Gigamon®

GigaVUE Cloud Suite for Nutanix - Deployment Guide

GigaVUE Cloud Suite

Product Version: 6.9

Document Version: 1.0

(See Change Notes for document updates.)

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
6.9	1.0	12/06/2024	The original release of this document with 6.9.00 GA.

Contents

GigaVUE Cloud Suite Deployment Guide - Nutanix

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

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 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.

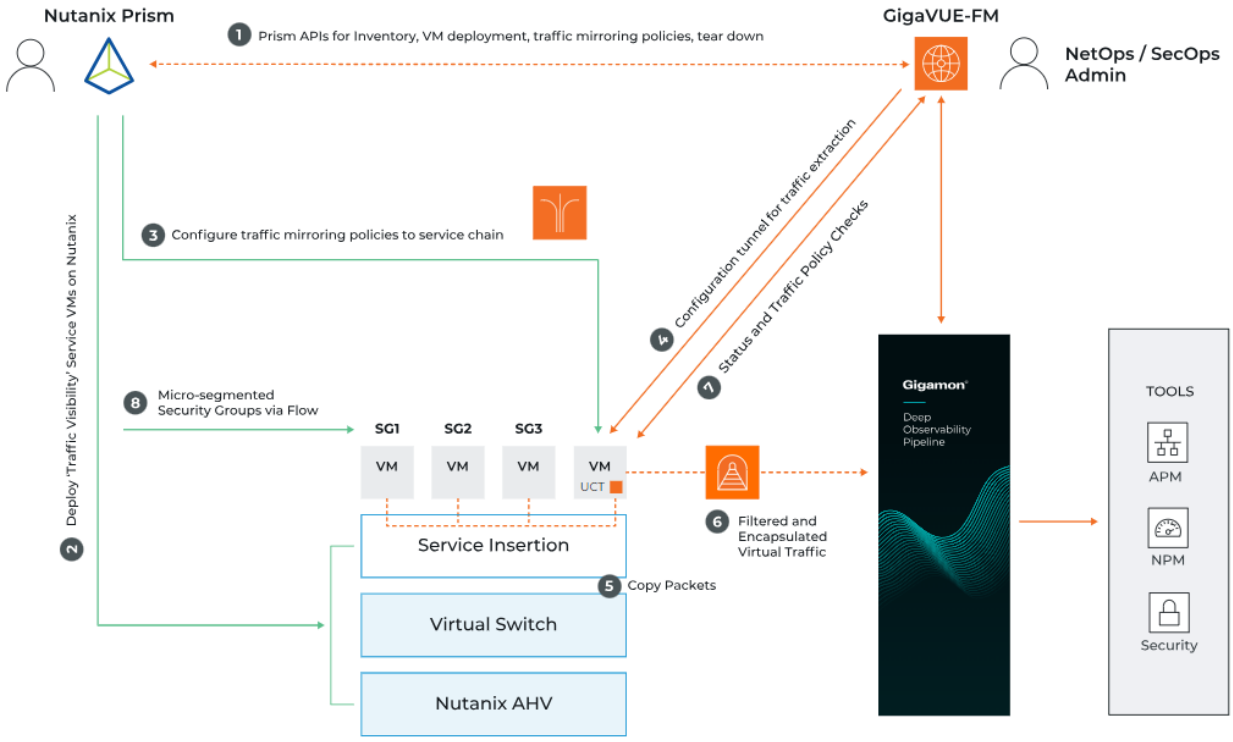
GigaVUE-FM integrates with the Nutanix Platform and deploys the components of the GigaVUE Cloud Suite for Nutanix in the underlay environment.

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

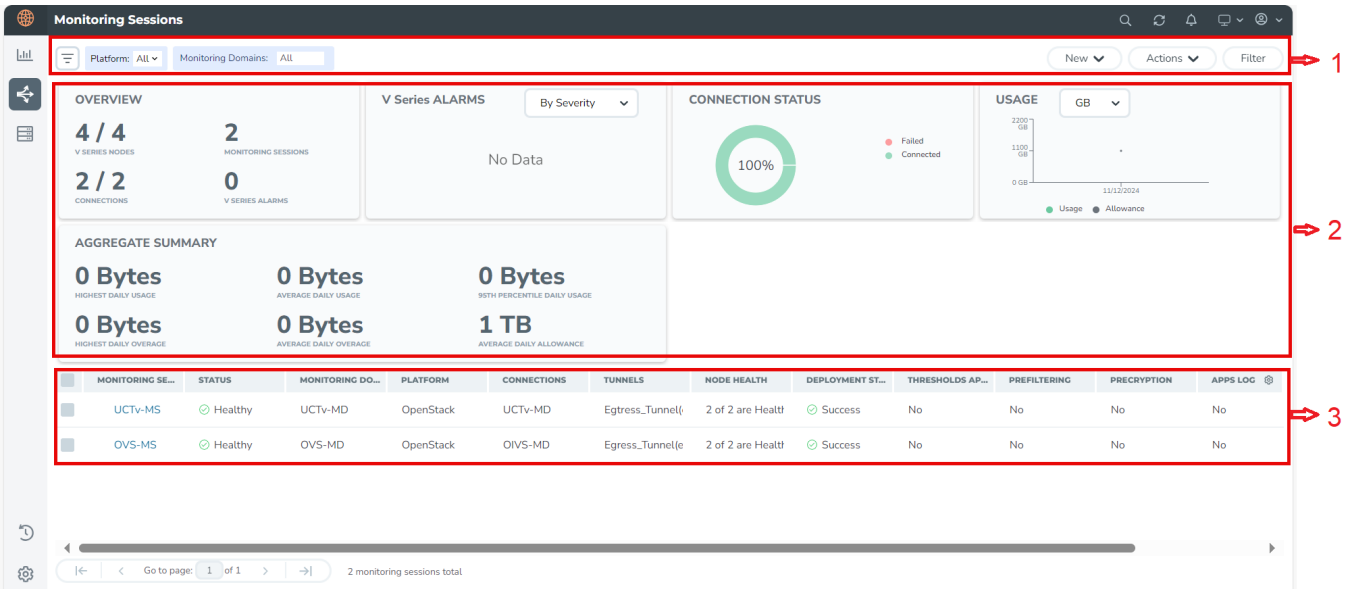
GigaVUE Cloud Suite for Nutanix includes the following components:

Component	Description
GigaVUE-FM fabric manager	GigaVUE-FM is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud Suite for VMware. 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.
GigaVUE® V Series Node	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.
GigaVUE® V Series Proxy	GigaVUE V Series Proxy is a 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.

Cloud Overview Page (Nutanix)

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.

To view the overall cloud overview page, go to **Traffic > Virtual > Overview**.



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

Number	Section	Description
1	Top Menu	Refer to Top Menu.
2	Charts	Refer to Viewing Charts.
3	Monitoring Session Details	In the Overview page, you can view the Monitoring Session details of all the cloud platforms. Refer to Viewing Monitoring Session Details section for more details.

Top Menu

The Top menu consists of the following options:

Options	Description
New	You can create a new Monitoring Session and new Monitoring Domain.
Actions	You can do the following actions using the **Action** button: **Edit** - Opens the edit page for the selected Monitoring Session. **Delete** - Deletes the selected Monitoring Session. **Clone** - Duplicates the selected Monitoring Session. **Deploy** - Deploys the selected Monitoring Session. **Undeploy** - Undeploys the selected Monitoring Session. **Apply Threshold** - Applies the threshold template created for monitoring cloud traffic health. Refer to *Monitor Cloud* section for details.

Options	Description
Filter	You can filter the Monitoring Session details based on a criterion or combination of criteria. For more information, refer to Filters.

Filters

You can apply the filters on the Monitoring Sessions page in the below two ways:

- Filter on the left corner
- Filter on the right corner

Filter on the left corner 

1. Select the required platform from the **Platform** drop- down list.
2. Click  and select the Monitoring Domain.

You can select one or multiple domains. You can also edit and create a new Monitoring Domain in the filter section.

Filter on the right corner 

You can filter Monitoring Session and Monitoring Domain details 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
- 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, 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 quickly view the V Series alarms generated. 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

You can view the following details in the overview table:

Details	Description
Monitoring Sessions	Name of the Monitoring Session. When you click the name of the session, you will be redirected to the platform specific Monitoring Session page.
Status	Health status of the Monitoring Session.
Monitoring Domain	Name of the Monitoring Domain to which the Monitoring Session is associated.

Details	Description
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 status of the GigaVUE V Series Node.
Deployment Status	Status of the deployment.
Threshold Applied	Specifies whether the threshold is applied or not.
Prefiltering	Specifies whether Prefiltering is configured or not.
Precryption	Specifies whether Precryption is configured or not.
APPS logging	Specifies whether APPS logging is configured or not.
Traffic Mirroring	Specifies whether Traffic Mirroring is configured or not.

