Gigamon®

GigaVUE Cloud Suite Deployment Guide - OpenStack

GigaVUE Cloud Suite

Product Version: 6.13

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
6.13	1.0	02/25/2026	The original release of this document with 6.13.00 GA.

Contents

GigaVUE Cloud Suite Deployment Guide - OpenStack

This guide describes how to install, configure and deploy the GigaVUE Cloud solution on OpenStack. Use this document for instructions on configuring the GigaVUE Cloud components and setting up the traffic monitoring sessions for OpenStack.

Refer to the following sections for details:

Overview of GigaVUE Cloud Suite for OpenStack

GigaVUE-FM fabric manager is a web-based fabric management interface that provides a single-pane-of-glass visibility and management of both the physical and virtual traffic. GigaVUE-FM is a key component of the GigaVUE Cloud Suite for OpenStack.

The OpenStack software is designed for multi-tenancy (multiple projects), where a common set of physical compute and network resources are used to create project domains that provide isolation and security. Characteristics of a typical OpenStack deployment include the following:

- Projects are unaware of the physical hosts on which their instances are running.
- A project can have several virtual networks and may span across multiple hosts.

In a multi-project OpenStack cloud, where project isolation is critical, the Gigamon solution extends visibility for the project's workloads without impacting others by doing the following:

- Support project-wide monitoring domains—a project may monitor any of its instances.
- Honor project isolation boundaries—no traffic leakage from one project to any other project during monitoring.
- Monitor traffic without needing cloud administration privileges. There is no requirement to create port mirror sessions and so on.
- Monitor traffic activity of one project without adversely affecting other projects.

Refer Deploying Gigamon CloudSuite on OpenStack to scale-inand Open vSwitch with Hardware offload and scale-out monitoring tools for more detailed information.

GigaVUE-FM

GigaVUE-FM fabric manager provides unified access, centralized administration, and high-level visibility for all GigaVUE traffic visibility nodes in the enterprise or data center, allowing a global perspective which is not possible from individual nodes.

In addition to centralized management and monitoring GigaVUE-FM helps you with configuration of the physical and virtual traffic policies for the visibility fabric thereby allowing administrators to map and direct network traffic to the tools and analytics infrastructure.

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

UCT-V

Universal Cloud Tap - Virtual Machine(**UCT-V**) (earlier known as G-vTAP Agent) is a standalone service that is installed in the VM instance. UCT-V mirrors the selected traffic from the instances (virtual machines) to the GigaVUE V Series Node. The UCT-V is offered as a Debian (.deb), Redhat Package Manager (.rpm) package, ZIP and MSI .

Next generation UCT-V is a lightweight solution that acquires traffic from Virtual Machines and in-turn improves the performance of the UCT-V mirroring capability. The solution has a prefiltering capability at the tap level that reduces the traffic flow from the UCT-V to

GigaVUE V Series Node and in-turn reduces the load on the GigaVUE V Series Node. Next generation UCT-V gets activated on Windows and also on Linux systems with a Kernel version above 4.18.

Prefiltering helps you reduce the costs significantly. It allows you to filter the traffic at UCT-Vs before sending it to the GigaVUE V Series Node. For prefiltering the traffic, GigaVUE-FM allows you to create a prefiltering policy template and the template can be applied to a monitoring session.

For more information on installing the UCT-V see Install UCT-V.

UCT-V Controller

UCT-V Controller (earlier known as G-vTAP Controller) manages multiple UCT-Vs and orchestrates the flow of mirrored traffic to GigaVUE V Series Nodes. GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs. A UCT-V Controller can only manage UCT-Vs that has the same version. For example, the UCT-V Controller 6.13.00 can only manage UCT-Vs 6.13.00. If you have the previous version of UCT-V still deployed in the Virtual Network, you must configure both UCT-V Controller 6.13.00 and the previous version. While configuring the UCT-V Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the UCT-Vs to the GigaVUE V Series Nodes.

NOTE: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

GigaVUE V Series Node

GigaVUE® V Series Node is 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 backhaul to on premise device or tools. GigaVUE Cloud Suite for AWS uses the TLS-PCAPNG, ERSPAN, L2GRE, UDPGRE and, VXLAN tunnels to deliver traffic to tool endpoints.

NOTE: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

For more information on installing and configuring a GigaVUE V Series Node, refer to Configure GigaVUE Fabric Components in GigaVUE-FM.

GigaVUE V Series Proxy

GigaVUE V Series Proxy manages multiple GigaVUE V Series nodes and orchestrates the flow of traffic from GigaVUE V Series nodes to the GigaVUE-FM. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series nodes.

NOTE: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

For more information on installing and configuring a GigaVUE V Series Proxy, refer to Configure GigaVUE Fabric Components in GigaVUE-FM.

Monitoring Domain

Monitoring domain helps you establish connection in between GigaVUE-FM and AWS platform. Once the connection is established, you can use GigaVUE-FM to launch the GigaVUE V Series Nodes, GigaVUE V Series Proxy and UCT-V Controller.

For more information on creating a Monitoring Domain, see Create Monitoring Domain.

Monitoring Session

Monitoring sessions are the rules created in GigaVUE-FM to collect inventory data from all target instances in your cloud environment. You can design your monitoring session to include or exclude the instances 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 more information on creating a monitoring session, see Configure Monitoring Session.

Cloud Overview Page (OpenStack)

The Overview page lets you view and manage all Monitoring Sessions in one place. You can quickly find issues to help with troubleshooting or take simple actions like viewing, editing, cloning, or deleting sessions.

This page shows key information at a glance, including:

- Basic statistics
- V Series alarms
- Connection status
- Volume usage vs. allowance
- A summary table of active monitoring sessions

You can edit a Monitoring Session directly from this page without switching to each platform's session page.

