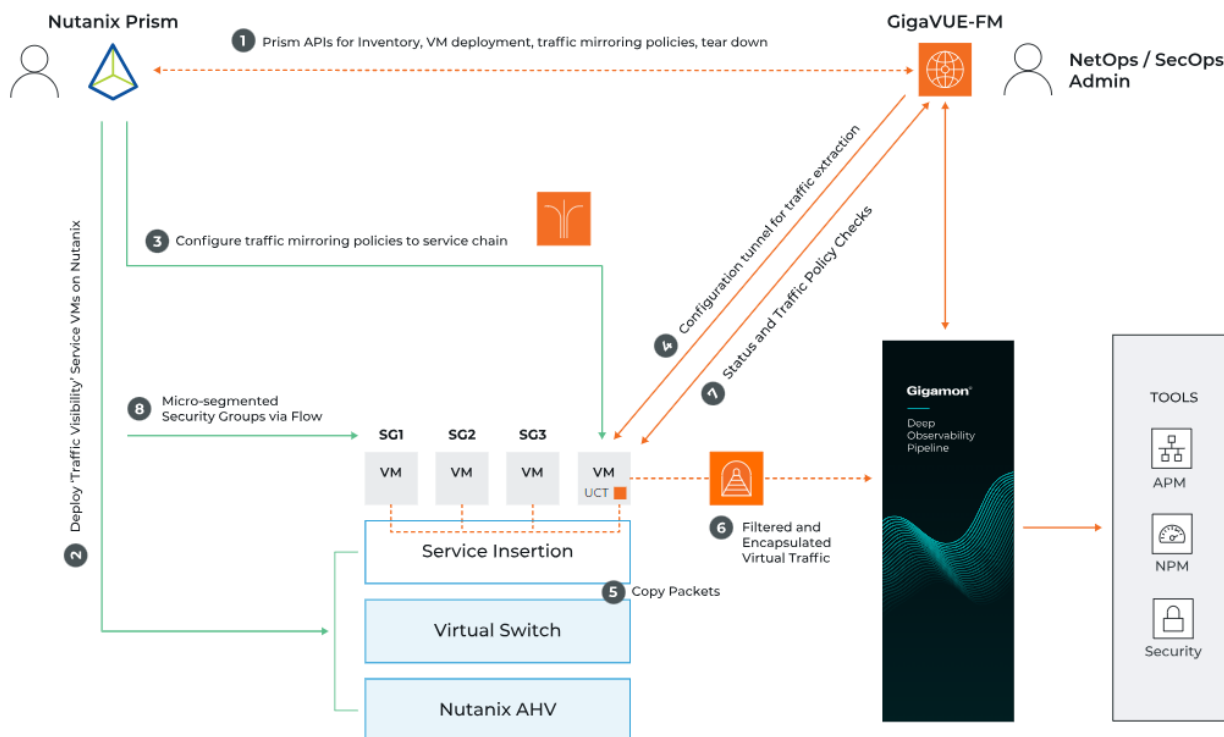
GigaVUE-FM integrates with the Nutanix Platform and deploys the components of the GigaVUE Cloud Suite for Nutanix in the underlay environment.

Once the GigaVUE Cloud Suite for Nutanix instance is launched in the Nutanix Prism central, the rest of the VM instances are automatically launched from GigaVUE-FM.

GigaVUE Cloud Suite for Nutanix provides the following benefits:

**Improves tool effectiveness:** Optimizes traffic processing and distribution with complete application visibility while reducing tool load.

**Simplifies operation:** Centralizes orchestration and management with a single-pane-of-glass fabric management and simplify tasks with full automation.



## Components of GigaVUE Cloud Suite for Nutanix

GigaVUE Cloud Suite for Nutanix includes the following components:



Component	Description
<b>GigaVUE® Fabric Manager (GigaVUE-FM)</b>	<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 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>
<b>GigaVUE® V Series Node</b>	<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>
<b>GigaVUE® V Series Proxy</b>	<p>GigaVUE V Series Proxy is an optional component. If GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network, a Proxy should be used. It can also be used if there is a large number of nodes connected to GigaVUE-FM or if you wish to keep IP addresses of the nodes private. It manages multiple GigaVUE V Series Nodes and orchestrates the flow of traffic from GigaVUE V Series Nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series Nodes. A single GigaVUE V Series Proxy can be launched to provide the GigaVUE-FM network communication to hundreds of GigaVUE V Series Nodes present in private networks behind the Proxy.</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](#)

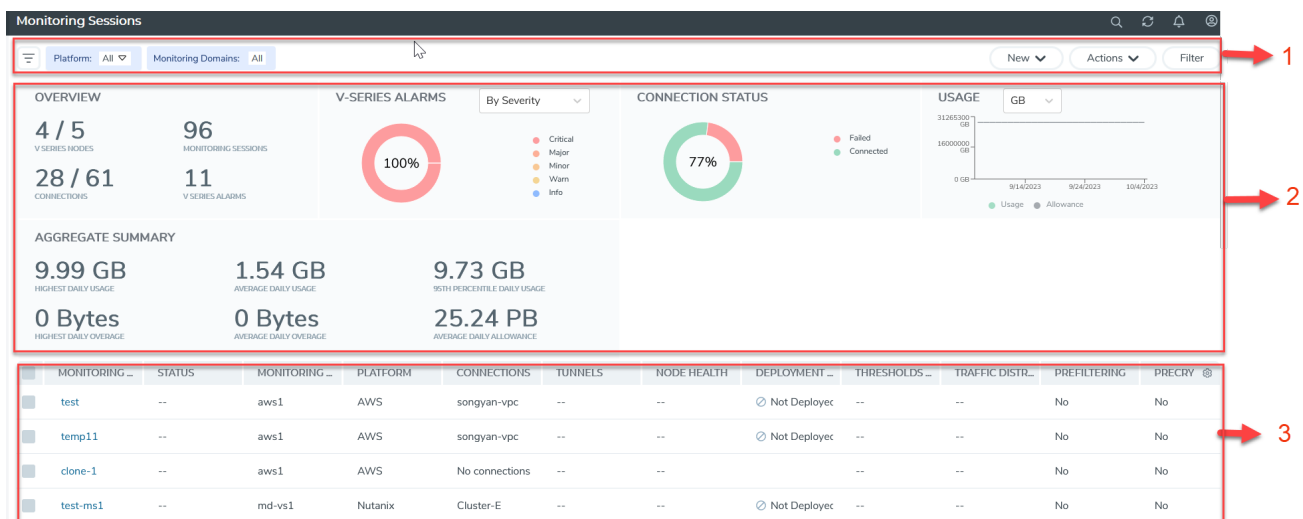
## Overall Cloud Overview Page

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 **MonitoringSessions** 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	<a href="#">Top Menu</a>
2	Charts	<a href="#">Viewing Charts</a>
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 <a href="#">Viewing Monitoring Session Details of all Cloud Platforms</a></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 <a href="#">Filters</a>
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 <b>Action</b> Drop down list box:</p> <ul style="list-style-type: none"> <li>■ <b>Edit</b> - Opens the Edit page for the selected monitoring session.</li> <li>■ <b>Delete</b> - Deletes the selected monitoring session.</li> <li>■ <b>Clone</b> - Duplicates the selected monitoring session.</li> <li>■ <b>Deploy</b> - Deploys the selected monitoring session.</li> <li>■ <b>Undeploy</b> - Un-deploys the selected monitoring session.</li> <li>■ <b>Apply Threshold</b> - Applies the threshold template created for monitoring cloud traffic health.</li> </ul> <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"> <li><b>View</b>- When you click this option, you can view a split window displaying the details of the monitoring sessions such as <b>Statistics, Connections, V Series Nodes, Source Health, Http2 Logging</b>. For more information, refer to <a href="#">Viewing Monitoring Session Details of Individual Cloud Platforms</a></li> <li><b>Edit</b> - When you click this option, you can view the <b>EditMonitoringSession</b> page.</li> </ul>
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 whether traffic distribution 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 <a href="#">View Monitoring Session Statistics</a> .
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.

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

## Points to Note (Nutanix)

1. When deploying GigaVUE fabric components using GigaVUE-FM, ensure you use underlay network.
2. Nutanix Prism Central and Nutanix Prism Element must have the same login credentials, for the GigaVUE V Series Node to be reachable.

## Prerequisites for GigaVUE Cloud Suite for Nutanix Deployment

The following are the prerequisites for configuring GigaVUE-FM, GigaVUE V Series Node, and GigaVUE V Series Proxy in Nutanix.

- The minimum requirement for deploying GigaVUE Cloud Suite for Nutanix is that the Nutanix admin account must be a **Prism Central Admin** on Prism Central and a **Cluster Admin** on individual clusters. The password must set to be the same across the environment if they are locally managed. Alternatively, if the Nutanix Prism Central is configured with external authentication like AD/LDAP then you can avoid replicating the manual password creation across the environment.
- You must upload the GigaVUE-FM, GigaVUE V Series Node, and GigaVUE V Series Proxy image files in the Prism Central repository. Do not use the Prism Element to upload the GigaVUE-FM image and fabric image files. Refer to [Upload Fabric Images](#) for more detailed information on how to upload the image to Prism Central.

- Assigning a static IP for GigaVUE V Series Node and GigaVUE V Series Proxy is not supported. DHCP must be enabled for the management subnet and tunnel subnet.
- Only one GigaVUE® V Series Node can be deployed per Nutanix Host.
- You must create a subnet in Nutanix Prism Central. For more information on creating a subnet, see [Configuring Network Connections](#).

Refer to the following topics for more detailed information:

- [Minimum Compute Requirements](#)
- [Network Firewall Requirements](#)
- [Default Login Credentials](#)

## Minimum Compute Requirements

The minimum recommended computing requirements are listed in the following table.

Compute Instances	vCPU	Memory	Disk Space	Description
GigaVUE-FM	2 vCPU	16GB	2 x 40GB	GigaVUE-FM must be able to access the GigaVUE V Series Nodes directly or a GigaVUE V Series Proxy that will relay the commands to the GigaVUE V Series Nodes.
GigaVUE V Series Node	4 vCPU	8GB	10GB	NIC 1: Monitored Network IP; Can be used as Tunnel IP NIC 2: Tunnel IP (optional) NIC 3: Management IP
GigaVUE V Series Proxy	1 vCPU	4GB	8GB	One GigaVUE V Series Proxy can be deployed per Cluster

## Network Firewall Requirements

Following are the Network Firewall Requirements for Gigamon fabrics for Nutanix deployments.