NOTE: Click the settings icon to select the required options to appear in the table.

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 (Nutanix)

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 Node.

- You must create a subnet and security group in Nutanix Prism Central. For more information on creating a subnet, see Configuring Network Connections.
- User account with same credentials should be created in PRISM ELEMENT as in Prism Central.
- CLUSTER ADMIN role should be enabled for selected user account in PRISM ELEMENT role configuration.

Roles/Permission required for Prism Central user account

- AHV VM
- Access Console Virtual Machine
- Allow Virtual Machine Power Off
- Allow Virtual Machine Power On
- Allow Virtual Machine Reboot
- Allow Virtual Machine Reset
- Create Virtual Machine
- Delete Virtual Machine
- Update Virtual Machine
- Update Virtual Machine Boot Config
- Update Virtual Machine Categories
- Update Virtual Machine NIC List
- Update Virtual Machine Power State
- View Virtual Machine

Refer to the following topics for more detailed information:

- Minimum Requirements -Nutanix
- Network Firewall Requirements
- Default Login Credentials

Minimum Requirements -Nutanix

Refer to the following sections for details on minimum ompute requirements, AOS versions, and prism Central details.

Minimum Compute Requirements for Nutanix

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

Supported Prism Central Versions for Nutanix

Minimum requirements for GigaVUE V Series Node are listed in the following table:

Platforms	GigaVUE-FM	AOS	Prism Central	GigaVUE V Series Node	GigaVUE V Series Proxy
Versions Supported	6.7	6.5	pc.2022.6	6.7.00	6.7.00
	6.8	6.5	pc.2022.6	6.8.00	6.8.00
	6.9	6.5	pc.2024.2	6.9.00	6.9.00

Network Firewall Requirements

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

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
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 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.
GigaVUE V Series Node					
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 toGigaVUE 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	• UDP (VXLAN) • IP Protocol (L2GRE)	• VXLAN (default 4789) • L2GRE (IP 47)	Tool IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound (optional)	Custom ICMP Rule	ICMP	• echo request • echo reply	Tool IP	Allows GigaVUE® V Series Node to health check the tunnel destination traffic.

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE V Series Proxy (optional)					
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

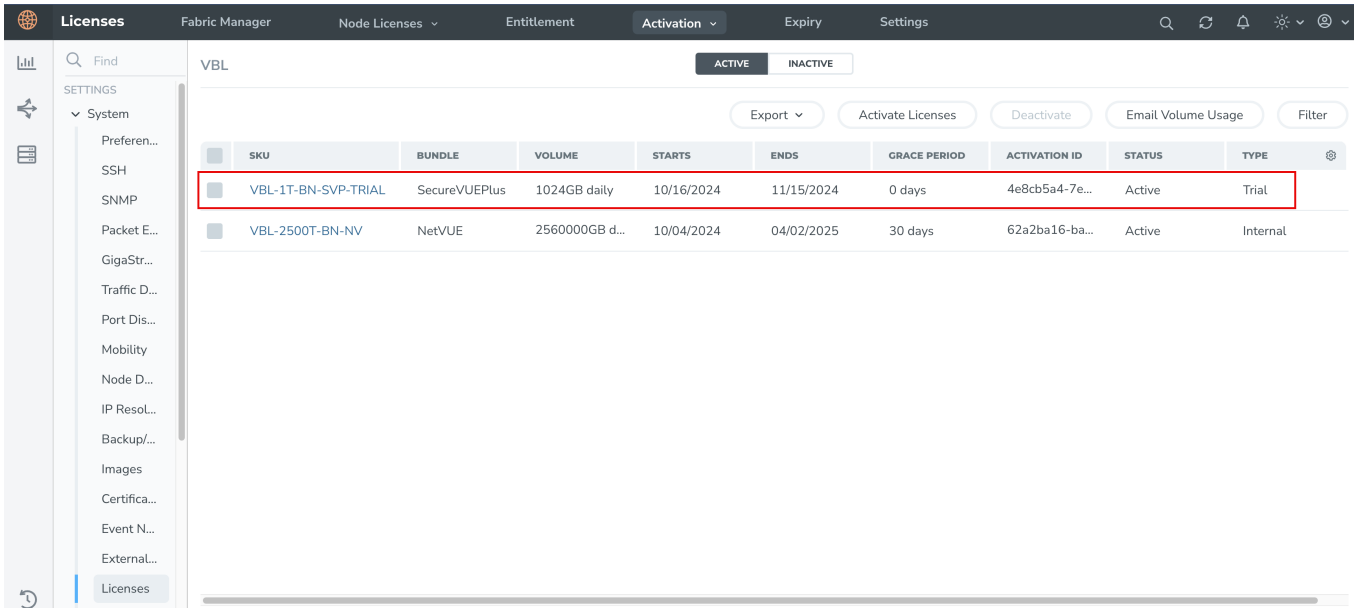
GigaVUE Cloud Suite for Nutanix supports Volume Based License (VBL) model.

Refer to the following sections for details:

- Default Trial Licenses
- Volume Based License (VBL)
- Activate Volume-Based Licenses
- Manage Volume-Based Licenses

Default Trial Licenses

After you install GigaVUE-FM, you will receive a one-time, free 1TB SecureVUE Plus trial Volume-Based License (VBL) for 30 days, starting from the installation date.



This license includes the following applications:

- ERSPAN
- GENEVE
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flow map
- Header Stripping
- Header Addition
- De-duplication
- NetFlow
- Application Packet Filtering
- Application Filtering Intelligence
- Application Metadata Intelligence
- Application Metadata Exporter
- Inline SSL
- SSL Decrypt
- Precryption

NOTE: 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.

When you install a new Volume-Based License (VBL), the existing trial license will remain active alongside the new VBL. Once the trial license period expires, it will be automatically deactivated. After deactivation, the trial license will be moved to the **Inactive** tab in the **VBL** page.

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 GigaVUE Cloud Suite is volume-based. In the Volume-Based Licensing (VBL) scheme, a license entitles specific applications on your V Series Nodes to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes becomes irrelevant for 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 one month. Service period is the period of time for which the total usage or overage is tracked.

For purchasing licenses with the Volume-Based License (VBL) option, contact our 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[1]. The number in the SKU indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE has a daily volume allowance of 250 terabytes for CoreVUE bundle.

Bundle Replacement Policy

Refer to the following notes:

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

Add-on Packages

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

Rules for add-on packages:

- Add-on packages can only to be added when there is an active base bundle available in GigaVUE-FM.
- The base bundle limits the total volume usage of the add-on package.
- If your add-on package has volume allowance less than the base bundle, then your add-on package can only handle volume allocated for add-on package.
- When the life term of an add-on package extends beyond the base bundle, then when the base bundle expires, the volume allowance of the add-on package will be reduced to zero until a new base bundle is added.

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

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

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

How GigaVUE-FM Tracks Volume-Based License Usage

GigaVUE-FM tracks the license usage for each GigaVUE 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).
- When a license expires, you will be notified with an audit log. Refer to the *About Audit Logs* section in the respective GigaVUE Cloud Suite Deployment Guide.
- 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.

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** from the **Activation** drop-down.
3. Click **Activate Licenses**. The **Activate License** page appears.
4. Select **IP Address** or **Hostname** to include this information. If you exclude the IP Address or Hostname, you will have to identify the chassis or GigaSMART card by its ID when activating.
5. Download the fabric inventory file that contains information about GigaVUE-FM. Click **Next**. Refer to the What is a Fabric Inventory File section in *GigaVUE Licensing Guide* for more details.
6. Click **Gigamon License Portal** to 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.
7. Return to GigaVUE-FM and upload the file by clicking **Choose File** button.

Manage Volume-Based Licenses

This section provides information on how to manage active and inactive Volume-Based Licenses in GigaVUE-FM.

Manage active Volume-Based License

To manage active Volume-Based License (VBL):

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

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

Field	Description
SKU	Unique identifier associated with the license.
Bundle	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. Entitlement ID is the permission with which the acquired license can be activated online.
Reference ID	Reference ID.
Status	License status.

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

Manage Inactive Volume-Based License

To manage inactive Volume-Based License (VBL):

1. On the left navigation pane, click  .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL** from the **Activation** drop-down and click **Inactive**.

Field	Description
SKU	Unique identifier associated with the license.
Bundle	Bundle to which the license belongs to.
Ends	License end date.
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 Inactive tab of VBL page. To display these fields, click on the column setting configuration option and enable these fields.

Use the following buttons to manage your VBL.

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

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

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

Install and Upgrade GigaVUE-FM

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

- Cloud —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.
- On-premises—To install and upgrade GigaVUE-FM in your enterprise data center, refer to *GigaVUE-FM Installation and Upgrade Guide* available in the Gigamon Documentation Library.

Upload Fabric Images

The recent GigaVUE V Series Node and GigaVUE-FM image file can be downloaded from Gigamon Customer Portal. After fetching the images, upload the fabric images to Prism Central. Select all the available clusters as placements while uploading fabric images.