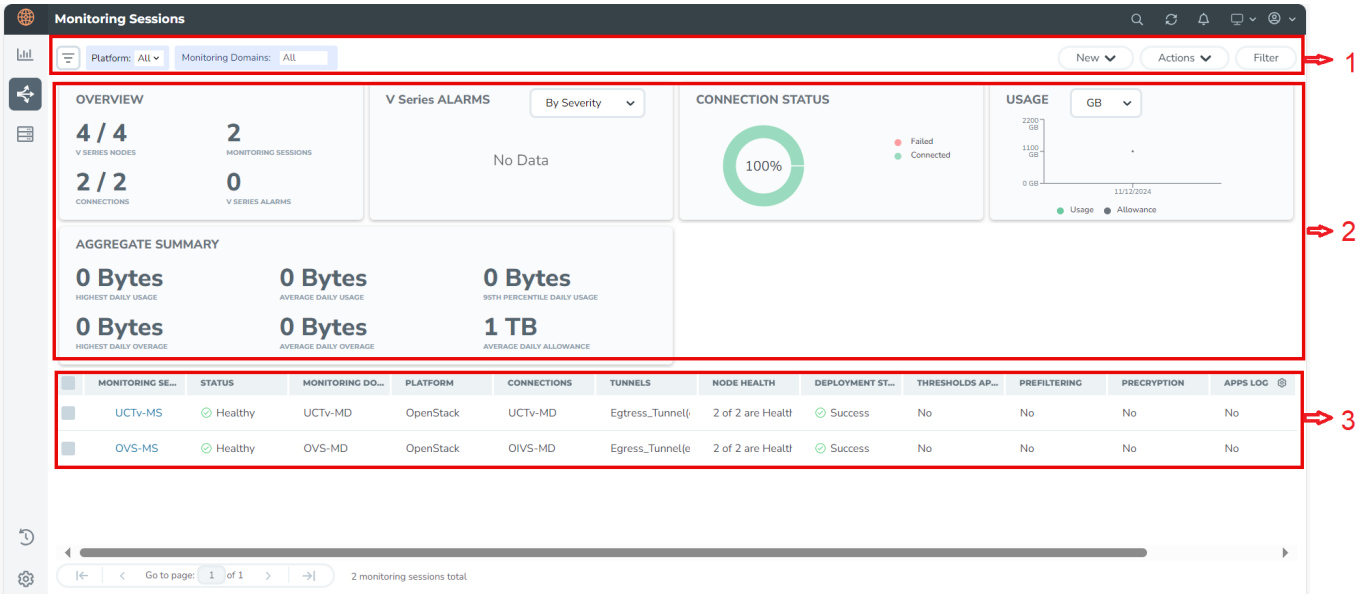
How to Access the Overview Page

You can access the overall Cloud overview or the platform-specific Cloud overview.

Perform one of the following:

- Go to Traffic > Virtual > Overview for the overall cloud overview page.
- For the Platform-specific cloud overview details:
    1. Go to Traffic > Virtual > Overview.
    2. On the top-left menu from the Platform drop-down option, select the name of your cloud.

The **Monitoring Sessions** page appears.



Page Layout for Easy Use

The page is split into three main sections for easier navigation, as displayed in the screenshot and explained in the following table:

Number	Section	Description
1	Top Menu	Refer to Cloud Overview Page (OpenStack).
2	Charts	Refer to Cloud Overview Page (OpenStack).
3	Monitoring Session Details	On the Overview page, you can view the Monitoring Session details of all the cloud platforms. For details, refer to the Cloud Overview Page (OpenStack) section.

Top Menu

The Top menu consists of the following options:

Options	Description
New	Allows to create a new Monitoring Session and new Monitoring Domain.
Actions	Allows the following actions: • **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. For details, refer to the *Monitor Cloud* section. • **Apply Policy:** Enables functions like Precryption, Prefiltering, or Secure Tunnel.
Filter	You can filter the Monitoring Session details based on a criterion or a combination of criteria. For more information, refer to Cloud Overview Page (OpenStack).

Filters

On the Monitoring Sessions page, you can apply the filters using the following options:

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

Filter on the left corner

1. From the **Platform** drop-down list, select the required platform.
2. Select 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 Filter

Use this filter to narrow down results with one or more of the following:

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

Viewing Charts on the Overview Page

You can view the following charts on the overview page:

- Overview
- V Series Alarms
- Connection Status
- Usage
- Aggregate Summary

Overview

This chart shows:

- The number of active GigaVUE V Series Nodes.
- The number of configured Monitoring Sessions and connections.
- The number of V Series alarms triggered.

V Series Alarms

This widget uses a pie chart to display V Series alarms.

- Each alarm type has its own color that is visible in the legend.
- Hover over a section to see the total number of alarms triggered.

Connection Status

This pie chart shows the status of connections in a Monitoring Domain.

- Successful and failed connections are marked in different colors.
- Hover over a section to view the total number of connections.

Usage

The Usage chart shows daily traffic volume through the V Series Nodes.

- Each bar represents one day's usage.
- Hovering over a bar helps you see the volume used and the limit for that day.

Aggregate Summary

This summary shows key volume usage stats:

- Highest daily volume usage
- Average daily volume usage
- Highest daily over-usage
- Average daily over-usage
- 95th percentile daily usage
- Average daily volume allowance

Viewing Monitoring Session Details

The overview table shows key details about each monitoring session. You can use this table to check session health, view settings, or take actions quickly.

Details	Description
Monitoring Sessions	Displays the name of each session. Select a name to open the Monitoring Session's page in the selected cloud platform.
Status	Displays the Health status of the Monitoring Session.
Monitoring Domain	Displays the name of the Monitoring Domain to which the Monitoring Session is associated.
Platform	Indicates the Cloud platform in which the session is created.
Connections	Displays Connection details of the Monitoring Session.