Direction	Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM</b>					
Inbound	HTTPS	TCP	443	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Inbound	SSH	TCP	22	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators

Direction	Type	Protocol	Port	CIDR	Purpose
					to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
Outbound	Custom TCP Rule	TCP	9440	Prism Central IP, Prism Element IP	Allows GigaVUE-FM to communicate with Prism Central and Prism Element.
<b>GigaVUE V Series Node</b>					
Inbound	Custom TCP Rule	TCP	9903	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Proxy to communicate with GigaVUE® V Series Nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound	Custom UDP Rule	<ul style="list-style-type: none"> <li>UDP (VXLAN)</li> <li>IP Protocol (L2GRE)</li> </ul>	<ul style="list-style-type: none"> <li>VXLAN (default 4789)</li> <li>L2GRE (IP 47)</li> </ul>	Tool IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound (optional)	Custom ICMP Rule	ICMP	<ul style="list-style-type: none"> <li>echo request</li> <li>echo reply</li> </ul>	Tool IP	Allows GigaVUE® V Series Node to health check the tunnel destination traffic.
<b>GigaVUE V Series Proxy (optional)</b>					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Node

## Default Login Credentials

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



Product	Login credentials
GigaVUE V Series Node	You can login to the GigaVUE V Series Node by using ssh. The default username and password is: Username: gigamon Password: Gigamon123!
GigaVUE V Series proxy	You can login to the GigaVUE V Series proxy by using ssh. The default username and password is: Username: gigamon Password: Gigamon123!

## License Information

GigaVUE Cloud Suite for Nutanix supports Volume Based License (VBL) model.

Refer to the following sections for details:

- [Volume Based License \(VBL\)](#)
- [Apply License](#)

### Volume Based License (VBL)

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 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 Gigamon 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 1 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 SKUs<sup>1</sup>. 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 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.
- 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:

---

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

GigaVUE Data Sheets
<a href="#">GigaVUE Cloud Suite for VMware Data Sheet</a>
<a href="#">GigaVUE Cloud Suite for AWS Data Sheet</a>
<a href="#">GigaVUE Cloud Suite for Azure Data Sheet</a>
<a href="#">GigaVUE Cloud Suite for OpenStack</a>
<a href="#">GigaVUE Cloud Suite for Nutanix</a>
<a href="#">GigaVUE Cloud Suite for Kubernetes</a>

## 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 and Activate 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
<b>Activate Licenses</b>	Use this button to activate a Volume-based License. Refer to <a href="#">Activate Volume-based Licenses</a> for more information.
<b>Email Volume Usage</b>	Use this button to send the volume usage details to the email recipients.
<b>Filter</b>	Use this button to narrow down the list of active Volume-based Licenses that are displayed on the VBL active page.
<b>Export</b>	Use this button to export the details in the VBL active page to a CSV or XLSX file.
<b>Deactivate</b>	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	<a href="#">Generate VBL Usage Reports</a>	GigaVUE Administration Guide
Volume-based Licensed report details	<a href="#">Volume Based License Usage Report</a>	GigaVUE Administration Guide
Fabric health analytics dashboards for Volume-based Licenses usage	<a href="#">Dashboards for Volume Based Licenses Usage</a>	GigaVUE-FM User Guide

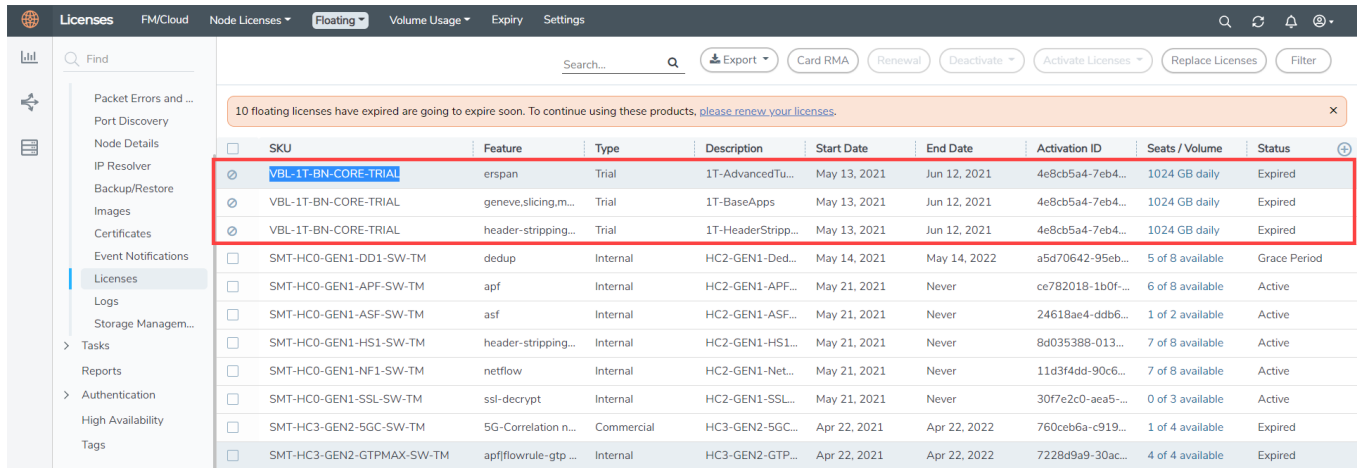
## Activate Volume-based Licenses

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	760ceb5a-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.

## Apply License

For instructions on how to generate and apply license refer to the *GigaVUE Licensing Guide*.

# Install and Upgrade GigaVUE-FM

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

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 Cloud Suite® Fabric Manager (GigaVUE-FM) on cloud platforms or on-premises.

- o Installation: Refer to GigaVUE-FM Installation and Upgrade Guide available in the [Gigamon Documentation Library](#). If you wish to install GigaVUE-FM in Nutanix Prism Central Platform, you must upload the recent GigaVUE-FM image file to the Prism Central. For the GigaVUE-FM installation procedures, refer to [Install GigaVUE-FM on Nutanix](#).
- o Upgrade: Refer to Upgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

## Upload Fabric Images

Before deploying GigaVUE-FM, you must upload the fabric image to Prism Central. To upload the fabric components images to the Prism Central, follow the steps given below:

1. Log in to the [Gigamon Customer Portal](#) and click on Software and Release Notes.
2. Search for **qcow2** in the Search option. Click **GO**.
3. Use the filter option in the respective search results column to filter your search by Product, Release, Release Type and Release date. Select GigaVUE-FM as the product, and the select the release version in the Release field.
4. The QCOW2 file appears in the list view. Click on the latest QCOW2 file to download it.
5. Download the images for GigaVUE-FM, GigaVUE V Series Node and GigaVUE V Series Proxy.
6. Log in to Prism Central.

7. In Prism Central, select **Dashboard > Compute & Storage > Images**. The **Images** page appears.
8. In the **Images** page, click **Add Image**. The **Add Image** page appears.
9. Select the **Image File** option for Image Source.
10. Click **Add File** and upload the previously downloaded QCOW2 file. Click **Next**.
11. Select **Place image directly on cluster** option for the Place Method and click **Save**.

The images are uploaded to Prism Central. You can view the uploaded images under **Compute & Storage > Images**.

# Deploy GigaVUE Cloud Suite for Nutanix

This section describes how to connect, launch, and deploy fabric components of GigaVUE Cloud Suite for Nutanix.

Refer to the following sections for details:

- [Install Custom Certificate](#)
- [Create a Monitoring Domain](#)
- [Configure GigaVUE Fabric Components in GigaVUE-FM](#)

## Install Custom Certificate

GigaVUE V Series Node and GigaVUE V Series Proxy 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 or GigaVUE V Series Proxy run through the security scanners.

## 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 and GigaVUE V Series Proxy 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.

## Adding Certificate Authority

This section describes how to add Certificate Authority in GigaVUE-FM.

### CA List

The Certificate Authority (CA) List page allows you to add the root CA for the devices.

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

1. Go to **Inventory > Resources > Security > CA List**.
2. Click **Add**, to add a new Custom Authority. The **Add Certificate Authority** page appears.
3. Enter or select the following information.

Field	Action
Alias	Alias name of the CA.
File Upload	Choose the certificate from the desired location.

4. Click **Save**.

## Create a Monitoring Domain

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

GigaVUE-FM provides you the flexibility to connect to multiple clusters.

**NOTE:** To configure the monitoring domain and launch the fabric components in Nutanix Prism, you must be a user with **Admin** role or a user with write access to the **Cluster Management** category.

To create a Monitoring Domain:

1. Go to **Inventory > VIRTUAL > Nutanix** and then click **Monitoring Domain**. The Monitoring Domain page appears.
2. On the Monitoring Domain page, click the **New** button. The Monitoring Domain Configuration page appears.
3. Enter or select the appropriate information as shown in the following table.

Field	Action
<b>Monitoring Domain</b>	Enter a monitoring domain name.
<b>Connection Alias</b>	An alias used to identify the monitoring domain.
<b>Use Legacy V Series Mode</b>	By default, V Series 2 is enabled. Enable this option, if you want to use the legacy V Series Mode
<b>Nutanix Prism Central IP</b>	Enter the Nutanix Prism Central IP address.
<b>Nutanix Prism Central Username</b>	Enter the Prism Central username. <b>NOTE:</b> Ensure Prism Element is accessible using the same login credentials.
<b>Nutanix Prism Central Password</b>	Enter the Prism Central password. <b>NOTE:</b> Ensure Prism Element is accessible using the same login credentials.
<b>Clusters</b>	Select the cluster where the GigaVUE V Series Proxy and GigaVUE® V Series Node are to be deployed.
<b>Traffic Acquisition tunnel MTU</b>	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the tunnel to the GigaVUE V Series node. The default value is 1500.