Upload the appropriate Nutanix image file.

Once the images are uploaded, you can view the images under **Virtual Infrastructure > Images** in the Nutanix console.

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 GigaVUE-FM on Nutanix
- Create a Monitoring Domain
- Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM
- Configure Monitoring Session

Install Custom Certificate

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

You can upload the custom certificate in two ways:

- Upload Custom Certificates using GigaVUE-FM
- Upload Custom Certificate using Third Party Orchestration

Upload Custom Certificates using GigaVUE-FM

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

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

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

4. Click **Save**.

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

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

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

Upload Custom Certificate using Third Party Orchestration

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

For integrated mode:

- Configure GigaVUE Fabric Components in AWS
- Configure GigaVUE Fabric Components in Azure
- Configure GigaVUE Fabric Components in OpenStack

For generic mode:

- Configure GigaVUE Fabric Components in AWS
- Configure GigaVUE Fabric Components in Azure
- Configure GigaVUE Fabric Components in GCP
- Configure GigaVUE Fabric Components in Nutanix
- Configure GigaVUE Fabric Components in OpenStack
- Configure GigaVUE V Series Nodes using VMware ESXi

Adding Certificate Authority

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

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.
Certificate Authority	Use any of the following option to enter the Certificate Authority
Copy and Paste	
Certificate	Enter the certificate.
Install from URL	
Path	Enter the URL in the following format: <protocol>://<username>@<hostname/IP address>/<file path>/<file name>
Password	Enter the password
Install from Local Directory	
File Name	Click **Choose File** button and choose the certificate from the desired location.

4. Click **Save**.

Create a Monitoring Domain

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**.
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
Monitoring Domain	Enter a monitoring domain name.
Connection Alias	An alias used to identify the monitoring domain.
Use Legacy V Series Mode	By default, V Series 2 is enabled. Enable this option, if you want to use the legacy V Series Mode
Nutanix Prism Central IP	Enter the Nutanix Prism Central IP address. **NOTE:** To ensure the validity of Nutanix Prism central certificates issued by a trusted Certificate Authority (CA), you must enable the Trust Store. Refer to the Trust Store section in GigaVUE Administration Guide for more detailed information.
Nutanix Prism Central Username	Enter the username.
Nutanix Prism Central Password	Enter the password.
Cluster	Select the cluster where the GigaVUE V Series Proxy and GigaVUE® V Series Node are to be deployed.
Traffic Acquisition tunnel MTU	Enter the Tunnel MTU size.

4. Click **Save**. The **Nutanix Fabric Launch Configuration** page appears.

.

Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM

You must establish a connection between GigaVUE-FM and your Prism environment before you can perform the configuration steps for GigaVUE® V Series Node and GigaVUE V Series Proxy. After a connection is established, you can use GigaVUE-FM to specify a launch configuration for the GigaVUE® V Series Nodes.

Nutanix Fabric Launch Configuration

The fabric images (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.

GigaVUE V Series Proxy manages multiple GigaVUE® V Series Node and orchestrates the flow of traffic from GigaVUE® V Series Nodes to the monitoring tools.

To configure the Nutanix Fabric Images 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
Cluster	Select the cluster where the GigaVUE V Series Proxy and GigaVUE® V Series Node are to be deployed.
Enable Custom Certificates	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. **NOTE:** If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate.
Configure a V Series Proxy (Optional)	Select this option to configure a V Series Proxy.
GigaVUE® V Series Node	• **Hosts**—Select a node or multiple nodes from the selected Cluster. • **Version**—Select a GigaVUE® V Series Node image file. Refer to Upload Fabric Images for more information. • **Manangement Subnet**—The subnets registered in Prism Central are listed. Select a management subnet as specified in the Prerequisites (Nutanix). • **Data Subnets**—Select the subnet(s) based on the required VMs and vNICs. Click **Add Subnet** to add additional Subnets. • **Memory Size (GB)**—Enter the memory size of the vCPU(s) • **Disk Size (GB)**—Enter the image size of the GigaVUE® V Series Node. • **Number of vCPUs**—Enter the number of vCPUs required. • **Cloud-init User Data (Optional)**—Enter cloud-init user data (YAML, JSON, or Shell script)

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 fabric images. 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.

Upgrade GigaVUE V Series Node in GigaVUE-FM for Nutanix

This section describes how to upgrade the GigaVUE V Series Node for GigaVUE Cloud Suite for Nutanix:

1. Go to **Traffic > Virtual > Orchestrated Flows > Nutanix**. The **Monitoring Sessions** page appears.
2. Select the Monitoring Sessions with the GigaVUE V Series Node you want to upgrade.
3. Click **Actions > Undeploy**.
4. Go to **Inventory > VIRTUAL > Nutanix**. The **Monitoring Domain** page appears.
5. On the Monitoring Domain page, select the Monitoring Domain check box for the Monitoring Domain with the GigaVUE V Series Node you want to upgrade.
6. Click **Actions > Delete Fabric**. The GigaVUE V Series Nodes are deleted.
7. Deploy the latest version of GigaVUE V Series Node. Refer to Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM for step-by-step instructions on deploying GigaVUE V Series Node.
8. Go to **Monitoring Sessions** page.
9. Select the Monitoring Sessions undeployed in Step 2.
10. Click **Actions > Deploy**.

The GigaVUE V Series Nodes are successfully upgraded.

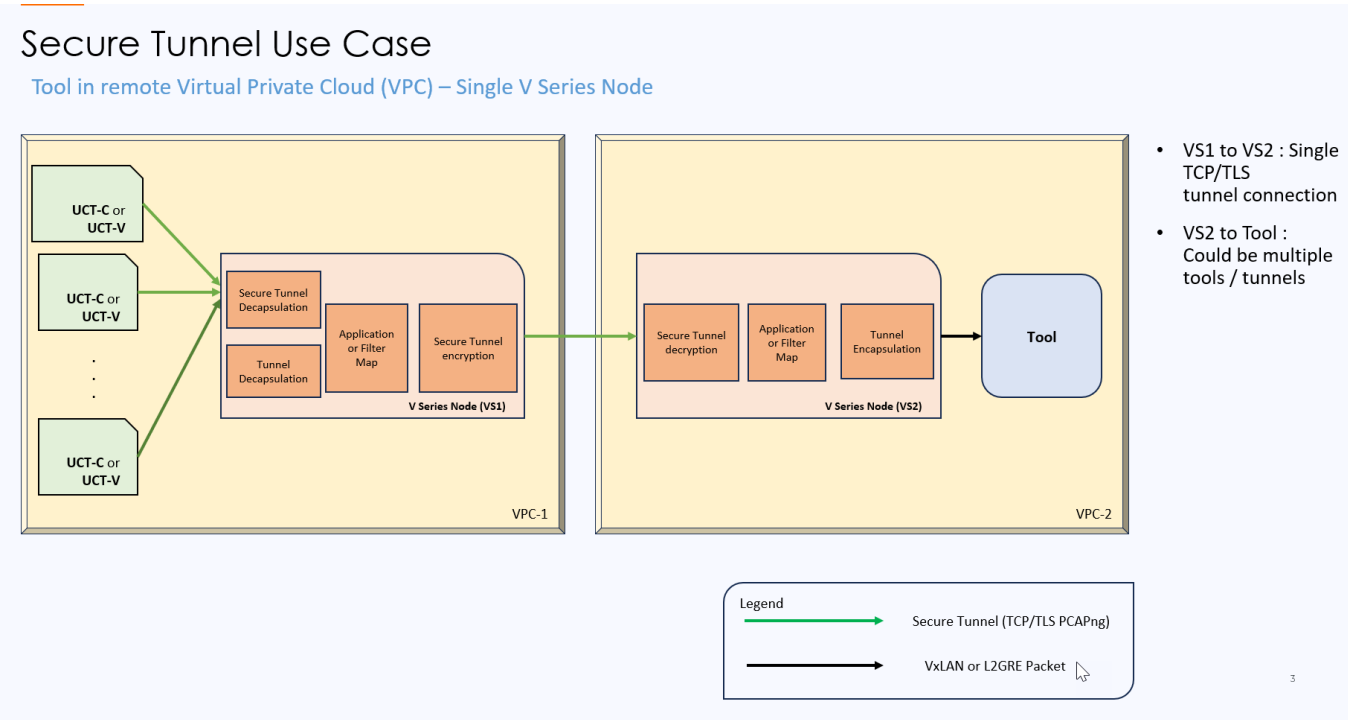
Secure Tunnels

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.



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 (Nutanix).

Configure Secure Tunnel (Nutanix)

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:

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td>1.</td><td>Upload a Certificate Authority (CA) Certificate</td><td>You must upload a Custom Certificate to UCT-V Controller for establishing a connection between the GigaVUE V Series Node.