Details	Description
Tunnels	Lists the Tunnel details related to the Monitoring Session.
Node Health	Displays the Health status of the GigaVUE V Series Node.
Deployment Status	Displays the status of the deployment.
Threshold Applied	Specifies if the threshold is applied.
Prefiltering	Specifies if Prefiltering is configured.
Precryption	Specifies if Precryption is configured.
APPS logging	Specifies if APPS logging is configured.
Traffic Mirroring	Specifies if Traffic Mirroring is configured.

NOTE: Select the settings icon and customize the options visible in the table.

Introduction to the Supported Features for OpenStack

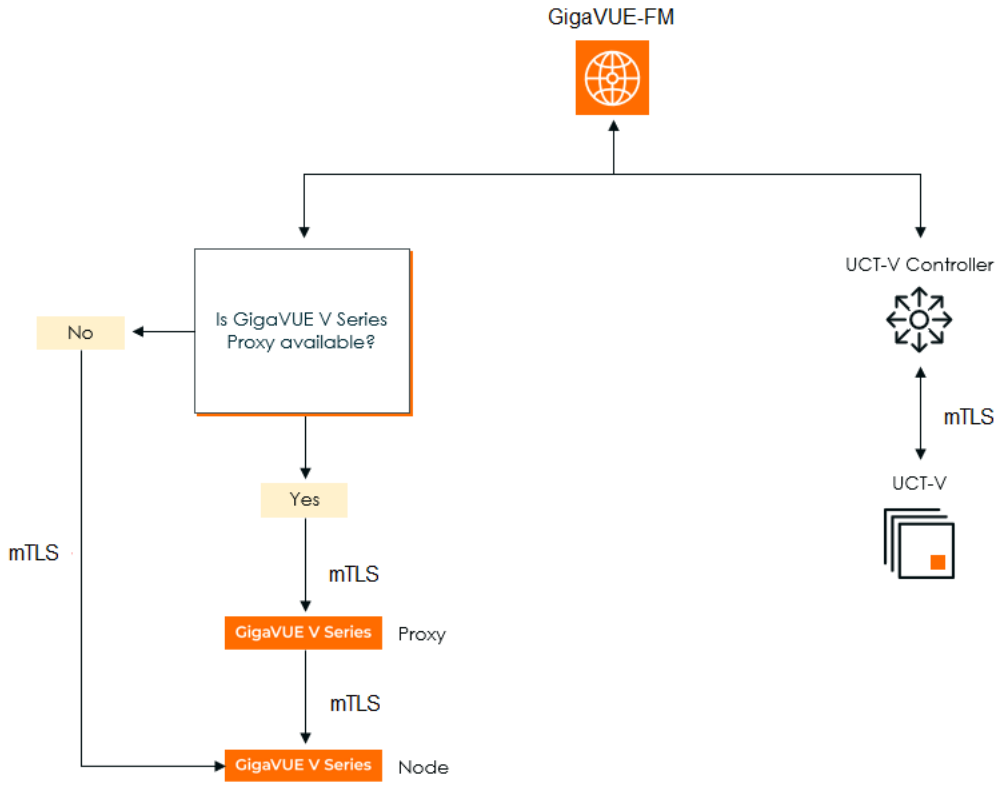
GigaVUE Cloud Suite for OpenStack supports the following features:

- Precryption™
- Secure Tunnels
- Prefiltering
- Load Balancer
- Analytics for Virtual Resources
- Traffic Health Monitoring

Secure Communication between GigaVUE Fabric Components

The Secure Communication feature in GigaVUE-VM uses mutual TLS (mTLS) authentication to improve network security. It ensures all GigaVUE Fabric Components communicate over encrypted, verified connections using certificates issued by a Certificate Authority (CA), without relying on static credentials.

How it Works!



In this setup:

- GigaVUE-FM establishes an mTLS connection and checks for GigaVUE V Series Proxy availability.
- If GigaVUE V Series Proxy is unavailable, it directly connects to the GigaVUE V Series Node through mTLS.
- If a GigaVUE V Series is available, GigaVUE-FM first connects to the GigaVUE V Series Proxy and establishes an mTLS connection with the GigaVUE V Series Node.
- GigaVUE-FM also initiates an mTLS connection to theUCT-V Controller, establishing an mTLS connection with UCT-V.

  This structured flow ensures secure communication using mTLS-based authentication across all the fabric components.

GigaVUE-FM acts as the PKI

GigaVUE-FM manages all certificates for fabric components. It acts as a private PKI and uses Step-CA with the ACME protocol to issue and renew certificates. This automated process reduces the need for manual certificate handling and avoids external dependencies.

Bring Your Own CA

If your organization already uses a corporate CA, you can import those certificates into GigaVUE-FM. This allows your existing PKI infrastructure to work with Gigamon's secure communication system.

For more details on how to integrate your PKI infrastructure with GigaVUE-FM, refer to Integrate Private CA

Secure Communication in FMHA Mode

In FMHA (Fabric Manager High Availability) mode:

- The active GigaVUE-FM instance shares intermediate CA files with all standby nodes.
- Only the active instance handles certificate requests. In case of a failover, a standby node takes over.
- The root and intermediate CAs are copied to all nodes to ensure continuity.
- If an instance is removed, it generates a new self-signed CA on restart.