4. Click **Save**. The Monitoring Domain is created and the **Nutanix Fabric Launch Configuration** page appears. Refer to [Configure GigaVUE Fabric Components in GigaVUE-FM](#) for more detailed information on how to deploy GigaVUE V Series Node and GigaVUE V Series Proxy using GigaVUE-FM.

## Configure GigaVUE Fabric Components in GigaVUE-FM

This chapter describes how to deploy GigaVUE V Series Nodes and GigaVUE V Series Proxy in Prism environment through GigaVUE-FM.

### Nutanix Fabric Launch Configuration

GigaVUE V Series Proxy and GigaVUE V Series Node are launched by GigaVUE-FM based on the configuration made in Nutanix Fabric Launch Configuration page.

To configure the fabric components in GigaVUE-FM, do the following:

1. After [Nutanix Configuration](#) in GigaVUE-FM, you are navigated to **Nutanix Fabric Launch Configuration** page.

## 2. On the Nutanix Fabric Launch Configuration page, enter or select the following information.

Field	Description						
<b>Cluster</b>	Select the cluster where the GigaVUE V Series Proxy and GigaVUE® V Series Node are to be deployed. The clusters that were selected during Monitoring Domain creation will be available here for selection. Refer to <a href="#">Create a Monitoring Domain</a> for more detailed information on how to create a monitoring domain.						
<b>Enable Custom Certificates</b>	<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 an handshake error occurs.</p> <p><b>NOTE:</b> If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.</p>						
<b>Custom SSL Certificate</b> <p><b>NOTE:</b> This option appears only when <b>Enable Custom Certificates</b> option is enabled.</p>	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Node and GigaVUE V Series Proxy. For more detailed information, refer to <a href="#">Install Custom Certificate</a> .						
<b>Configure a V Series Proxy (Optional)</b>	Select this option to configure GigaVUE V Series Proxy.						
	<table border="1"> <tr> <td><b>Version</b></td> <td>Select a GigaVUE® V Series Node image file. Refer to <a href="#">Upload Fabric Images</a> for more information on how to upload image files to Nutanix Prism Central.</td> </tr> <tr> <td><b>Management Subnet</b></td> <td>The subnets registered in Prism Central are listed. Select a Management Subnet from the drop-down menu.</td> </tr> <tr> <td><b>Cloud-Init User Data (optional)</b></td> <td>           Enter cloud-init user data (YAML, JSON, or Shell script). You can use this field to carry out a set of predefined tasks. For example:           <ul style="list-style-type: none"> <li>• Ensure a specific set of packages is installed.</li> <li>• Install Specific SSH key pairs.</li> <li>• Create User accounts.</li> <li>• Assign Static IP address.</li> </ul> </td> </tr> </table>	<b>Version</b>	Select a GigaVUE® V Series Node image file. Refer to <a href="#">Upload Fabric Images</a> for more information on how to upload image files to Nutanix Prism Central.	<b>Management Subnet</b>	The subnets registered in Prism Central are listed. Select a Management Subnet from the drop-down menu.	<b>Cloud-Init User Data (optional)</b>	Enter cloud-init user data (YAML, JSON, or Shell script). You can use this field to carry out a set of predefined tasks. For example: <ul style="list-style-type: none"> <li>• Ensure a specific set of packages is installed.</li> <li>• Install Specific SSH key pairs.</li> <li>• Create User accounts.</li> <li>• Assign Static IP address.</li> </ul>
	<b>Version</b>	Select a GigaVUE® V Series Node image file. Refer to <a href="#">Upload Fabric Images</a> for more information on how to upload image files to Nutanix Prism Central.					
	<b>Management Subnet</b>	The subnets registered in Prism Central are listed. Select a Management Subnet from the drop-down menu.					
<b>Cloud-Init User Data (optional)</b>	Enter cloud-init user data (YAML, JSON, or Shell script). You can use this field to carry out a set of predefined tasks. For example: <ul style="list-style-type: none"> <li>• Ensure a specific set of packages is installed.</li> <li>• Install Specific SSH key pairs.</li> <li>• Create User accounts.</li> <li>• Assign Static IP address.</li> </ul>						

Field	Description	
GigaVUE® V Series Node	Host	Select a host or multiple hosts from the selected Cluster.
	Version	Select a GigaVUE® V Series Node image file. Refer to <a href="#">Upload Fabric Images</a> for more information.
	Management Subnet	The subnets registered in Prism Central are listed. Select a Management Subnet from the drop-down menu.
	Data Subnet	Select the subnet(s) based on the required VMs and vNICs. Click <b>Add Subnet</b> to add additional Subnets.
	Memory Size (GB)	Enter the memory size of the vCPUs.
	Disk Size (GB)	Enter the image size of the GigaVUE V Series Nodes
	Number of vCPUs	Enter the number of vCPUs required.
	SSL Keys (optional)	If you wish to configure secure tunnels between two GigaVUE V Series Node, select the uploaded SSL Key from the drop-down menu. Refer to <a href="#">Configure Secure Tunnel</a> for more detailed information on how to upload SSL keys and configure Secure tunnels.
Cloud-Init User Data (optional)	Enter cloud-init user data (YAML, JSON, or Shell script). You can use this field to carry out a set of predefined tasks. For example: <ul style="list-style-type: none"> <li>• Ensure a specific set of packages is installed.</li> <li>• Install Specific SSH key pairs.</li> <li>• Create User accounts.</li> </ul>	

**NOTE:** Assigning a Static IP for GigaVUE V Series Nodes is not supported. DHCP must be enabled for the management subnet and tunnel subnet.

3. Click **Save & Configure Next Cluster** to configure next Cluster, or Click **Save & Exit** to initiate the deployment of the selected GigaVUE V Series Node. You can view the status of the deployment on the Tasks page of Prism Central.

To view the fabric launch configuration specification of a fabric component, click on a V Series node, and a quick view of the Fabric Launch Configuration appears on the Monitoring Domain page.

## Secure Tunnels

Secure Tunnel can transfer the cloud captured packets from a GigaVUE V Series Node to another GigaVUE V Series Node.

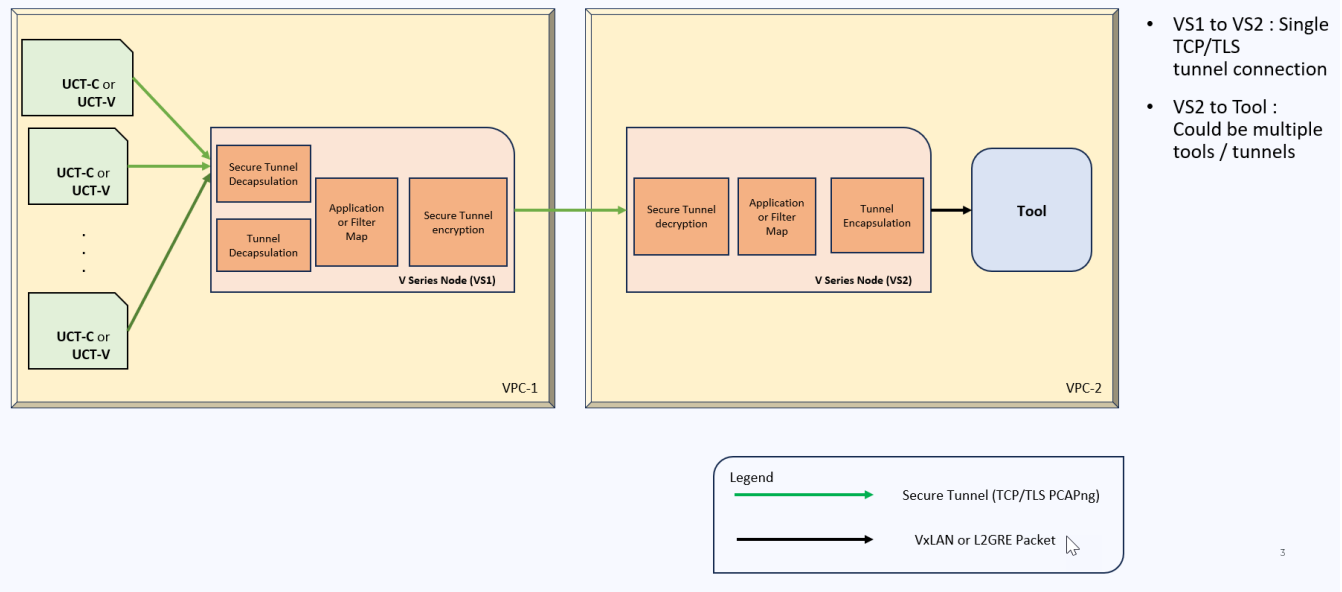
In case of GigaVUE V Series Node to GigaVUE V Series node, the traffic from the GigaVUE V Series Node 1 is encapped using PCAPng format and transported to GigaVUE V Series Node 2 where the traffic is decapped. The secure tunnels between V Series Node to V Series Node have multiple uses cases.

The GigaVUE V Series Node decapsulates and processes the packet per the configuration. The decapsulated packet can be sent to the application such as De-duplication, Application Intelligence, Load balancer and to the tool. The Load Balancer on this node can send the packets to multiple V Series Nodes, in this case the packets can be encapsulated again and sent over a secure tunnel.

For more information about PCAPng, refer to [PCAPng Application](#).

## Secure Tunnel Use Case

Tool in remote Virtual Private Cloud (VPC) – Single V Series Node



## Supported Platforms

Secure tunnel is supported on:

- OpenStack
- Azure
- AWS
- VMware NSX-T (only for Third Party Orchestration)
- VMware ESXi (only for Third Party Orchestration)
- Nutanix (only for Third Party Orchestration)
- Google Cloud Platform (only for Third Party Orchestration)

For information about how to configure secure tunnels, refer to the section [Configure Secure Tunnel](#).

## Configure Secure Tunnel

This section provides step-by-step instructions on how to configure secure tunnels for GigaVUE Cloud Suite for Nutanix.

### Prerequisites

While creating Secure Tunnel, you must provide the following details:

- SSH key pair
- CA certificate

### Notes

- Protocol version IPv4 and IPv6 are supported.
- If you wish to use IPv6 tunnels, your GigaVUE-FM and the fabric components version must be 6.6.00 or above. For UCT-V agents with version lower than 6.6.00, if secure tunnel is enabled in the monitoring session, secure mirror traffic will be transmitted over IPv4, regardless of IPv6 preference.

## Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2

You can create secure tunnel in the following ways:

- Between GigaVUE V Series Node 1 to GigaVUE V Series Node 2
- From GigaVUE V Series Node 1 to multiple GigaVUE V Series nodes.

You must have the following details before you start the configuration of secure tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2:

- IP address of the tunnel destination endpoint (GigaVUE V Series Node 2).
- SSH key pair (pem file).

To configure secure tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2, refer to the following steps:



S · N o	Task	Refer to						
1.	Upload a Certificate Authority (CA) Certificate	<p>You must upload a Custom Certificate to UCT-V Controller for establishing a connection between the GigaVUE V Series Node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> <li>Go to <b>Inventory &gt; Resources &gt; Security &gt; CA List</b>.</li> <li>Click <b>Add</b>, to add a new Certificate Authority. The <b>Add Certificate Authority</b> page appears.</li> <li>Enter or select the following information. <table border="1" data-bbox="381 617 1471 781"> <thead> <tr> <th data-bbox="381 617 620 695">Field</th> <th data-bbox="620 617 1471 695">Action</th> </tr> </thead> <tbody> <tr> <td data-bbox="381 695 620 737">Alias</td> <td data-bbox="620 695 1471 737">Alias name of the CA.</td> </tr> <tr> <td data-bbox="381 737 620 781">File Upload</td> <td data-bbox="620 737 1471 781">Choose the certificate from the desired location.</td> </tr> </tbody> </table> </li> <li>Click <b>Save</b>.</li> <li>Click <b>Deploy All</b>.</li> </ol> <p>For more information, refer to the section <a href="#">Adding Certificate Authority</a></p>	Field	Action	Alias	Alias name of the CA.	File Upload	Choose the certificate from the desired location.
Field	Action							
Alias	Alias name of the CA.							
File Upload	Choose the certificate from the desired location.							
2.	Upload a SSL Key	<p>You must add a SSL key to GigaVUE V Series node. To add SSL Key, follow the steps in the section <a href="#">Upload SSL Keys</a>.</p>						
3	Create a secure tunnel between UCT-V and GigaVUE V Series Node 1.	<p>You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE V Series node 1. To enable the secure tunnel feature follow these steps:</p> <ol style="list-style-type: none"> <li>In the Edit Monitoring Session page, click <b>Options</b>. The <b>Apply template</b> page appears.</li> <li>Enable the <b>Secure Tunnel</b> button. You can enable secure tunnel for both mirrored and preencrypted traffic.</li> </ol>						
4.	Select the added SSL Key while creating a monitoring domain.	<p>Select the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in GigaVUE V Series Node 1.</p> <p>You must select the added SSL Key in GigaVUE V Series Node 1.</p> <p>To select the SSL key, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a></p>						

S · N o	Task	Refer to						
5.	Select the added CA certificate while creating the monitoring domain	You should select the added Certificate Authority (CA) in UCT-V Controller. To select the CA certificate, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a>						
6	Create an Egress tunnel from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session.	<p>You must create a tunnel for traffic to flow out from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to <a href="#">Create Ingress and Egress Tunnel</a> for more detailed information on how to create tunnels.</p> <p>To create the egress tunnel, follow these steps:</p> <ol style="list-style-type: none"> <li>1. After creating a new monitoring session, or click <b>Actions &gt; Edit</b> on an existing monitoring session, the GigaVUE-FM canvas appears.</li> <li>2. In the canvas, select <b>New &gt; New Tunnel</b>, drag and drop a new tunnel template to the workspace. The <b>Add Tunnel Spec</b> quick view appears.</li> <li>3. On the New Tunnel quick view, enter or select the required information as described in the following table:</li> </ol> <table border="1" data-bbox="302 1062 1471 1230"> <thead> <tr> <th data-bbox="302 1062 472 1136">Field</th> <th data-bbox="472 1062 1471 1136">Action</th> </tr> </thead> <tbody> <tr> <td data-bbox="302 1136 472 1182">Alias</td> <td data-bbox="472 1136 1471 1182">The name of the tunnel endpoint.</td> </tr> <tr> <td data-bbox="302 1182 472 1230">Description</td> <td data-bbox="472 1182 1471 1230">The description of the tunnel endpoint.</td> </tr> </tbody> </table>	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.
Field	Action							
Alias	The name of the tunnel endpoint.							
Description	The description of the tunnel endpoint.							

S · N o	Task	Refer to								
		<table border="1"> <thead> <tr> <th data-bbox="305 340 472 415">Field</th> <th data-bbox="472 340 1474 415">Action</th> </tr> </thead> <tbody> <tr> <td data-bbox="305 415 472 464">Type</td> <td data-bbox="472 415 1474 464">Select TLS-PCAPNG for creating egress secure tunnel</td> </tr> <tr> <td data-bbox="305 464 472 1220">Traffic Direction</td> <td data-bbox="472 464 1474 1220">           Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:           <ul style="list-style-type: none"> <li>o MTU- The default value is 1500 for Azure.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p><b>NOTE:</b> Increasing the MTU value will impact the performance and may even result in packet loss. By default, Azure VNet will attempt to fragment jumbo frames even if sending and receiving VMs are configured with a higher MTU.</p> </div> <ul style="list-style-type: none"> <li>o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64.</li> <li>o DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li> <li>o Flow Label - Enter the Flow Label value.</li> <li>o Source L4 Port- Enter the Souce L4 Port value</li> <li>o Destination L4 Port - Enter the Destination L4 Port value.</li> <li>o Flow Label</li> <li>o Cipher- Only SHA 256 is supported.</li> <li>o TLS Version - Select TLS Version1.3.</li> <li>o Selective Acknowledgments - Choose <b>Enable</b> to turn on the TCP selective acknowledgments.</li> <li>o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.</li> <li>o Delay Acknowledgments - Choose <b>Enable</b> to turn on delayed acknowledgments.</li> </ul> </td> </tr> <tr> <td data-bbox="305 1220 472 1295">Remote Tunnel IP</td> <td data-bbox="472 1220 1474 1295">Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).</td> </tr> </tbody> </table> <p data-bbox="305 1312 472 1346">4. Click <b>Save</b>.</p>	Field	Action	Type	Select TLS-PCAPNG for creating egress secure tunnel	Traffic Direction	Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: <ul style="list-style-type: none"> <li>o MTU- The default value is 1500 for Azure.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p><b>NOTE:</b> Increasing the MTU value will impact the performance and may even result in packet loss. By default, Azure VNet will attempt to fragment jumbo frames even if sending and receiving VMs are configured with a higher MTU.</p> </div> <ul style="list-style-type: none"> <li>o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64.</li> <li>o DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li> <li>o Flow Label - Enter the Flow Label value.</li> <li>o Source L4 Port- Enter the Souce L4 Port value</li> <li>o Destination L4 Port - Enter the Destination L4 Port value.</li> <li>o Flow Label</li> <li>o Cipher- Only SHA 256 is supported.</li> <li>o TLS Version - Select TLS Version1.3.</li> <li>o Selective Acknowledgments - Choose <b>Enable</b> to turn on the TCP selective acknowledgments.</li> <li>o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.</li> <li>o Delay Acknowledgments - Choose <b>Enable</b> to turn on delayed acknowledgments.</li> </ul>	Remote Tunnel IP	Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).
Field	Action									
Type	Select TLS-PCAPNG for creating egress secure tunnel									
Traffic Direction	Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: <ul style="list-style-type: none"> <li>o MTU- The default value is 1500 for Azure.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p><b>NOTE:</b> Increasing the MTU value will impact the performance and may even result in packet loss. By default, Azure VNet will attempt to fragment jumbo frames even if sending and receiving VMs are configured with a higher MTU.</p> </div> <ul style="list-style-type: none"> <li>o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64.</li> <li>o DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li> <li>o Flow Label - Enter the Flow Label value.</li> <li>o Source L4 Port- Enter the Souce L4 Port value</li> <li>o Destination L4 Port - Enter the Destination L4 Port value.</li> <li>o Flow Label</li> <li>o Cipher- Only SHA 256 is supported.</li> <li>o TLS Version - Select TLS Version1.3.</li> <li>o Selective Acknowledgments - Choose <b>Enable</b> to turn on the TCP selective acknowledgments.</li> <li>o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.</li> <li>o Delay Acknowledgments - Choose <b>Enable</b> to turn on delayed acknowledgments.</li> </ul>									
Remote Tunnel IP	Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).									
7.	Select the added SSL Key while creating a monitoring domain and configuring the	You must select the added SSL Key in GigaVUE V Series Node 2. To select the SSL key, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a>								

S · N o	Task	Refer to														
	fabric components in GigaVUE-FM in GigaVUE V Series Node 2															
8	Create an ingress tunnel in the GigaVUE V Series Node 2 with tunnel type as TLS-PCAPNG while creating the monitoring session for GigaVUE Node 2.	<p>You must create an ingress tunnel for traffic to flow in from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session.</p> <p>To create the ingress tunnel, follow these steps:</p> <ol style="list-style-type: none"> <li>1. After creating a new monitoring session, or click <b>Actions</b> &gt; <b>Edit</b> on an existing monitoring session, the GigaVUE-FM canvas appears.</li> <li>2. In the canvas, select <b>New</b> &gt; <b>New Tunnel</b>, drag and drop a new tunnel template to the workspace. The <b>Add Tunnel Spec</b> quick view appears.</li> <li>3. On the New Tunnel quick view, enter or select the required information as described in the following table:</li> </ol> <table border="1" data-bbox="302 1005 1468 1541"> <thead> <tr> <th data-bbox="302 1005 493 1083">Field</th> <th data-bbox="493 1005 1468 1083">Action</th> </tr> </thead> <tbody> <tr> <td data-bbox="302 1083 493 1125">Alias</td> <td data-bbox="493 1083 1468 1125">The name of the tunnel endpoint.</td> </tr> <tr> <td data-bbox="302 1125 493 1167">Description</td> <td data-bbox="493 1125 1468 1167">The description of the tunnel endpoint.</td> </tr> <tr> <td data-bbox="302 1167 493 1346">Type</td> <td data-bbox="493 1167 1468 1346">           Select TLS-PCAPNG for creating egress secure tunnel.           <div data-bbox="509 1220 1455 1339" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.</p> </div> </td> </tr> <tr> <td data-bbox="302 1346 493 1419">Traffic Direction</td> <td data-bbox="493 1346 1468 1419">Choose <b>In</b> (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6.</td> </tr> <tr> <td data-bbox="302 1419 493 1461">IP Version</td> <td data-bbox="493 1419 1468 1461">The version of the Internet Protocol. IPv4 and IPv6 are supported.</td> </tr> <tr> <td data-bbox="302 1461 493 1541">Remote Tunnel IP</td> <td data-bbox="493 1461 1468 1541">Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 1 (Destination IP).</td> </tr> </tbody> </table> <ol style="list-style-type: none"> <li>4. Click <b>Save</b>.</li> </ol>	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.	Type	Select TLS-PCAPNG for creating egress secure tunnel. <div data-bbox="509 1220 1455 1339" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.</p> </div>	Traffic Direction	Choose <b>In</b> (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6.	IP Version	The version of the Internet Protocol. IPv4 and IPv6 are supported.	Remote Tunnel IP	Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 1 (Destination IP).
Field	Action															
Alias	The name of the tunnel endpoint.															
Description	The description of the tunnel endpoint.															
Type	Select TLS-PCAPNG for creating egress secure tunnel. <div data-bbox="509 1220 1455 1339" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.</p> </div>															
Traffic Direction	Choose <b>In</b> (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6.															
IP Version	The version of the Internet Protocol. IPv4 and IPv6 are supported.															
Remote Tunnel IP	Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 1 (Destination IP).															