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 Certificate Authority. The Add Certificate Authority page appears.
3. Enter or select the following information.
<table><tr><th>Field</th><th>Action</th></tr><tr><td>Alias</td><td>Alias name of the CA.</td></tr><tr><td>File Upload</td><td>Choose the certificate from the desired location.</td></tr></table>4. Click Save.
5. Click Deploy All.

For more information, refer to the section Adding Certificate Authority</td></tr>
<tr><td>2.</td><td>Upload a SSL Key</td><td>You must add a SSL key to GigaVUE V Series node. To add SSL Key, follow the steps in the section Upload SSL Keys section in GigaVUE V Series Applications Guide.</td></tr>
<tr><td>3</td><td>Create a secure tunnel between UCT-V and GigaVUE V Series Node 1.</td><td>You should enable the secure tunnel feature to establish a connection between the UCT-Vand GigaVUE V Series node 1. To enable the secure tunnel feature follow these steps:
1. In the Edit Monitoring Session page, click Options. The Apply template page appears.
2. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and precrypted traffic.</td></tr>
<tr><td>4.</td><td>Select the added SSL Key while creating a monitoring domain.</td><td>Select the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in GigaVUE V Series Node 1.

You must select the added SSL Key in GigaVUE V Series Node 1.

To select the SSL key, follow the steps in the section Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td>5.</td><td>Select the added CA certificate while creating the monitoring domain</td><td>You should select the added Certificate Authority (CA) in UCT-V Controller. To select the CA certificate, follow the steps in the section Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM</td></tr>
<tr><td>6</td><td>Create an Egress tunnel from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session.</td><td>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 Create Ingress and Egress Tunnel (Nutanix) for more detailed information on how to create tunnels.
To create the egress tunnel, follow these steps:
1. After creating a new monitoring session, or click Actions > Edit on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table:
<table><tr><th>Field</th><th>Action</th></tr><tr><td>Alias</td><td>The name of the tunnel endpoint.</td></tr><tr><td>Description</td><td>The description of the tunnel endpoint.</td></tr></table></td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td>Type</td><td>Select TLS-PCAPNG for creating egress secure tunnel</td></tr>
<tr><td>Traffic Direction</td><td>Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:
o MTU- The default value is 1500 for Azure.
NOTE: 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.
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.
o DSCP - Enter the Differentiated Services Code Point (DSCP) value.
o Flow Label - Enter the Flow Label value.
o Source L4 Port- Enter the Souce L4 Port value
o Destination L4 Port - Enter the Destination L4 Port value.
o Flow Label
o Cipher- Only SHA 256 is supported.
o TLS Version - Select TLS Version1.3.
o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments.
o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.
o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments.</td></tr>
<tr><td>Remote Tunnel IP</td><td>Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).</td></tr>
</table>
4. Click Save.
</td></tr>
<tr><td>7.</td><td>Select the added SSL Key while creating a monitoring domain and config</td><td>You must select the added SSL Key in GigaVUE V Series Node 2. To select the SSL key, follow the steps in the section Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td>uring the fabric components in GigaVUE-FM in GigaVUE V Series Node 2</td><td></td></tr>
<tr><td>8</td><td>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.</td><td>
You must create a ingress tunnel for traffic to flow in from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session.

To create the ingress tunnel, follow these steps:
1. After creating a new monitoring session, or click Actions > Edit on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table:
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td>Alias</td><td>The name of the tunnel endpoint.</td></tr>
<tr><td>Description</td><td>The description of the tunnel endpoint.</td></tr>
<tr><td>Type</td><td>Select TLS-PCAPNG for creating egress secure tunnel.
NOTE: 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.</td></tr>
<tr><td>Traffic Direction</td><td>Choose In (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>IP Version</td><td>The version of the Internet Protocol. IPv4 and IPv6 are supported.</td></tr>
<tr><td>Remote Tunnel IP</td><td>Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 1 (Destination IP).</td></tr>
</table>
4. Click Save.
</td></tr>
</table>

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 (Nutanix)
- Create Ingress and Egress Tunnel (Nutanix)
- Create Raw Endpoint (Nutanix)
- Create a New Map
- Add Applications to Monitoring Session
- Interface Mapping (Nutanix)
- Deploy Monitoring Session
- View Monitoring Session Statistics
- Visualize the Network Topology

Create a Monitoring Session (Nutanix)

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

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

For the connections without UCT-Vs, there are no targets that are automatically selected. You can use Customer Orchestrated Source in the Monitoring Session to accept a tunnel from anywhere.

You can create multiple Monitoring Sessions per Monitoring Domain.

To create a new Monitoring Session:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Click **New Monitoring Session** button to open the New Monitoring Session configuration page.
3. Enter the required information as described in the following table.

Field	Description
Alias	The name of the Monitoring Session.
Monitoring Domain	Select the required Monitoring Domain from the drop-down list or click **Create New** to create a new one.
Connections	Select the required connections that are to be included as part of the Monitoring Domain.

4. Click **Save**. The Monitoring Session Overview page appears.

Monitoring Session Page (Nutanix)

You can view the following tabs on the Monitoring Session page:

Tab	Description
Overview	You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can also view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can filter the statistics based on the elements associated with the Monitoring Session. For more information, refer to View Monitoring Session Statistics.
Sources	Displays the sources and target details monitored by the Monitoring Session. You can view and edit the connection details of the Monitoring Session. You can view the deployment status, number of targets, and targets source health. **NOTE:** In the case of OVS Mirroring, the Sources tab also displays the Hypervisor details along with the Instances.

Tab	Description
Traffic Acquisition	You can enable or disable Prefiltering, Precryption, and Secure Tunnel here. You can also create a prefiltering template and apply it to the Monitoring Session. Refer to Configure Monitoring Session Options (Nutanix) for more detailed information. **NOTE:** Traffic Acquisition is only applicable for Monitoring Domain created with UCT-V as Acquisition method.
Traffic Processing	You can view, add, and configure applications, tunnel endpoints, raw endpoints, and maps. You can view the statistical data for individual applications and also apply threshold template, enable user defined applications, and enable or disable distributed De-duplication. Refer to Configure Monitoring Session Options (Nutanix) for more detailed information.
V Series Nodes	You can view the V Series nodes associated with the Monitoring Session. In the split view, you can view details such as name of the V Series Node, health status, deployment status, Host VPC, version, and Management IP. You can also change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping (Nutanix) section for details.

The Monitoring Session page **Actions** button has the following options. The Actions menu is placed common in all the tabs explained above.

Button	Description
Delete	Deletes the selected Monitoring Session.
Clone	Duplicates the selected Monitoring Session.
Deploy	Deploys the selected Monitoring Session.
Undeploy	Undeploys the selected Monitoring Session.

You can use the  icon on the left side of the Monitoring Session page to view the Monitoring Sessions list. Click  to filter the Monitoring Sessions list. In the side bar, you can perform the following bulk actions by selecting a single or multiple Monitoring Sessions:

- Delete
- Deploy
- Undeploy

Configure Monitoring Session Options (Nutanix)

In the Monitoring Session page, you can perform the following actions in the **TRAFFIC ACQUISITION** and **TRAFFIC PROCESSING** tabs.

- Enable Prefiltering
- Enable Precryption

- Apply Threshold Template
- Enable User-defined applications
- Enable Distributed De-duplication

TRAFFIC ACQUISITION

To navigate to **TRAFFIC ACQUISITION** tab, follow the steps given below:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a Monitoring Session from the Monitoring Sessions list view on the left side of the screen and click the **TRAFFIC ACQUISITION** tab.

You can perform the following actions in the **TRAFFIC ACQUISITION** page:

- Enable Prefiltering
- Enable Precryption

Enable Prefiltering

To enable Prefiltering, follow the steps given below:

1. In the Monitoring Session **TRAFFIC ACQUISITION** page, click **Mirroring** tab and click **Edit Mirroring**.
2. Enable the **Mirroring** toggle button.
3. Enable the **Secure Tunnel** button if you wish to configure Secure Tunnels. For more information about Secure Tunnel, refer to Configure Secure Tunnel (AWS).
4. You can select an existing Prefiltering template from the **Template** drop-down menu, or you can create a new template using **Add Rule** option and apply it. Refer to Create Prefiltering Policy Template for more details on how to create a new template. Click the **Save as Template** button to save the newly created template.
5. Click **Save** to apply the template to the Monitoring Session.

Enable Precryption

Rules and Notes

- To avoid packet fragmentation, you should change the option precryption-path-mtu in UCT-V configuration file (**/etc/uctv/uctv.conf**) within the range 1400-9000 based on the platform path MTU.
- 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.

NOTE: It is recommended to enable the secure tunnel feature whenever the Precryption feature is enabled. Secure tunnel helps to securely transfer the cloud captured packets or precrypted data to a GigaVUE V Series Node. For more detailed information refer to *Secure Tunnels* in in the respective GigaVUE Cloud Suite Deployment Guide.