Supported Platforms

- AWS
- Azure
- OpenStack
- Nutanix
- Third Party Orchestration
- VMware ESXi
- VMware NSX-T

Supported Components

- GigaVUE V Series Node
- GigaVUE V Series Proxy
- UCT-V
- UCT-V Controller

Rules and Notes

- If a public IP is revoked in public cloud platforms, you can issue a new certificate to remove the old IP.
- This feature is optional.
- Ensure NTP (Network Time Protocol) runs if GigaVUE-FM and components are on different hosts.
- Applying a certificate may temporarily cause a component to show as Down, but it recovers automatically.
- In AWS, disable the Source/Destination Check on network interfaces for GigaVUE V Series Proxy.

  Note: Enabling this check may block traffic if the IP address does not match the associated interface.

Precryption™

License: Precryption requires a **SecureVUE Plus** license.

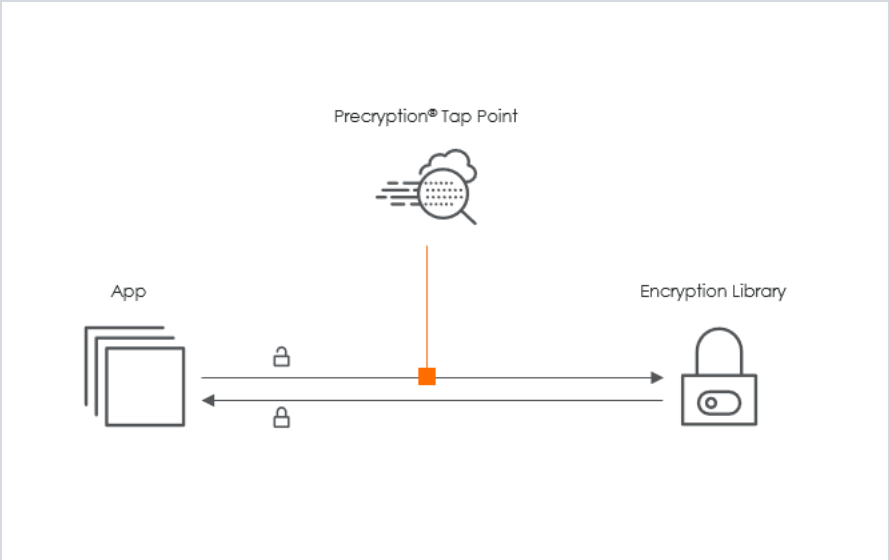
Gigamon Precryption™ technology[1] provides you clear-text visibility into encrypted network traffic without the need for traditional decryption. It works across virtual, cloud, and container environments, helping you get the full security stack without added complexity

In this section:

[1] **Disclaimer**: The Precryption feature allows you to capture decrypted traffic from both virtual machine (VM) and container-based environments. After capturing the traffic using (via UCT-C or UCT-V), you can send to the V Series product for further processing. You can choose to secure this traffic using encrypted tunnels between the capture point and the V Series. This option helps protect sensitive data during transit. If you don't enable encrypted tunnels, the captured (decrypted) traffic remains in plain text while moving between the source and the V Series—introducing potential exposure risks. Please note that the feature behavior and security options may change over time. Stay informed about updates to ensure you use the latest protections. By using this feature, you acknowledge and accept the current limitations and potential risks associated with the transmission of decrypted traffic.

How Gigamon Precryption Technology Works

Precryption technology leverages built-in Linux functionality to copy communications between the application and the encryption library, such as OpenSSL.



Key Highlights

- Captures network traffic in plain text, either before the system encrypts it or after it decrypts it.
- Does not change how encryption or transmission works.
- Avoids proxies, retransmissions, and “break-and-inspect” steps. Instead, it sends the plaintext copy to the Gigamon Deep Observability Pipeline, where tools can optimize, transform, and forward the traffic as needed.
- Runs on GigaVUE® Universal Cloud Tap (UCT) and supports hybrid and multi-cloud environments, including on-prem and virtual platforms.
- Runs independently of your applications, so you don’t need to change your development lifecycle.

Why Gigamon Precryption

GigaVUE Universal Cloud Tap with Precryption technology is a lightweight, friction-free solution that eliminates blind spots present in modern hybrid cloud infrastructure.

Precryption helps you:

- Improve visibility for East-West traffic into virtual, cloud, and container platforms
- Delivers unobscured visibility into all encryption types, including TLS 1.3, without managing and maintaining decryption keys.
- Manages compliance with IT organizations, keeps communications private, architects a Zero Trust foundation, and boosts security-tool effectiveness by a factor of 5x or more.

Key Features

The following are the key features of this technology:

- Plain text visibility into communications with modern encryption (TLS 1.3, mTLS, and TLS 1.2 with Perfect Forward Secrecy).
- Plain text visibility into communications with legacy encryption (TLS 1.2 and earlier).
- Non-intrusive traffic access without agents running inside container workloads.
- Elimination of expensive resource consumption associated with traditional traffic decryption.
- Elimination of key management required by traditional traffic decryption.
- Zero performance impact based on cipher type, strength, or version.
- Support across hybrid and multi-cloud environments, including on-prem, virtual, and container platforms.
- Keep private communications private across the network with plaintext threat activity delivered to security tools.
- Integration with Gigamon Deep Observability Pipeline for the full suite of optimization, transformation, and brokering capabilities.