# Configure Monitoring Session

GigaVUE-FM collects inventory data on all V Series nodes deployed in your environment through Nutanix Prism Central. You can design your monitoring session to include or exclude the target VMs that you want to monitor. 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.

To design your monitoring session, refer to the following sections:

- [Create a Monitoring Session](#)
- [Interface Mapping](#)
- [Create Ingress and Egress Tunnel](#)
- [Create a New Map](#)
- [Add Applications to Monitoring Session](#)
- [To deploy the monitoring session:](#)
- [View Monitoring Session Statistics](#)
- [Visualize the Network Topology](#)

## Create a Monitoring Session

A monitoring session defines how traffic should be processed and send to the tunnel endpoints.

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.

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

You can create multiple monitoring sessions per monitoring domain.

To create a new monitoring session:

1. Go to **Traffic > Virtual > Orchestrated Flows > Nutanix**. The **Monitoring Session** page appears.
2. Click **New** to open the **New Monitoring Session** page.

New Monitoring Session Cancel Next

A monitoring session defines how traffic should be processed and sent to the tunnel endpoints. You can specify prefiltering and precryption on UCT-Vs or traffic thresholds by applying the pre-defined templates to your monitoring session.

Alias

Monitoring Domain

Connections

Traffic Distribute

ⓘ Traffic distribute is only supported on V Series version 6.5.00 and later.

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

Field	Description
<b>Alias</b>	The name of the monitoring session.
<b>Monitoring Domain</b>	The name of the monitoring domain that you want to select.
<b>Connection</b>	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.
<b>Traffic Distribute</b>	Enabling the "Traffic Distribute" option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring.

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

The Monitoring Session page **Actions** button also has the following options:

Button	Description
<b>Edit</b>	Opens the Edit page for the selected monitoring session. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"><b>NOTE:</b> In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.</div>
<b>Delete</b>	Deletes the selected monitoring session.
<b>Clone</b>	Duplicates the selected monitoring session.

Button	Description
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 <a href="#">Monitor Cloud Health</a> 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, and maps.

Refer to the following topics for detailed information:

- [Create Ingress and Egress Tunnels](#)
- [Add Applications to Monitoring Session](#)
- [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 <b>Instances</b> dialog box.
Interface mapping	Use to change the interfaces mapped to an individual GigaVUE V Series Node. Refer to <a href="#">Interface Mapping</a> 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 monitoring session.
Ok / Cancel	<p><b>Ok:</b> Use to save the configurations in the monitoring session when the monitoring session is in undeployed state.</p> <p><b>Cancel:</b> 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 <a href="#">To deploy the monitoring session:</a> topic for more details.

## Monitoring Session Options

User-defined applications and Thresholds can be enabled for the monitoring session from the **Options** page.

To navigate to **Options** page, follow the steps given below:

1. Go to **Traffic > Virtual > Orchestrated Flows > Nutanix**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. In the Edit Monitoring Session page, click **Options**. The **Options** page appears.

You can perform the following actions in the Options page:

- [Enable User Defined Applications](#)
- [Create Threshold](#)

### Enable User Defined Applications

To enable user defined application, follow the steps given below:

1. In the **Monitoring Session Options** page, Click **User-Defined Apps** tab.
2. Enable the **User-defined Applications** toggle button. Refer to [User Defined Application](#) for more detailed information User Defined Applications and how to configure it.

### Create Threshold

To create threshold, follow the steps given below:

1. In the **Monitoring Session Options** page, Click **Threshold** tab.
2. Refer to [Traffic Health Monitoring](#) topic for more detailed information on how to create threshold template and apply the templates to the monitoring session.

## 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:

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

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, or ERSPAN tunnel.

To create a new tunnel endpoint:

1. After creating a new monitoring session, or click **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.

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

Field	Description	
<b>Alias</b>	The name of the tunnel endpoint.  <b>NOTE:</b> Do not enter spaces in the alias name.	
<b>Description</b>	The description of the tunnel endpoint.	
<b>Type</b>	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN, or UDPGRE to create a tunnel.	
<b>VXLAN</b>		
<b>Traffic Direction</b> The direction of the traffic flowing through the GigaVUE V Series Node.		
<b>In</b>	Choose <b>In</b> (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	<b>IP Version</b>	The version of the Internet Protocol. Select IPv4 or IPv6.
	<b>Remote Tunnel IP</b>	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	<b>VXLAN Network Identifier</b>	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	<b>Source L4 Port</b>	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.
	<b>Destination L4 Port</b>	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.
<b>Out</b>	Choose <b>Out</b> (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	<b>Remote Tunnel IP</b>	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	<b>MTU</b>	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	<b>Time to Live</b>	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.
	<b>DSCP</b>	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.

Field	Description	
	<b>Flow Label</b>	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
	<b>VXLAN Network Identifier</b>	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	<b>Source L4 Port</b>	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.
	<b>Destination L4 Port</b>	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.
<b>L2GRE</b>		
<b>Traffic Direction</b>		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose <b>In</b> (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	<b>IP Version</b>	The version of the Internet Protocol. Select IPv4 or IPv6.
	<b>Remote Tunnel IP</b>	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	<b>Key</b>	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 <b>Out</b> (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	<b>Remote Tunnel IP</b>	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	<b>MTU</b>	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	<b>Time to Live</b>	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.
	<b>DSCP</b>	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.
	<b>Flow Label</b>	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

Field	Description	
		and 1048575.
	<b>Key</b>	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.
<b>ERSPAN</b>		
<b>Traffic Direction</b> The direction of the traffic flowing through the GigaVUE V Series Node.		
In	<b>IP Version</b>	The version of the Internet Protocol. Select IPv4 or IPv6.
	<b>Remote Tunnel IP</b>	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	<b>Flow ID</b>	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
<b>TLS-PCAPNG</b>		
<b>Traffic Direction</b> The direction of the traffic flowing through the GigaVUE V Series Node.		

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.
	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.

4. Click **Save**.

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

## Create a New Map

You must have the flow map license to deploy a map in the 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:

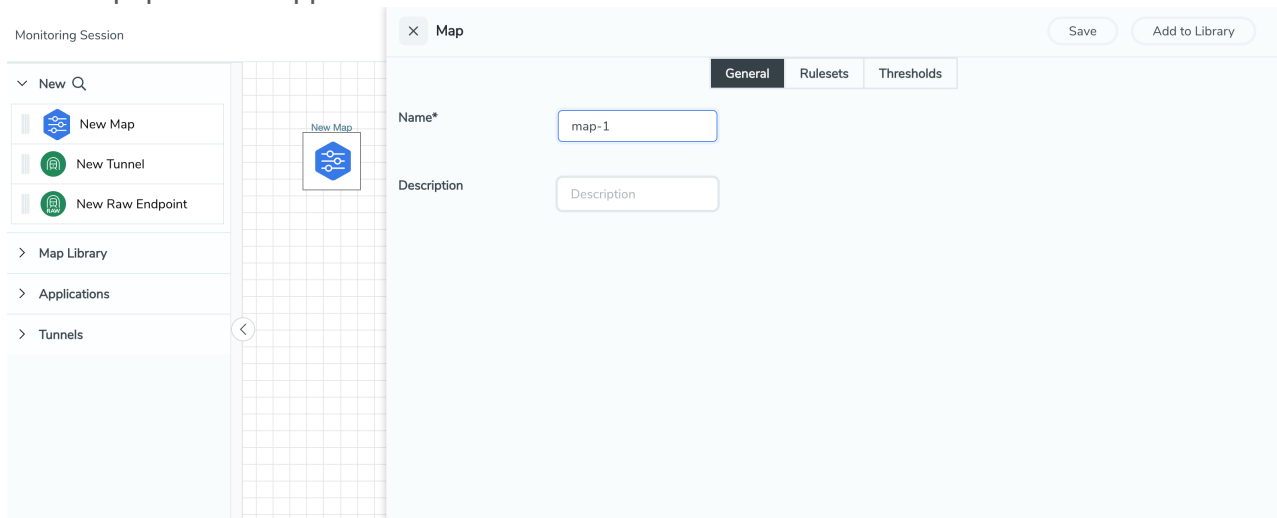
Parameter	Description
<b>Rules</b>	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and the (egress or ingress) direction of tapping the network traffic.
<b>Priority</b>	Priority determines the order in which the rules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

<b>Exclusion Map</b>	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
<b>Automatic Target Selection (ATS)</b>	<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><b>Selected Targets = Traffic Filter Maps <math>\cap</math> Inclusion Maps - Exclusion Maps</b></p> <p>Below are the filter rule types that work in ATS:</p> <ul style="list-style-type: none"> <li>• mac Source</li> <li>• mac Destination</li> <li>• ipv4 Source</li> <li>• ipv4 Destination</li> <li>• ipv6 Source</li> <li>• ipv6 Destination</li> <li>• VM Name Destination</li> <li>• VM Name Source</li> <li>• VM Tag Destination - Not applicable to Nutanix.</li> <li>• VM Tag Source - Not applicable to Nutanix.</li> <li>• VM Category Source - Applicable only to Nutanix</li> <li>• VM Category Destination - Applicable only to Nutanix.</li> <li>• Host Name -Applicable only to Nutanix and VMware.</li> </ul> <p>The traffic direction is as follow:</p> <ul style="list-style-type: none"> <li>• For any rule type as Source - the traffic direction is egress.</li> <li>• For Destination rule type - the traffic direction is ingress.</li> <li>• For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> 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 V Series Node does not receive traffic from any VM or vNIC.</p> </div>
<b>Group</b>	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.