To enable Precryption, follow the steps given below:

1. In the Monitoring Session **TRAFFIC ACQUISITION** page, click **Precryption** tab.
2. Enable the **Precryption** toggle button. Refer to Precryption™ topic for more details on Precryption.
3. You can apply Precryption to a few selective components based on the traffic:

   NOTE: If you wish to use Selective Precryption, your GigaVUE-FM and the fabric components version must be 6.8.00 or above.

   Applications:

   a. Click on the **APPLICATIONS** tab.
   b. The **Pass All Applications** is enabled by default. If you wish to use selective Precryption, disable this option.
   c. Select any one of the following options for **Actions**:
      i. Include: Select to include the traffic from the selected applications for Precryption.
      ii. Exclude: Select to exclude the traffic from the selected applications for Precryption.
   d. Click **Add**. The **Add Application** widget opens.
   e. Select **csv** as the **Type**, if you wish to add the applications using a .csv file. Click **Choose File** and upload the file.
   f. Select **Manual** as the **Type**, if you wish to add the applications manually. Enter the **Application Name** and click + icon to add more applications.
   g. Click **Apply**.

   L3-L4

   a. You can select an existing Precryption template from the **Template** drop-down menu, or you can create a new template and apply it. Refer to Create Precryption Template for UCT-V for more details on how to create a new template.
4. Enable the **Secure Tunnel** button if you wish to use Secure Tunnels. Refer to the *Configure Secure Tunnel* section in the respective GigaVUE Cloud Suite Deployment Guide.

Validate Precryption connection

To validate the Precryption connection, follow the steps:

- To confirm it is active, navigate to the **Monitoring Session** dashboard and check the Precryption option, which should show **yes**.
- Click **Status**, to view the rules configured.

Limitations

During Precryption, UCT-V generates a TCP message with the payload being captured in clear text. Capturing the L3/L4 details of this TCP packet by probing the SSL connect/accept APIs. The default gateway's MAC address will be the destination MAC address for the TCP packet when SSL data is received on a specific interface. If the gateway is incorrectly configured, the destination MAC address could be all Zeros.

TRAFFIC PROCESSING

To navigate to **TRAFFIC PROCESSING** tab, follow the steps given below:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a Monitoring Session from the Monitoring Sessions list view on the left side of the screen and click **TRAFFIC PROCESSING** tab.

You can perform the following actions in the **TRAFFIC PROCESSING** page:

- Apply Threshold Template
- Enable User Defined Applications
- Enable Distributed De-duplication

Apply Threshold Template

To apply threshold, follow the steps given below:

1. In the Monitoring Session **TRAFFIC PROCESSING** page, select **Thresholds** under **Options** menu.
2. Select the template you wish to apply from the drop-down. Click **Apply**. Refer to Traffic Health Monitoring section for more details on Threshold Template.

Enable User Defined Applications

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

1. In the Monitoring Session **TRAFFIC PROCESSING** page, click **User Defined Applications** under **Options** menu.
2. Enable the **User-defined Applications** toggle button. Refer to User Defined Application section in the GigaVUE V Series Applications Guide for more detailed information.

Enable Distributed De-duplication

Enabling the "Distributed De-duplication" option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring. Refer to Distributed De-duplication section for more details.

Notes:

- Distributed De-duplication is only supported on V Series version 6.5.00 and later.
- From version 6.9, Traffic Distribution option is renamed to Distributed De-duplication.

Create Ingress and Egress Tunnel (Nutanix)

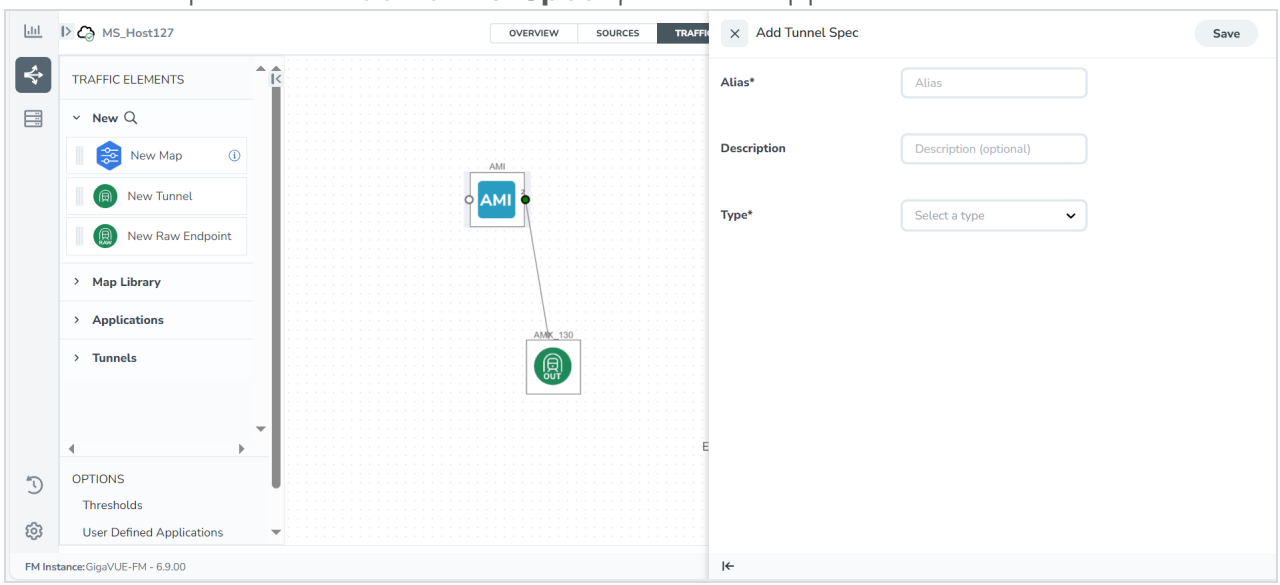
Traffic from the GigaVUE V Series Node is distributed to tunnel endpoints in a monitoring session. A tunnel endpoint can be created using a standard L2GRE, VXLAN, or ERSPAN tunnel.

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

To create a new tunnel endpoint:

1. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.

2. In the canvas, click the  icon on the left side of the page to view the traffic processing elements. 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	
Alias	The name of the tunnel endpoint.	
Description	The description of the tunnel endpoint.	
Admin State **NOTE:** This option appears only after the Monitoring session deployment.	Use this option to send or stop the traffic from GigaVUE-FM to the egress tunnel endpoint. Admin State is enabled by default. You can use this option to stop sending traffic to unreachable tools or tools that are in a down state. Each egress tunnel configured on the GigaVUE V Series Node has an administrative state that enables GigaVUE-FM to halt the tunnel's traffic flow. The tunnels will only be disabled by GigaVUE-FM when it receives a notification via REST API indicating that a tool or group of tools is down. **NOTE:** This option is not supported for TLS-PCAPNG tunnels.	
Type	The type of the tunnel. Select from the below options to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE.	
VXLAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **NOTE:** In the scenario where secure tunnels need to be established between a GigaVUE V Series Node and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device. Refer to the Secure Tunnels section.		
In	Choose **In** (Decapsulation) for creating an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	The 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	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose **Out** (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node to the destination endpoint.	

Field	Description	
	Remote Tunnel IP	For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that 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 being 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. The accepted value is between 0 and 1048575.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	The 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	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.

Field	Description	
	Source L4 Port	The 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	The 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.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **NOTE:** In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . Refer to the Secure Tunnels section.		
In	Choose **In** (Decapsulation)to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
Out	Choose **Out** (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint.	
	Remote Tunnel IP	For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that 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 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that

Field	Description	
		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. The accepted value is between 0 and 1048575.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
ERSPAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	**IP Version**	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **NOTE:** In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . Refer to the Secure Tunnels section.		
In	**IP Version**	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	The 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	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.

Field	Description	
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the 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.
Out	**IP Version**	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the 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) is a value that 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 being 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. The accepted value is between 0 and 1048575.
	Source L4 Port	The 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	The 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 Version 1.3.

Field	Description	
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.
UDP:		
Out	**L4 Destination IP Address**	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. Refer to Application Metadata Exporter for more detailed information.
	Source L4 Port	The 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	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.