Key Benefits

The following are the key benefits of this technology:

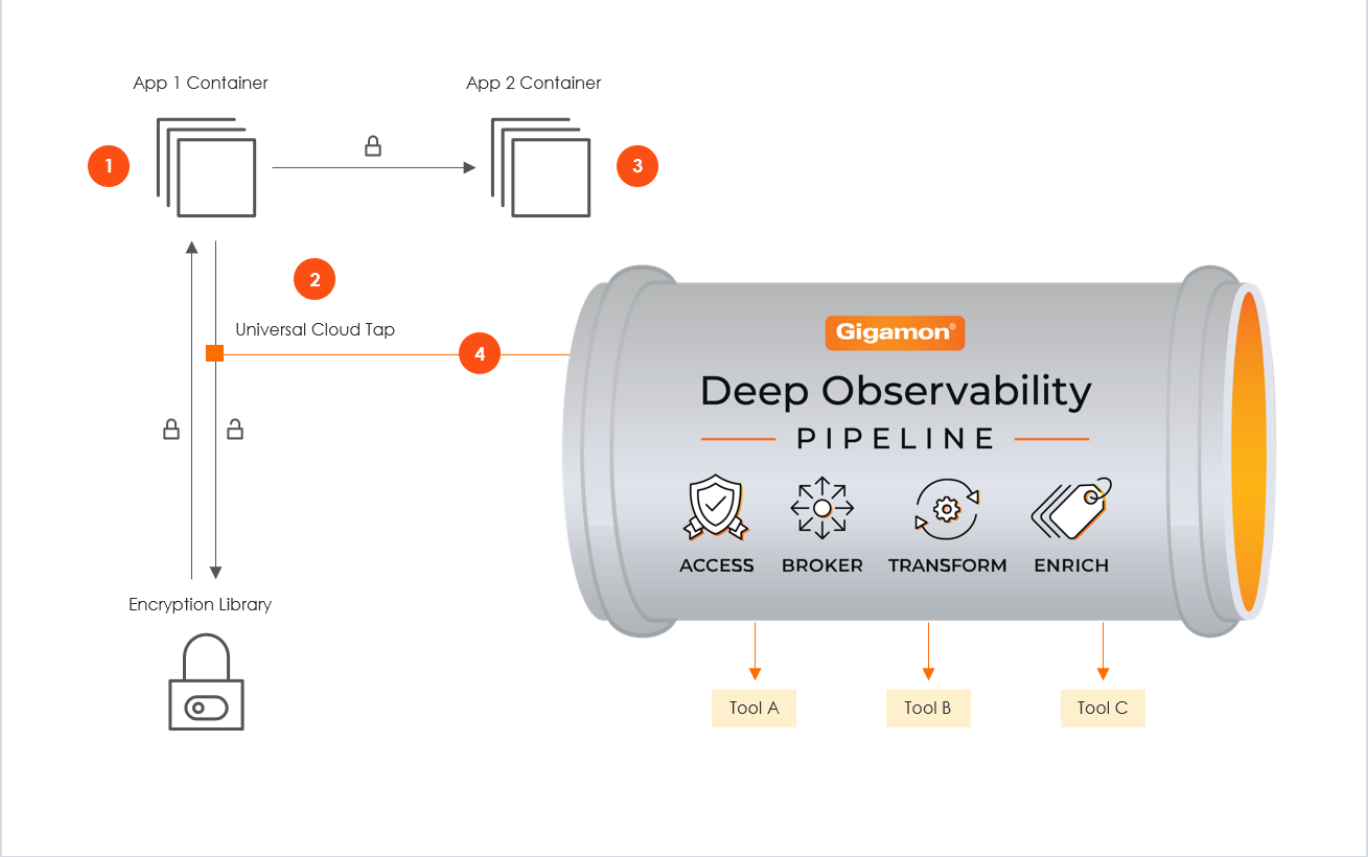
- Eliminates blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.
- Monitors application communications with an independent approach that enhances development team velocity.
- Extends security tools' visibility to all communications, regardless of encryption type.
- Achieves maximum traffic tapping efficiency across virtual environments.
- Leverages a 5–7x performance boost for security tools by consuming unencrypted data.
- Supports a Zero Trust architecture founded on deep observability.
- Maintains privacy and compliance adherence associated with decrypted traffic management.

How Gigamon Precryption Technology Works

This section explains how Precryption technology works on single nodes and multiple nodes in the following sections:

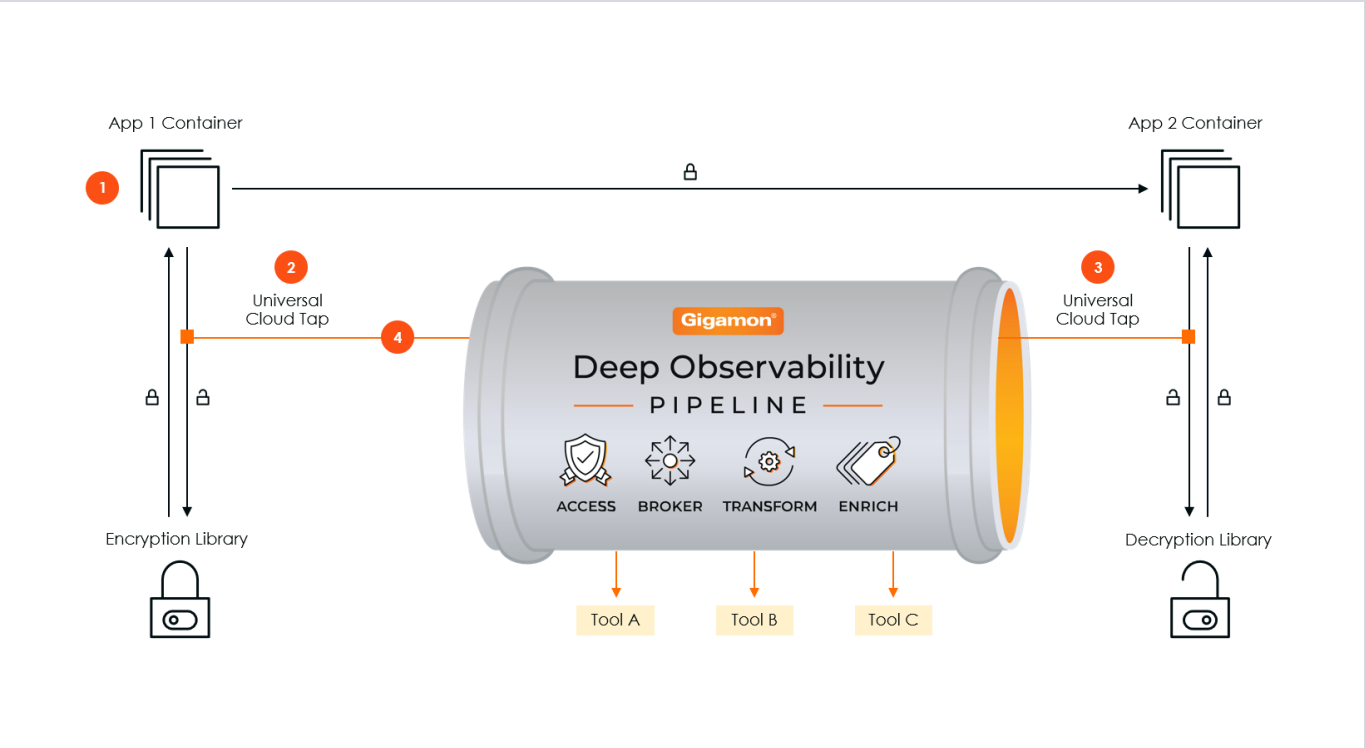
- Precryption Technology on Single Node
- Precryption Technology on Multi-Node