3. On the New Map quick view, click on **General** tab and enter the required information as described in the following table:

Field	Description
<b>Name</b>	Name of the new map
<b>Description</b>	Description of the map

- 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](#).

#### Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.

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.

## 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
- NetFlow
- Slicing
- Masking
- De-duplication
- Load Balancing
- Header Stripping
- SSL Decrypt

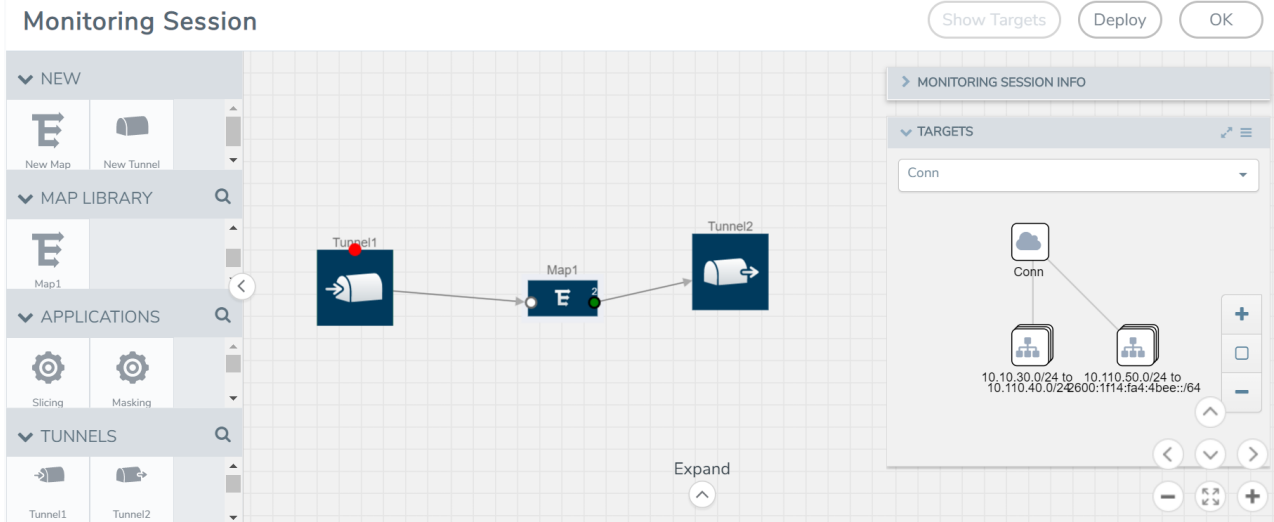
For more detailed information on how to configure these application, refer to *GigaVUE V Series Applications Guide*.

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

- 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.



- 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.
- 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.

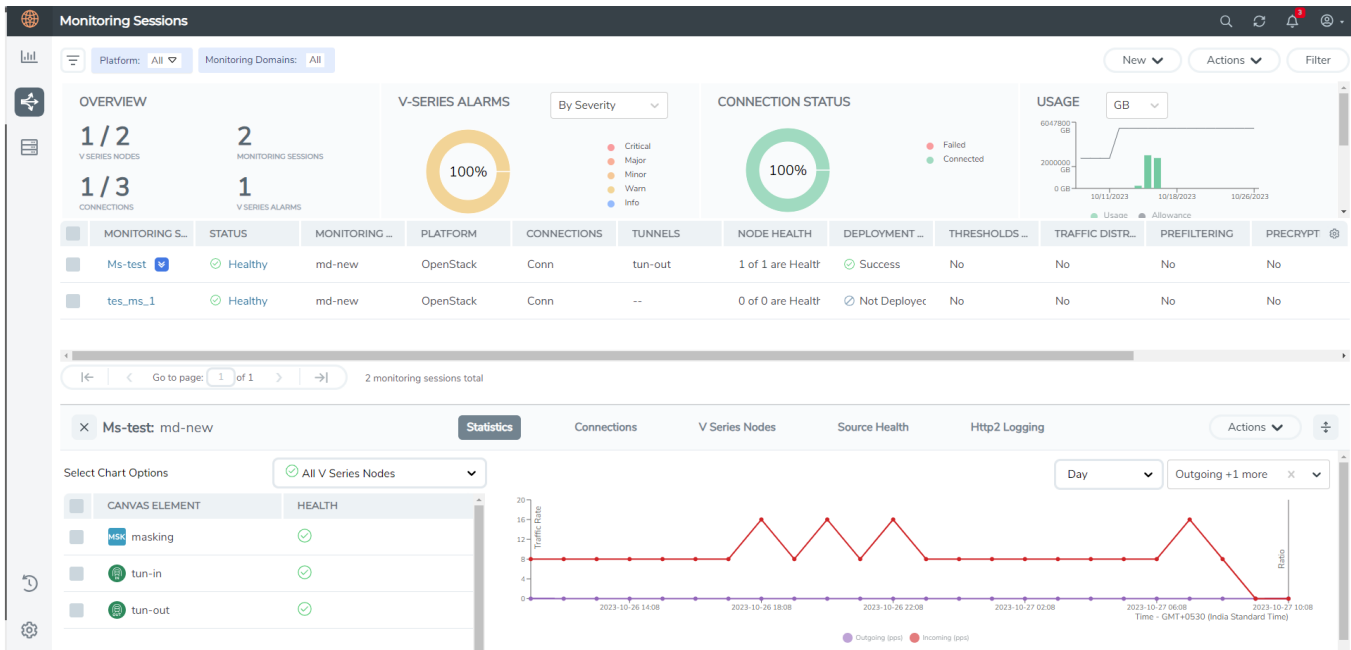
The Monitoring Session page also has the following buttons:

Button	Description
Undeploy	Undeploys the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Edit	Opens the Edit page for the selected monitoring session.  <b>NOTE:</b> In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.
Delete	Deletes the selected monitoring session.

## 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.
- 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 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 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.

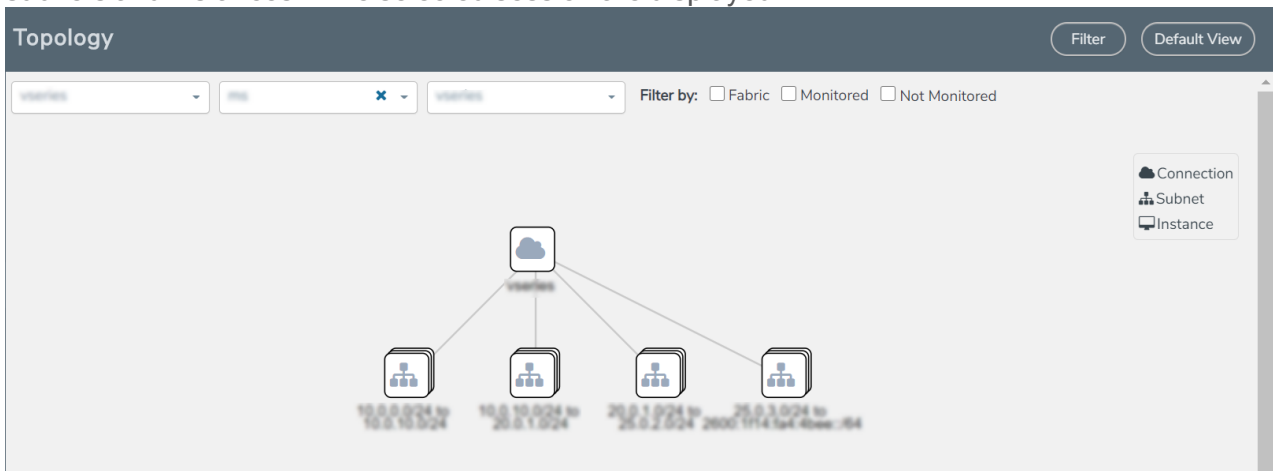
Raw EndPoint (REP) is a part of the monitoring session but can also receive the bypassed traffic that is not filtered by the map, so it is recording more packets than expected. For example, if the map has a rule as IPv4, but the REP can receive the bypassed (non-ipv4) traffic. The recorded number of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

## 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.

## Cloud Health Monitoring - Configuration Health Monitoring

GigaVUE-FM allows you to monitor the configuration health status of the entire monitoring session and also the individual fabric components for which monitoring session is configured. This feature provides 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



## View Monitoring Session Configuration Health

You can view the configuration status of the monitoring session and the components deployed, in the monitoring session page. This section provides information about the configuration health status of the various fabric components deployed in the monitoring session.

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

### Health

This column displays the configuration health status of the entire monitoring session.

The error message associated with monitoring session configuration appears when you hover over the health column. You can use the error message to help you troubleshoot and identify the components that are in conflict or mis-configured.

### V Series Node Health

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

You can view the health status of the individual V Series Nodes and also the error message associated with them, by clicking on the V Series Node Health column.

**NOTE:** V Series node health only displays the configuration health status therefore even if the V Series Node is down it will not be reflected in the monitoring session page.

The screenshot displays the AWS Monitoring Session configuration health page. The main table shows the following data:

Monitoring Domain	Monitoring Session	Statistics	Health	V Series Nodes Health	VPCs	Deployment Status	Number of Targets	Targets Source...
MD_1	MS1	View	Ok	1 of 1 are healthy				
					system-vpc-1	Success	6	2 of 2 are healthy

Below the table, there is a section for V Series Nodes Health with the following data:

V Series Node	Management IP	Version	Health
Gigamon-VSeriesNode-1	10.81.208.115	2.6.0	Ok

## Target Source Health

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.