4. Click **Save**.

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

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

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

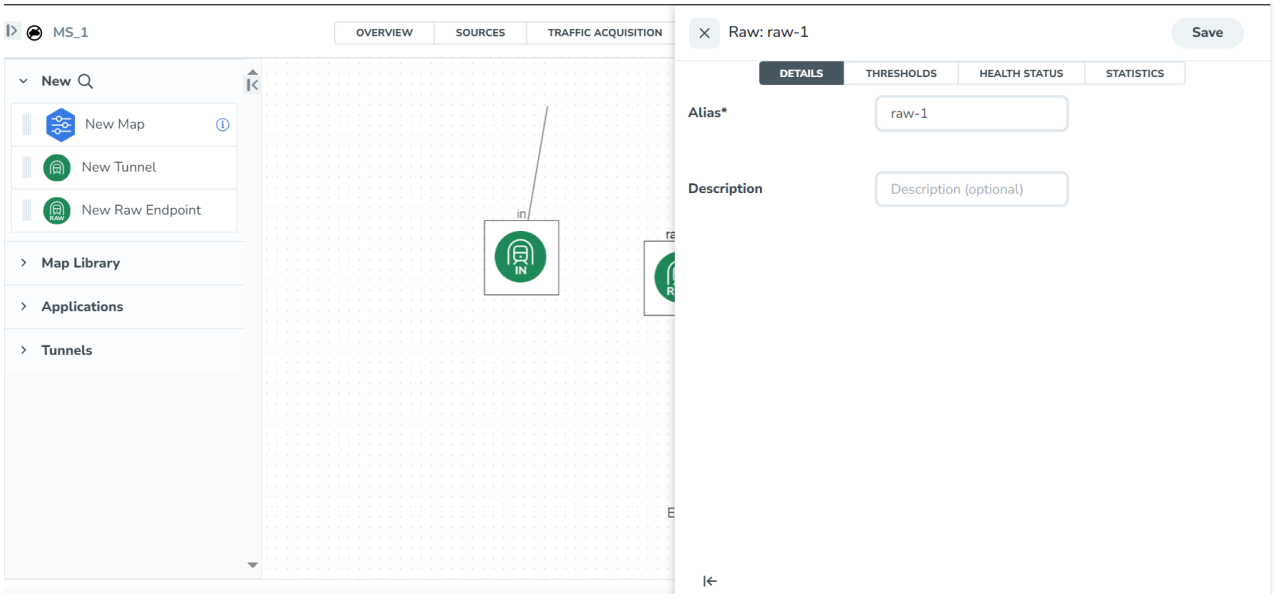
After configuring the tunnels and deploying the Monitoring Session, you can view the number of ingress and egress tunnels configured for a Monitoring Session. Click on the numbers of tunnels displayed to view the tunnel names and their respective **ADMIN STATUS** and **HEALTH STATUS**.

Create Raw Endpoint (Nutanix)

Raw End Point (REP) is used to pass traffic from an interface. REP is used to ingress data from a physical interface attached to GigaVUE V Series Nodes. You can optionally use this end point to send traffic to the applications deployed in the monitoring session.

To add Raw Endpoint to the monitoring session:

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



4. To deploy the monitoring session after adding the Raw Endpoint click the **Deploy** from the **Actions** drop-down menu on the Monitoring Session page.
5. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the V Series Nodes for which you wish to deploy the monitoring session.
6. After selecting the V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual V Series Nodes. Then, click **Deploy**.

Create a New Map

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

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

Keep in mind the following when creating a map:

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

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	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. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps** Below are the filter rule types that work in ATS: mac Source mac Destination ipv4 Source ipv4 Destination ipv6 Source ipv6 Destination VM Name Destination VM Name Source VM Tag Destination - Not applicable to Nutanix. VM Tag Source - Not applicable to Nutanix. VM Category Source - Applicable only to Nutanix VM Category Destination - Applicable only to Nutanix. Host Name -Applicable only to Nutanix and VMware. The traffic direction is as follow: For any rule type as Source - the traffic direction is egress. For Destination rule type - the traffic direction is ingress. For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. **Notes:** • For OpenStack environment, Subnet Name Source and Subnet Name Destination are the exclusion filters available as part of Exclusion Maps with Traffic Acquisition method as OVS Mirroring in the Monitoring Domain. • 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.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

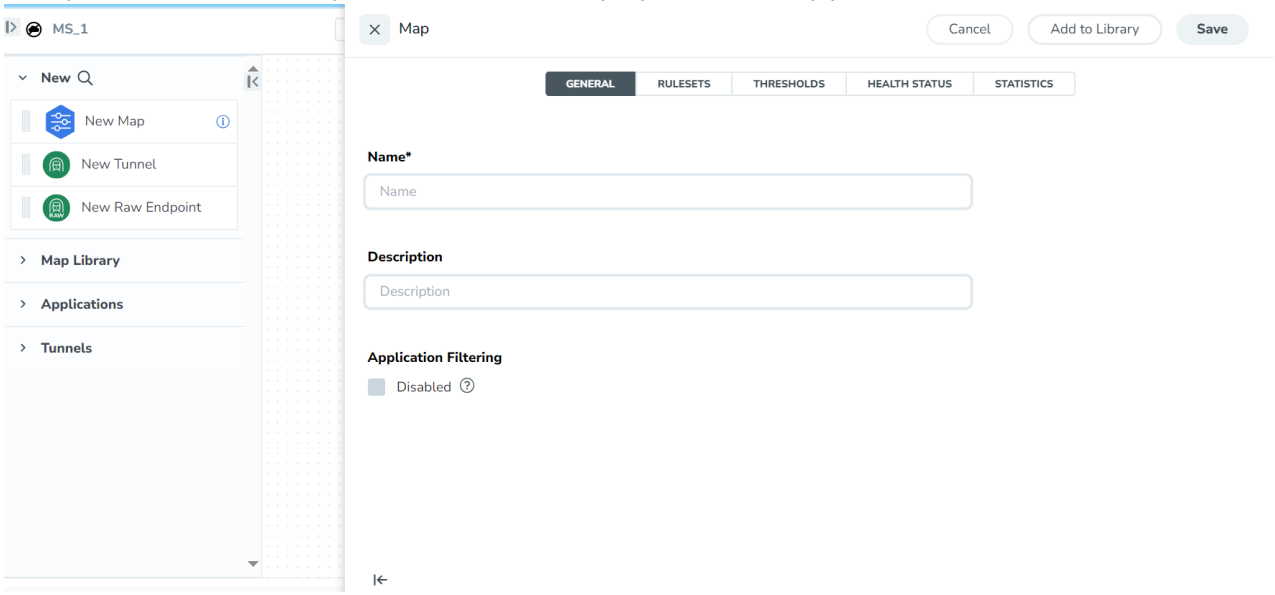
Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.
- Loopback captures bidirectional traffic from both ingress and egress. To prevent duplicate tapping, only egress tapping is permitted.
- If you are running GigaVUE Cloud Suite on OpenStack, you can add a subnet to the exclusion map. To do this, create an exclusion map and select the Subnet name in the ruleset.
- 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 "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide* for detailed information.

To create a new map:

1. After creating a new Monitoring Session, or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas appears.

2. In the canvas, click on the  icon expand icon on the left side of the page to view the traffic processing elements. 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
Name	Name of the new map
Description	Description of the map
Application Filtering	Enable this option if you wish to use Application Filtering Intelligence. Enabling this option allows you to filter traffic based on Application name or family. Refer to Application Filtering Intelligence for more details.

> 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**.

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 Thresholds tab. For more details on how to create or apply threshold templates, refer to Monitor Cloud Health.

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 **RULESETS** 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 **RULESETS**, 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 **RULESETS** 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 **TRAFFIC PROCESSING**. The GigaVUE-FM canvas page appears.
2. Click the map you wish to save as a template. Click **Details**. The Application quick view appears.
3. Click **Add to Library**. Select an existing group from the **Select Group** list or create a **New Group** with a name.
4. Enter a description in the **Description** field, and click **Save**.

The Map is saved to the **Map Library** in the **TRAFFIC PROCESSING** 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
- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- GENEVE Decap
- Header Stripping
- Application Metadata Exporter
- SSL Decrypt
- GigaSMART NetFlow Generation
- 5G-Service Based Interface Application
- 5G-Cloud Application

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

Interface Mapping (Nutanix)

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** landing page appears.
2. Navigate to **V SERIES NODES** tab and click **Interface Mapping**.
3. The **Deploy Monitoring Session** dialog box appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.

4. 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**.

NOTE: When using Raw and Tunnel In, Interface Mapping is mandatory before you deploy the Monitoring Session.