Precryption Technology on Single Node



1. An application uses an encryption library, such as OpenSSL, to encrypt a message.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption technology, gets a copy of this message before it is encrypted on the network.
3. The encrypted message is sent to the receiving application with unmodified encryption—no proxy, no re-encryption, no retransmissions.
4. GigaVUE UCT creates packet headers as needed, encapsulates them in a tunnel, and forwards them to GigaVUE V Series in the deep observability pipeline.
5. Gigamon optimizes, transforms, and delivers data to tools without further decryption.

Precryption Technology on Multi-Node



1. An application uses an encryption library, such as OpenSSL, to encrypt a message.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption technology, gets a copy of this message before it is encrypted on the network
3. Optionally, GigaVUE UCT enabled with Precryption can also acquire a copy of the message from the server end after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates them in a tunnel, and forwards them to GigaVUE V Series in the deep observability pipeline.
5. Gigamon optimizes, transforms, and delivers data to tools without further decryption.

Supported Platforms

VM environments: Precryption™ is supported on the following VM platforms that support UCT-V:

Platform Type	Platform
Public Cloud	• AWS • Azure • GCP (via Third Party Orchestration)
Private Cloud	• OpenStack • VMware ESXi (via Third Party Orchestration only) • VMware NSX-T (via Third Party Orchestration only) • Nutanix (via Third Party Orchestration only)

Container environments: Precryption™ is supported on the following container platforms that support UCT-C:

Platform Type	Platform
Public Cloud	• EKS • AKS • GKE
Private Cloud	• OpenShift • Native Kubernetes (VMware)

Prerequisites

Points to Note

- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x.
- For UCT-C, worker pods should always have libssl installed to ensure that UCT-C Tap can tap the Precryption packets from the worker pods whenever libssl calls are made from the worker pods.
- For GigaVUE-FM, add port 5671 in the security group to capture the statistics.
- In security group settings on the UCT-V Controller, enable Port 9900 to receive the statistics information from UCT-V.
- For UCT-C, add port 42042 and port 5671 to the security group.
- Precryption works only on Linux systems running Kernel version 4.18 or later.

License Prerequisite

- Precryption™ requires a SecureVUE Plus license.

Supported Kernel Version

Precryption is supported on kernel versions 4.18 and above, including 5.4+ kernels, across all Linux and Ubuntu operating systems. For the Kernel versions below 5.4, refer to the following table:

Kernel-Version	Operating System
4.18.0-193.el8.x86_64	RHEL release 8.2 (Ootpa)
4.18.0-240.el8.x86_64	RHEL release 8.3 (Ootpa)
4.18.0-305.76.1.el8_4.x86_64	RHEL release 8.4 (Ootpa)
4.18.0-348.12.2.el8_5.x86_64	RHEL release 8.5 (Ootpa)
4.18.0-372.9.1.el8.x86_64	RHEL release 8.6 (Ootpa)
4.18.0-423.el8.x86_64	RHEL release 8.7 Beta (Ootpa)
4.18.0-477.15.1.el8_8.x86_64	RHEL release 8.8 (Ootpa)
5.3.0-1024-kvm	Ubuntu 19.10
4.18.0-305.3.1	Rocky Linux 8.4
4.18.0-348	Rocky Linux 8.5
4.18.0-372.9.1	Rocky Linux 8.6
4.18.0-425.10.1	Rocky Linux 8.7
4.18.0-477.10.1	Rocky Linux 8.8
4.18.0-80.el8.x86_64	CentOS 8.2
4.18.0-240.1.1.el8_3.x86_64	CentOS 8.3
4.18.0-305.3.1.el8_4.x86_64	CentOS 8.4
4.18.0-408.el8.x86_64	CentOS 8.5

For more details, refer to Gigamon TV.

Note

- See the Configure Precryption in UCT-V section for details on how to enable Precryption™ in VM environments.
- See the Configure Precryption in UCT-C section for details on how to enable Precryption™ in container environments.
- See how Secure Tunnels feature can enable secure delivery of precrypted data.