## View Monitoring Session Statistics

You can now view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual V Series Node, select the name of the V Series Node for which you want to view the statistics from the V Series Node drop-down menu on the top left-corner of the Monitoring Session Statistics page.

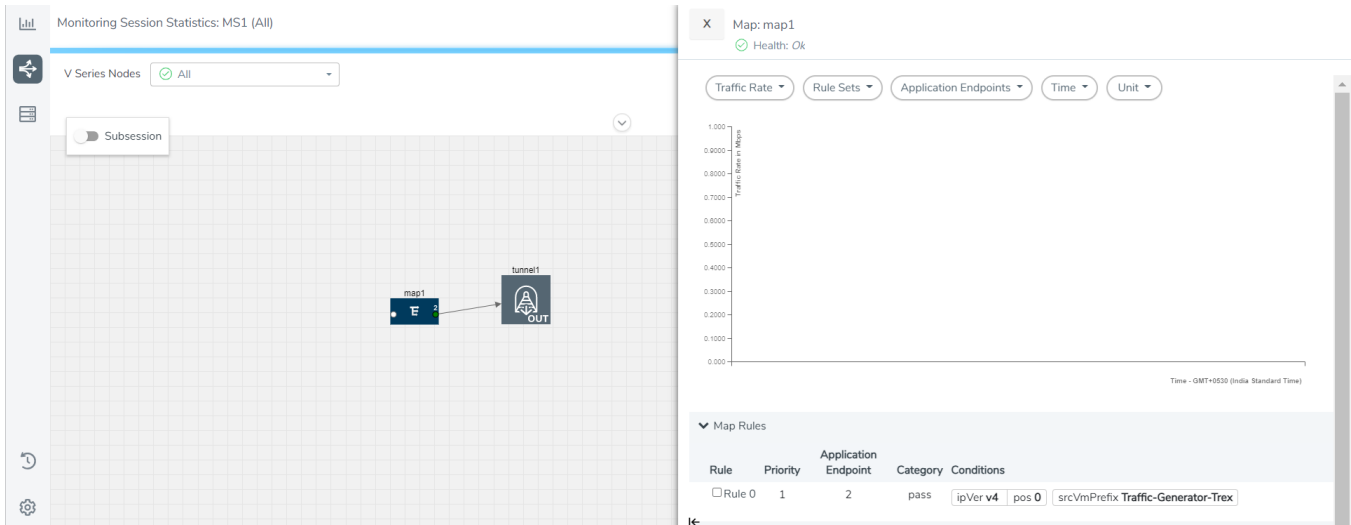
Hover over the V Series Node drop-down to view the number of the applications, end points, and other application environments configured for a particular V Series Node. It also displays the error message related to configuration for the particular V Series Node.

## View Monitoring Session Diagram

The Monitoring Session diagram page displays the applications and end points deployed in a particular monitoring session in pictorial form. To view the statistics of a particular application or an endpoint, click on the application icon for which you want to view the statistics. You can also view the statistics of a particular application for an individual V Series Node by selecting the name of the V Series Node for which you want to view the statistics from the V Series Node drop-down menu on the top left-corner of the Monitoring Session page.

When you select a V Series Node from the V Series Node drop-down, the application icon displays the name of that particular application as configured in the V Series Node.

The subsession toggle button available in the top-left corner of the canvas allows you to view the statistics of individual paths in the monitoring session.



## Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics<sup>1</sup> 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 for more details.
- 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:

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

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
<b>Inventory Status (Virtual)</b>	<p>Statistical details of the virtual inventory based on the platform and the health status.</p> <p>You can view the following metric details at the top of the dashboard:</p> <ul style="list-style-type: none"> <li>• Number of Monitoring Sessions</li> <li>• Number of V Series Nodes</li> <li>• Number of Connections</li> <li>• Number of GCB Nodes</li> </ul> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> <li>• Platform</li> <li>• Health Status</li> </ul>	<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
<b>V Series Node Statistics</b>	<p>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.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> <li>• Platform</li> <li>• Connection</li> <li>• V Series Node</li> </ul>	<i>V Series Node Maximum CPU Usage Trend</i>	<p>Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> <p><b>NOTE:</b> 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> </div>
		<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> <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> <p><b>NOTE:</b> You cannot use the time based filter options to filter and visualize the data.</p> </div>

Dashboard	Displays	Visualizations	Displays
		<i>V Series Node Rx Trend</i>	Receiving trend of the V Series node in 5 minutes interval, for the past one hour.
		<i>V Series Network Interfaces with Most Rx for Past 5 mins</i>	Total packets received by each of the V Series network interface for the past 5 minutes.  <b>NOTE:</b> You cannot use the time based filter options to filter and visualize the data.
		<i>V Series Node Tunnel Rx Packets/Errors</i>	Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation.
		<i>V Series Node Tunnel Tx Packets/Errors</i>	TX is for output tunnels from GigaVUE V Series Node. V Series Node Tunnel Tx Packets/Errors
<b>Dedup</b>	<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"> <li>Platform</li> <li>Connection</li> <li>VSeries Node</li> </ul>	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total dedup packets received (ipV4Dup, ipV6Dup and nonIPDup) against the dedup application overload.
		<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the dedup packets received against the dedup application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic
<b>Tunnel (Virtual)</b>	<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>	<i>Tunnel Bytes</i>	<p>Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.</p> <ul style="list-style-type: none"> <li>For input tunnel, transmitted traffic is displayed as zero.</li> <li>For output tunnel, received traffic is displayed as zero.</li> </ul>

Dashboard	Displays	Visualizations	Displays
	<ul style="list-style-type: none"> <li>• <b>Monitoring session:</b> 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.</li> <li>• <b>V Series node:</b> Management IP of the V Series node. Choose the required V-series node from the drop-down.</li> <li>• <b>Tunnel:</b> Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out.</li> </ul> <p>The following statistics are displayed for the tunnel:</p> <ul style="list-style-type: none"> <li>• Received Bytes</li> <li>• Transmitted Bytes</li> <li>• Received Packets</li> <li>• Transmitted Packets</li> <li>• Received Errored Packets</li> <li>• Received Dropped Packets</li> <li>• Transmitted Errored Packets</li> <li>• Transmitted Dropped Packets</li> </ul>	<p><i>Tunnel Packets</i></p>	<p>Displays packet-level statistics for input and output tunnels that are part of a monitoring session.</p>
<p><b>App (Virtual)</b></p>	<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"> <li>• <b>Monitoring session</b></li> <li>• <b>V series node</b></li> <li>• <b>Application:</b> Select the required application. By default, the visualizations displayed includes all the applications.</li> </ul> <p>By default, the following statistics are displayed:</p> <ul style="list-style-type: none"> <li>• Received Bytes</li> </ul>	<p><i>App Bytes</i></p>	<p>Displays received traffic vs transmitted traffic, in Bytes.</p>

Dashboard	Displays	Visualizations	Displays
	<ul style="list-style-type: none"> <li>• Transmitted Bytes</li> <li>• Received Packets</li> <li>• Transmitted Packets</li> <li>• Errored Packets</li> <li>• Dropped Packets</li> </ul>		
		<i>App Packets</i>	Displays received traffic vs transmitted traffic, as the number of packets.
<b>End Point (Virtual)</b>	<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"> <li>• Received Bytes</li> <li>• Transmitted Bytes</li> <li>• Received Packets</li> <li>• Transmitted Packets</li> <li>• Received Errored Packets</li> <li>• Received Dropped Packets</li> <li>• Transmitted Errored Packets</li> <li>• Transmitted Dropped Packets</li> </ul> <p>The endpoint drop-down shows &lt;V-series Node Management IP address : Network Interface&gt; 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"> <li>• <b>Monitoring session</b></li> <li>• <b>V Series node</b></li> <li>• <b>Endpoint:</b> Management IP of the V Series node followed by the Network Interface (NIC)</li> </ul>	<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.

# Administer GigaVUE Cloud Suite for Nutanix

You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for Nutanix:

- [Configure Nutanix Settings](#)
- [Role Based Access Control](#)
- [About Events](#)
- [About Audit Logs](#)

## Configure Nutanix Settings

To configure the Nutanix Settings:

1. Go to **Inventory > VIRTUAL > Nutanix** and then click **Settings**. The Settings page appears.
2. Click **Advanced** tab on the Settings page, click **Edit** to edit the Settings fields. Refer to the following table for descriptions of the Settings fields:

Settings	Description
Maximum number of connections allowed	Specifies the maximum number of 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 Nutanix.
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.
Traffic distribution MTU	

## Role Based Access Control

The Role Based Access Control (RBAC) feature controls the access privileges of users and restricts users from either modifying or viewing unauthorized data. Access privileges in GigaVUE Cloud Suite works on the same principles of access privileges in GigaVUE-FM in which the access rights of a user depends on the following:

- **User role:** A user role defines permission for users to perform any task or operation
- **User group:** A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more groups.



To access the resources and to perform a specific operation in GigaVUE Cloud Suite you must be a user with **fm\_super\_admin** role or a user with write access to the following resource category depending on the task you need to perform.

Resource Category	Cloud Configuration Task
<p><b>Physical Device Infrastructure Management:</b> This includes the following cloud infrastructure resources:</p> <ul style="list-style-type: none"> <li>• Cloud Connections</li> <li>• Cloud Fabric Deployment</li> <li>• Cloud Configurations</li> <li>• Sys Dump</li> <li>• Syslog</li> <li>• Cloud licenses</li> <li>• Cloud Inventory</li> </ul>	<ul style="list-style-type: none"> <li>• Configure GigaVUE Cloud Components</li> <li>• Create Monitoring Domain and Launch Visibility Fabric</li> </ul>
<p><b>Traffic Control Management:</b> This includes the following traffic control resources:</p> <ul style="list-style-type: none"> <li>• Monitoring session</li> <li>• Stats</li> <li>• Map library</li> <li>• Tunnel library</li> <li>• Tools library</li> <li>• Inclusion/exclusion Maps</li> </ul>	<ul style="list-style-type: none"> <li>• Create, Clone, and Deploy Monitoring Session</li> <li>• Add Applications to Monitoring Session</li> <li>• Create Maps</li> <li>• View Statistics</li> <li>• Create Tunnel End Points</li> </ul>

**NOTE:** Cloud APIs are also RBAC enabled.

Refer to the *GigaVUE Administration Guide* for detailed information about Roles, Tags, User Groups.