Deploy Monitoring Session

To deploy the Monitoring Session:

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

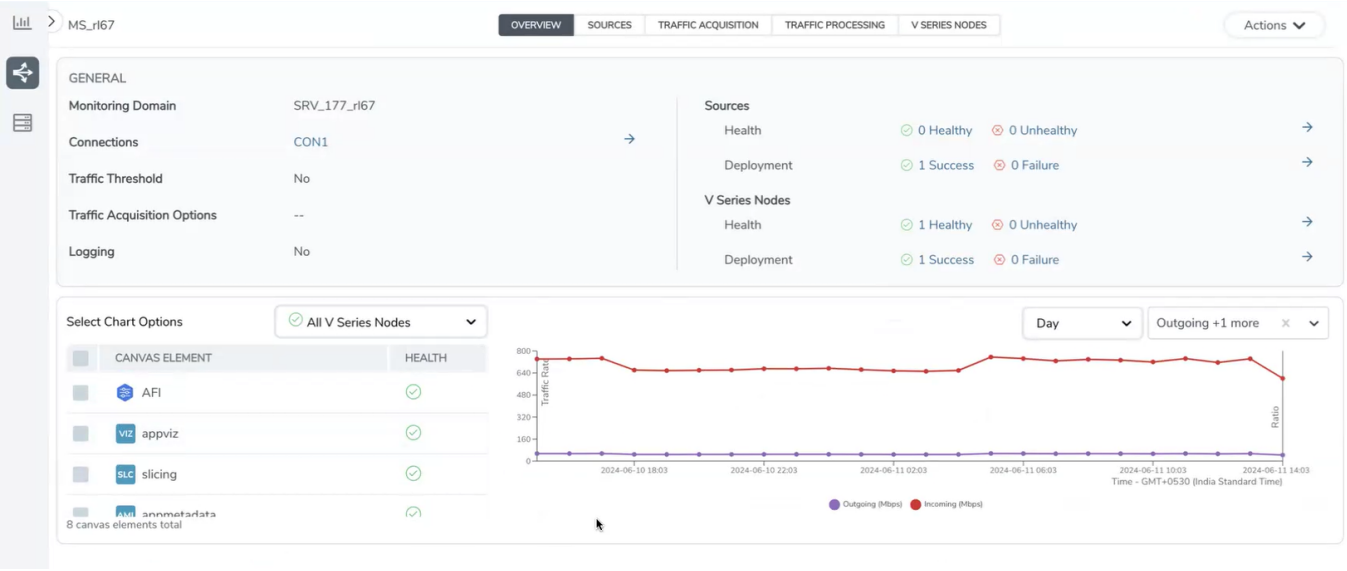
   NOTE: You can drag multiple arrows from a single map and connect them to different maps.
3. (Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method) Click **SOURCES** tab to view details about the subnets and monitored instances.
4. Click **Deploy** from the **Actions** menu 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.
5. You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab. 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.
   - 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 or Instances.

   The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

View Monitoring Session Statistics

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

You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab.



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

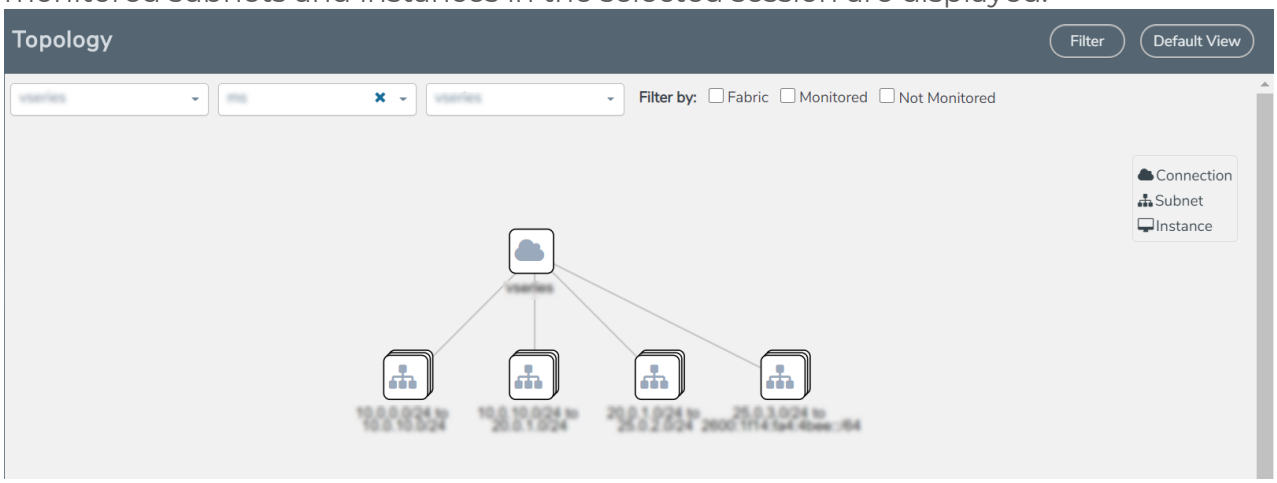
- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.
- You can filter the traffic and view the statistics based on factors such as **Incoming**, **Outgoing**, **Ratio (Out/In), Incoming Packets**, **Outgoing Packets**, **Ratio (Out/In) Packets**. You can select the options from the drop-down list box in the **TOTAL TRAFFIC** section of the **OVERVIEW** page.
- You can also view the statistics of the Monitoring Session deployed in the individual V Series Nodes. To view the statistics of the individual GigaVUE V Series Node, select the name of the **V Series Node** for which you want to view the statistics from the GigaVUE V Series Node drop-down list on the bottom left corner of the **OVERVIEW** page.

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.

Monitor Cloud Health

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

- Configuration Health Monitoring
- Traffic Health Monitoring
- View Health Status

Configuration Health Monitoring

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

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

Configuration Health Monitoring	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware	GigaVUE Cloud Suite for Nutanix
GigaVUE V Series Nodes	✓	✓	✓	✓	✓
UCT-V	✓	✓	✓	×	×
VPC Mirroring	✓	×	×	×	×
OVS Mirroring and VLAN Trunk Port	×	×	✓	×	×

To view the configuration health status, refer to the View Health Status section.

Traffic Health Monitoring

GigaVUE-FM allows you to monitor the traffic health status of the entire Monitoring Session and also the individual V Series Nodes for which the Monitoring Session is configured. Traffic health monitoring focuses on identifying any discrepancies (packet drop or overflow etc) in the traffic flow. When any such discrepancies are identified, GigaVUE-FM propagates the health status to corresponding Monitoring Session. GigaVUE-FM monitors the traffic health

status in near real-time. GigaVUE V Series Node monitors the traffic, when the traffic limit goes beyond the upper or lower threshold values that is configured, it notifies GigaVUE-FM, based on which traffic health is computed.

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

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

For V Series Nodes:

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

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

- Supported Resources and Metrics
- Create Threshold Templates
- Apply Threshold Template
- Clear Thresholds

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

- By default, Threshold Template is not configured to any Monitoring Session. If you wish to monitor the traffic health status, then create and apply threshold template to the Monitoring Session.
- Editing or redeploying the Monitoring Session will reapply all the threshold policies associated with that Monitoring Session.
- Deleting or undeploying the Monitoring Session will clear all the threshold policies associated with that Monitoring Session.
- After applying threshold template to a particular application, you need not deploy the Monitoring Session again.

Supported Resources and Metrics

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

Resource	Metrics	Threshold types	Trigger Condition
Tunnel End Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors	1. Difference 2. Derivative	1. Over 2. Under
RawEnd Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors	1. Difference 2. Derivative	1. Over 2. Under
Map	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Slicing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Masking	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Dedup	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
HeaderStripping	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
TunnelEncapsulation	1. Tx Packets	1. Difference	1. Over

	2. Rx Packets 3. Packets Dropped	2. Derivative	2. Under
LoadBalancing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SSLDecryption	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Application Metadata	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
AMI Exporter	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
5G-SBI	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SBIPOE	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
PCAPNG	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

Create Threshold Templates

To create threshold templates:

1. Go to **Inventory > Resouces > Threshold Templates**.
2. The **Threshold Templates** page appears. Click Create to open the New Threshold Template page.
3. Enter the appropriate information for the threshold template as described in the following table.

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

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

Apply Threshold Template

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

Apply Threshold Template to Monitoring Session

To apply the threshold template across a Monitoring Session, follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. In the **TRAFFIC PROCESSING** tab, select **Thresholds** under **Options** menu.
3. To apply a threshold template across a Monitoring Session, select the template you wish to apply across the Monitoring Session from the Threshold Template drop-down

menu.

4. Click **Apply**.

Apply Threshold Template to Applications

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

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

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

Clear Thresholds

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

Clear Thresholds for Applications

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

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

Clear Thresholds across the Monitoring Session

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

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Select the Monitoring Session and navigate to **TRAFFIC PROCESSING > Options > Thresholds**, click **Clear Thresholds**.
3. The **Clear Threshold** pop-up appears. Click **Ok**.

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

View Health Status

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

View Health Status of an Application

To view the health status of an application across an entire Monitoring Session:

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

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

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

View Health Status for Individual GigaVUE V Series Nodes

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

1. On the Monitoring Session page, click the required Monitoring Session from the list view.
2. In the **Overview** tab, you can view the health status of the required GigaVUE V Series Node from the chart options.

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics[1] 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 section in *GigaVUE Fabric Management Guide* for more detailed information on Analytics.