Secure Tunnels

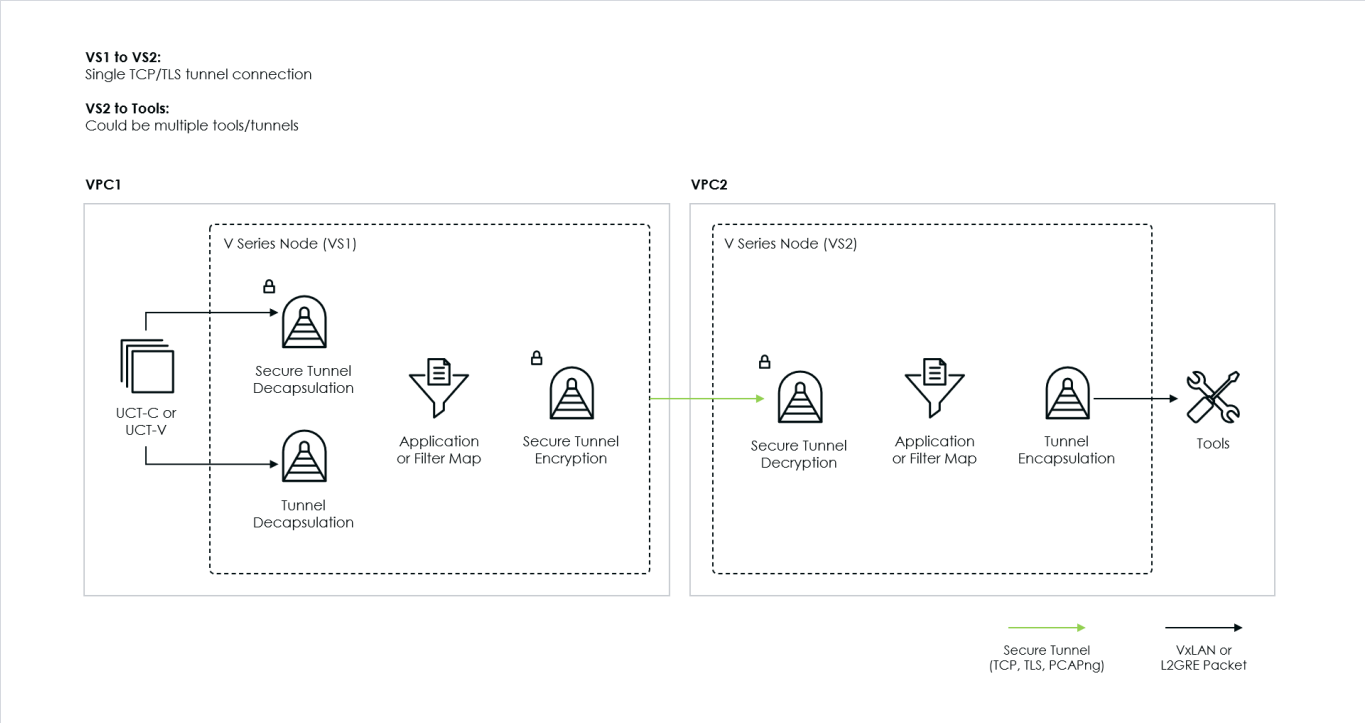
Secure Tunnel transfers the cloud captured packets from one GigaVUE V Series Node to another.

When sending traffic between two V Series Nodes, the source node captures and encapsulates the packets in PCAPng format. It then sends them to the destination V Series Node that decapsulates and processes the traffic based on your configuration.

How Does it Work!

- The source V Series forwards packets to the destination V series for further analysis.
- The destinatin node applies processing features such as de-duplication, application intelligence, or load balancing.
- The built-in load balancer distributes traffic across multiple V Series Nodes.
- If the load balancer sends packets to another node, it can re-encapsulate them and send them over another secure tunnel.

For more information, refer to PCAPng Application.



Supported Platforms

Secure Tunnels are 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 (OpenStack).

Prefiltering

Prefiltering allows you to filter the traffic at UCT-Vs before sending it to the GigaVUE V Series Nodes. For prefiltering the traffic, GigaVUE-FM allows you to create a prefiltering policy template and the policy template can be applied to a monitoring session.

You can define a policy template with rules and filter values. A policy template once created can be applied to multiple monitoring sessions. However a monitoring session can use only one template.

Each monitoring session can have a maximum of 16 rules.

You can also edit a specific policy template with required rules and filter values for a particular monitoring session while editing a monitoring session. However, the customized changes are not saved in the template.

Some of the points that must be remembered for prefiltering in Next Generation UCT-Vs are:

- Prefiltering is supported only in Next Generation UCT-Vs. It is not supported for classic mirroring mechanism.
- Prefiltering is supported for both Linux and Windows UCT-Vs .
- For single monitoring session only one prefiltering policy is applicable. All the agents in that monitoring sessions are configured with respective prefiltering policy .
- For multiple monitoring session using the same agent to acquire the traffic, if a monitoring session uses a prefilter and the other monitoring session does not use a prefilter, then the prefiltering policy cannot be applied. The policy is set to PassAll and prefiltering is not performed.
- When multiple monitoring sessions utilize a single agent to capture traffic, and one session uses a prefilter while the other does not, then the prefiltering policy is not applied. In this scenario, the policy defaults to PassAll, resulting in the omission of any prefiltering.

For more information on configuring a prefilter, refer to Create Prefiltering Policy Template

Customer Orchestrated Source - Use Case

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

When using Customer Orchestrated Source, you can directly configure tunnels or raw endpoints in the monitoring session, where you can use other applications like Slicing, Masking, Application Metadata, Application Filtering, etc., to process the tunneled traffic. Refer to Create Ingress and Egress Tunnels (OpenStack) for more detailed information on how to configure Tunnels in the Monitoring Session.