## About Events

The Events page displays all the events occurring in the virtual fabric component, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- Cloud provider License Expiry
- UCT-V Inventory Update Completed
- Cloud provider Connection Status Changed

An Alarm is a response to one or more related events. If an event is considered of high severity, then GigaVUE-FM raises an alarm. An example of alarm could be your cloud provider license expiry.

The alarms and events broadly fall into the following categories: Critical, Major, Minor, or info.

Navigate to **Dashboard > SYSTEM > Events**. The Event page appears.

Source	Time	Event Type	Severity	Affected Entity T...	Affected Entity	Alias	Device IP	Host Name	Scope	Description	Tags
FM	2022-08-10 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-09 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-08 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-07 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-06 0...	Licenses Expir...	Info	Floating License					FM	4 Floating	
FM	2022-08-05 1...	FM Applicatio...	Info	fm application ...				fmha1	fmService	CMS service f...	
FM	2022-08-04 1...	FM Applicatio...	Info	fm application ...				fmha1	fmService	CMS service f...	
FM	2022-08-04 1...	Alarm Delete ...	Critical	VSeries Node	vc-obc-pod2.u...				Alarm	Node Down. P...	

The following table describes the parameters recording for each alarm or event. You can also use filters to narrow down the results.

Controls/ Parameters	Description
<b>Source</b>	<p>The source from where the events are generated. The criteria can be as follows:</p> <ul style="list-style-type: none"> <li>■ FM - indicates the event was flagged by the Fabric Manager.</li> <li>■ IP address - is the address of the GigaVUE HC Series node that detected the event. For a node to be able to send notifications to the Fabric Manager, the SNMP_TRAP must be configured with the Fabric Manager's IP address specified as a host. Refer to the GigaVUE Administration Guide for instructions on adding a destination for SNMP traps.</li> <li>■ VMM - indicates the event was flagged by the Virtual Machine Manager.</li> <li>■ FM Health - indicates the event was flagged due to the health status change of GigaVUE-FM.</li> </ul>
<b>Time</b>	<p>The timestamp when the event occurred.</p> <p><b>IMPORTANT:</b> Timestamps are shown in the time zone of the client browser's computer and not the time zone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured time zone.</p>
<b>Event Type</b>	<p>The type of event that generated the events. The type of events can be CPU utilization high, cluster updated, device discovery failed, fan tray changed, netflow statistics, and so on.</p>
<b>Severity</b>	<p>The severity is one of Critical, Major, Minor, or Info.</p> <p>Info is informational messages. For example, when power status change notification is displayed, then the message is displayed as Info.</p>
<b>Affected Entity Type</b>	<p>The resource type associated with the event. For example, when low disk space notification is generated, 'Chassis' is displayed as the affected entity type.</p>
<b>Affected Entity</b>	<p>The resource ID of the affected entity type. For example, when low disk space notification is generated, the IP address of the node with the low disk space is displayed as the affected entity.</p>
<b>Alias</b>	<p>Event Alias</p>

Controls/ Parameters	Description
Device IP	The IP address of the device.
Host Name	The host name of the device.
<b>Scope</b>	The category to which the events belong. Events can belong to the following category: Domain, Node, Card, Port, Stack, Cluster, Chassis, GigaVUE-FM, GigaVUE-VM, and so on. For example, if there is a notification generated for port utilization low threshold, the scope is displayed as Physical Node.

To filter the alarms and event:

1. Click **Filter**. The Filter quick view is displayed.
2. Select the filtering criteria, then click **Apply Filter**. The results are displayed in the Events page.

## About Audit Logs

Audit logs track the changes and activities that occur in the virtual nodes due to user actions. The logs can be filtered to view specific information.

Navigate to **Dashboard > SYSTEM > Audit Logs**. The **All Audit Logs** page appears.

**All Audit Logs** Filter Manage

---

Filter : none

Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags
2020-1...	admin	login fmUser ad...	User	fm			SUCCESS		
2020-1...	admin	logout fmUser a...	User	fm			SUCCESS		
2020-1...	admin	login fmUser ad...	User	fm			SUCCESS		
2020-1...	admin	update map confi...	Map	fm			SUCCESS		

< < Go to page:  of 16 > > Total Records: 106

The Audit Logs have the following parameters:

Parameters	Description
<b>Time</b>	Provides the timestamp on the log entries.
<b>User</b>	Provides the logged user information.
<b>Operation Type</b>	Provides specific entries that are logged by the system such as: <ul style="list-style-type: none"> <li>■ Log in and Log out based on users.</li> <li>■ Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.</li> </ul>
<b>Source</b>	Provides details on whether the user was in GigaVUE-FM or on the node when the

Parameters	Description
	event occurred.
<b>Status</b>	Success or Failure of the event.
<b>Description</b>	In the case of a failure, provides a brief update on the reason for the failure.

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

Filtering the audit logs allows you to display specific type of logs. You can filter based on any of the following:

- **When:** display logs that occurred within a specified time range.
- **Who:** display logs related a specific user or users.
- **What:** display logs for one or more operations, such as Create, Read, Update, and so on.
- **Where:** display logs for GigaVUE-FM or devices.
- **Result:** display logs for success or failure.

To filter the audit logs, do the following:

1. Click **Filter**. The quick view for Audit Log Filters displays.
2. Specify any or all of the following:
  - **Start Date** and **End Date** to display logs within a specific time range.
  - **Who** limits the scope of what displays on the Audit Logs page to a specific user or users.
  - **What** narrows the logs to the types of operation that the log is related to. You can select multiple operations. Select **All Operations** to apply all operation types as part of the filter criteria.
  - **Where** narrows the logs to particular of system that the log is related to, either GigaVUE-FM or device. Select **All Systems** apply both GigaVUE-FM and device to the filter criteria.
  - **Result** narrows the logs related to failures or successes. Select All Results to apply both success and failure to the filter criteria.
3. Click **OK** to apply the selected filters to the Audit Logs page.

# 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 6.6 Hardware and Software Guides
<p><b>DID YOU KNOW?</b> 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 <b>Edit &gt; Advanced Search</b> from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p>
<p><b>Hardware</b></p> <p>how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices</p>
<a href="#">GigaVUE-HC1 Hardware Installation Guide</a>
<a href="#">GigaVUE-HC2 Hardware Installation Guide</a>
<a href="#">GigaVUE-HC3 Hardware Installation Guide</a>
<a href="#">GigaVUE-HC1-Plus Hardware Installation Guide</a>
<a href="#">GigaVUE-HCT Hardware Installation Guide</a>
<a href="#">GigaVUE-TA25 Hardware Installation Guide</a>
<a href="#">GigaVUE-TA25E Hardware Installation Guide</a>
<a href="#">GigaVUE-TA100 Hardware Installation Guide</a>
<a href="#">GigaVUE-TA200 Hardware Installation Guide</a>
<a href="#">GigaVUE-TA200E Hardware Installation Guide</a>

<b>GigaVUE Cloud Suite 6.6 Hardware and Software Guides</b>	
<b>GigaVUE-TA400 Hardware Installation Guide</b>	
<b>GigaVUE-OS Installation Guide for DELL S4112F-ON</b>	
<b>G-TAP A Series 2 Installation Guide</b>	
<b>GigaVUE M Series Hardware Installation Guide</b>	
<b>GigaVUE-FM Hardware Appliances Guide</b>	
<b>Software Installation and Upgrade Guides</b>	
<b>GigaVUE-FM Installation, Migration, and Upgrade Guide</b>	
<b>GigaVUE-OS Upgrade Guide</b>	
<b>GigaVUE V Series Migration Guide</b>	
<b>Fabric Management and Administration Guides</b>	
<b>GigaVUE Administration Guide</b>	covers both GigaVUE-OS and GigaVUE-FM
<b>GigaVUE Fabric Management Guide</b>	how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
<b>Cloud Guides</b>	
how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms	
<b>GigaVUE V Series Applications Guide</b>	
<b>GigaVUE V Series Quick Start Guide</b>	
<b>GigaVUE Cloud Suite Deployment Guide - AWS</b>	
<b>GigaVUE Cloud Suite Deployment Guide - Azure</b>	
<b>GigaVUE Cloud Suite Deployment Guide - OpenStack</b>	
<b>GigaVUE Cloud Suite Deployment Guide - Nutanix</b>	
<b>GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)</b>	
<b>GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)</b>	
<b>GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration</b>	
<b>Universal Cloud Tap - Container Deployment Guide</b>	
<b>Gigamon Containerized Broker Deployment Guide</b>	
<b>GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide</b>	

## GigaVUE Cloud Suite 6.6 Hardware and Software Guides

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 TA Series devices

#### GigaVUE-OS Security Hardening Guide

#### GigaVUE Firewall and Security Guide

#### GigaVUE Licensing Guide

#### GigaVUE-OS Cabling Quick Reference Guide

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

#### GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

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

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

### Release Notes

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

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

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

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

### In-Product Help

#### GigaVUE-FM Online Help

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

## How to Download Software and Release Notes from My Gigamon

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

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or

- Older versions of PDFs (pre-v5.7).

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

1. Log in to [My Gigamon](#).
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "6.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 6.6.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](mailto: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?	<b>Describe the issue</b>	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	<b>How can we improve the content?</b> <b>Be as specific as possible.</b>	
	<b>Any other comments?</b>	

## 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](mailto:support@gigamon.com).

## Contact Sales

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

**Telephone:** +1.408.831.4025

**Sales:** [inside.sales@gigamon.com](mailto:inside.sales@gigamon.com)

**Partners:** [www.gigamon.com/partners.html](http://www.gigamon.com/partners.html)

## Premium Support

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

## The VÜE Community

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

Visit the VÜE site to:

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

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

**Register today at [community.gigamon.com](https://community.gigamon.com)**

**Questions?** Contact our Community team at [community@gigamon.com](mailto: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)