Rules and Notes:

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

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

The following table lists the various virtual dashboards:

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

Dashboard	Displays	*Visualizations*	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: • Number of Monitoring Sessions • Number of V Series Nodes • Number of Connections • Number of GCB Nodes You can filter the visualizations based on the following control filters: • Platform • Health Status	*V Series Node Status by Platform*	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		Monitoring Session Status by Platform	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		Connection Status by Platform	Number of healthy and unhealthy connections for each of the supported cloud platforms
		GCB Node Status by Platform	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*V Series Node Maximum CPU Usage Trend*	Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour. **NOTE:** The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V Series nodes do not have service cores, therefore the CPU usage is reported as 0.
		V Series Node with Most CPU Usage For Past 5 minutes	Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes. **NOTE:** You cannot use the time based filter

Dashboard	Displays	*Visualizations*	Displays
			options to filter and visualize the data.
		V Series Node Rx Trend	Receiving trend of the V Series node in 5 minutes interval, for the past one hour.
		V Series Network Interfaces with Most Rx for Past 5 mins	Total packets received by each of the V Series network interface for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.
		V Series Node Tunnel Rx Packets/Errors	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.
		V Series Node Tunnel Tx Packets/Errors	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*Dedup Packets Detected/Dedup Packets Overload*	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload.
		Dedup Packets Detected/Dedup Packets Overload Percentage	Percentage of the de-duplicated packets received against the de-duplication application overload.
		Total Traffic In/Out Dedup	Total incoming traffic against total outgoing

Dashboard	Displays	*Visualizations*	Displays
			traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session**: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V Series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. • **V Series node**: Management IP of the V Series node. Choose the required V Series node from the drop-down. • **Tunnel:** Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. The following statistics are displayed for the tunnel: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets	*Tunnel Bytes*	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes. • For input tunnel, transmitted traffic is displayed as zero. • For output tunnel, received traffic is displayed as zero.
		Tunnel Packets	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
App (Virtual)	Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V Series node.	*App Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	*Visualizations*	Displays
	You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session** • **V Series node** • **Application**: Select the required application. By default, the visualizations displayed includes all the applications. By default, the following statistics are displayed: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Errored Packets • Dropped Packets		
		App Packets	Displays received traffic vs transmitted traffic, as the number of packets.
End Point (Virtual)	Displays Byte and packet level statistics for the un-tunneled traffic deployed on the V Series nodes. The following statistics that are shown for Endpoint (Virtual): • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets The endpoint drop-down shows *<V Series Node Management IP address : Network Interface>* for each endpoint.	*Endpoint Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	*Visualizations*	Displays
	You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session** • **V Series node** • **Endpoint:** Management IP of the V Series node followed by the Network Interface (NIC)		
		Endpoint Packets	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.

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
Physical Device Infrastructure Management: This includes the following cloud infrastructure resources: • Cloud Connections • Cloud Fabric Deployment • Cloud Configurations • Sys Dump • Syslog • Cloud licenses • Cloud Inventory	• Configure GigaVUE Cloud Components • Create Monitoring Domain and Launch Visibility Fabric
Traffic Control Management: This includes the following traffic control resources: • Monitoring session • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps	• Create, Clone, and Deploy Monitoring Session • Add Applications to Monitoring Session • Create Maps • View Statistics • Create Tunnel End Points

NOTE: Cloud APIs are also RBAC enabled.

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

About Events

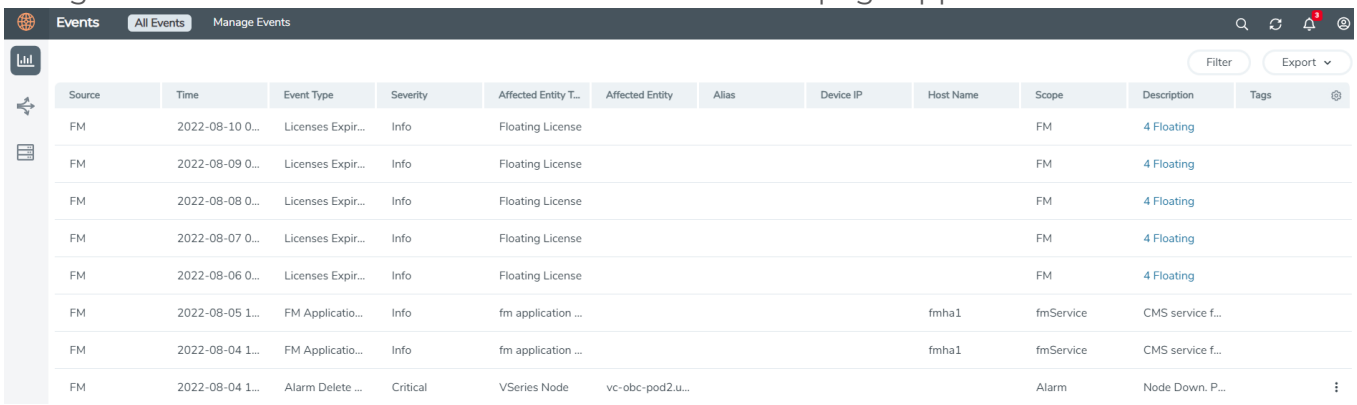
The Events page displays all the events occurring in the virtual fabric component, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- 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.



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
Source	The source from where the events are generated. The criteria can be as follows: ▪ FM - indicates the event was flagged by the GigaVUE-FM fabric manager. ▪ VMM - indicates the event was flagged by the Virtual Machine Manager. ▪ FM Health - indicates the event was flagged due to the health status change of GigaVUE-FM.
Duration	The timestamp when the event occurred or the duration in which the event occured. **IMPORTANT:**Timestamps or the duration 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.
Scope	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.
Alarm Type	The type of events that generate the alarms. The types of alarms can be Abnormal Fan Operation, Card Unhealthy, Circuit Tunnel Unhealthy, CPU Over Loaded, Device Upgrade Failed.
Event Severity	The severity is one of Critical, Major, Minor, Warning or Info. Info is informational messages. For example, when power status change notification is displayed, then the message is displayed as Info.
Event Status	The status of the event. The status can be Acknowledged or Unacknowledged.
Event Type	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 generation statistics, and so on.
Affected Entity Type	The resource type associated with the event. For example, when low disk space notification is generated, 'Chassis' is displayed as the affected entity type.

Controls/ Parameters	Description
Cluster ID	Enter the Cluster ID.
Affected Entity	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.
Device IP	The IP address of the device.
Host Name	The host name of the device.
Alias	Event Alias
Monitoring Domain	The name of the Monitoring Domain.
Connection	The name of the Connection.
Show Non-taggable Entities	Enable to display the events for entities that cannot be tagged. For example, Policies, GigaVUE-FM instance and other such entities.
Tags	Select the Key and the Value from the drop-down list.

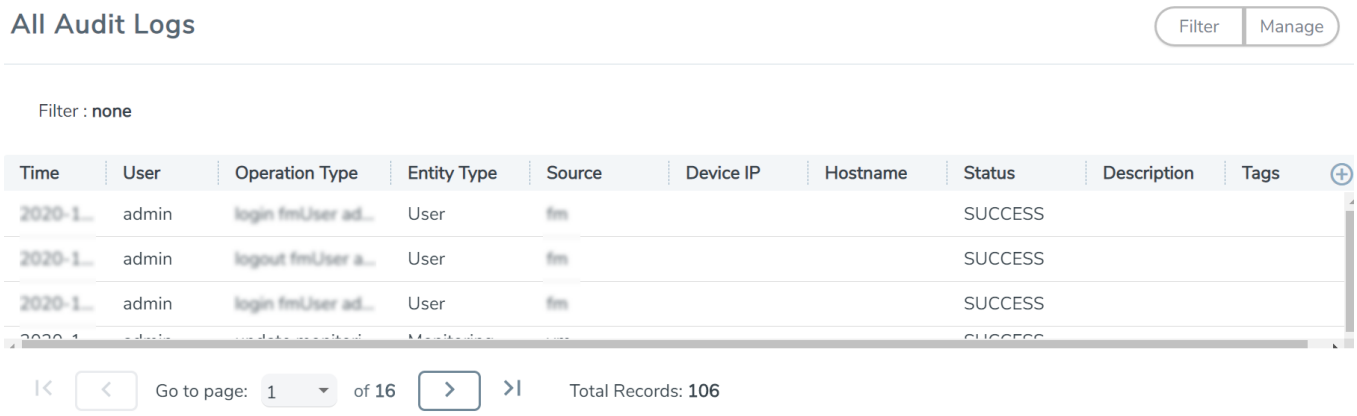
To filter the alarms and event:

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.



The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: ▪ Log in and Log out based on users. ▪ Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details on whether the user was in GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	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 VÜE Community

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.8 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide

GigaVUE Cloud Suite 6.8 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud TAP - Container Deployment Guide

GigaVUE Cloud Suite 6.8 Hardware and Software Guides
Gigamon Containerized Broker Deployment Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices Sanitization guidelines for GigaVUE Fabric Management Guide and GigavUE-OS devices.
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The VÜE Community

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

Visit the VÜE Community site to:

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

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)