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

Licensing GigaVUE Cloud Suite

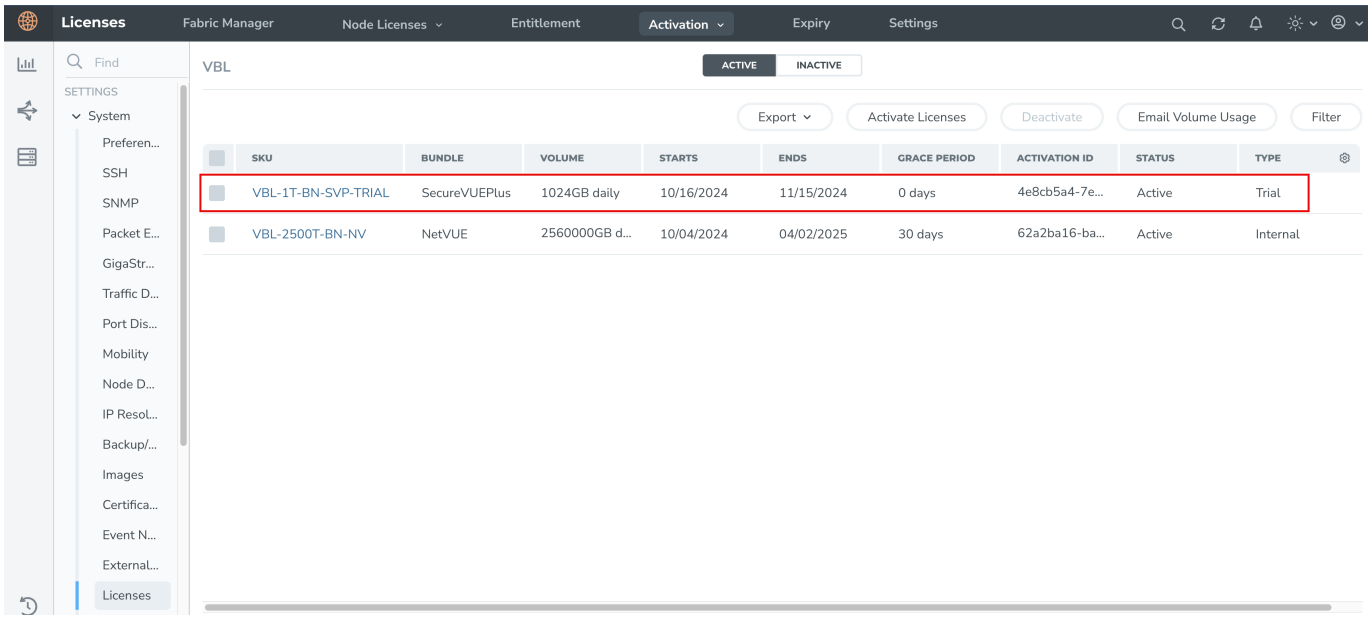
You can license the GigaVUE Cloud Suite using one of the following method:

- Purchase GigaVUE Cloud Suite using CPPO
- Volume Based License (VBL)

For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales. Refer to Contact Sales. For instructions on how to generate and apply license refer to the *GigaVUE Administration Guide* and the GigaVUE Licensing Guide.

Default Trial Licenses

After installing GigaVUE-FM, you receive a one-time, free 1TB SecureVUE Plus trial Volume-Based License (VBL) for 60 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, the deployed monitoring sessions are undeployed from the existing GigaVUE V Series Nodes after 60 days at the expiration of the trial license.

When you install a new Volume-Based License (VBL), the existing trial license remains active alongside the new VBL. When the trial license period expires, it is automatically deactivated. After deactivation, the trial license moves to the Inactive tab on 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 reflect the data volume flowing through the V Series Nodes, with the usage statistics of all licensed applications that run on these nodes.

GigaVUE Cloud Suite uses volume-based licensing (VBL), available as monthly subscription licenses. In the Volume-based Licensing (VBL) scheme, specific applications on the V Series Nodes are entitled to a specified amount of total data volume over the term of the license.

Distributing the license to individual nodes becomes irrelevant for Gigamon accounting purposes. GigaVUE-FM monitors overall consumption across all nodes and tracks individual application usage and overages.

Related Information

- Contact Sales: For purchasing licenses with the Volume-Based License (VBL) option.
- For more information, refer to the Data Sheet for the required GigaVUE Cloud Suite.

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUE Plus

The bundles are available as SKUs [1]. The SKUs are named such that the number indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE indicates a daily volume allowance of 250 Terabytes (250T) for the CoreVUE bundle.

The features supported for base bundle licenses are given in the following table:

Feature	CoreVUE	NetVUE	SecureVUE Plus
Slicing	√	√	√
Masking	√	√	√
Advanced Load Balancing	√	√	√
Advanced Tunneling	√	√	√
Deduplication	-	√	√
NetFlow Generation	-	√	√
Adaptive Packet Filtering (APF)	-	-	√
Application Filtering	-	-	√

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

Feature	CoreVUE	NetVUE	SecureVUE Plus
Intelligence (AFI)			
Application Metadata Intelligence (AMI)	-	-	√
Application Metadata Exporter (AMX)	-	-	√
Inline Decryption	-	-	√
OOB Decryption	-	-	√
Precryption	-	-	√
Gigamon Enriched Metadata	-	-	√

Bundle Replacement Policy

Refer to the following notes:

- You can only upgrade to a higher bundle.
- You cannot have two different base bundles at the same time. However, you can have multiple base bundles of the same type.
- As soon as you upgrade to a higher bundle, the existing lower bundles are automatically deactivated.

Add-on Packages

GigaVUE-FM allows you to add 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.

The following add-on SKUs are available:

- VBL-50T-ADD-5GC
- VBL-250T-ADD-5GC
- VBL-2500T-ADD-5GC
- VBL-25KT-ADD-5GC

Rules for add-on packages:

- An active base bundle is required to use an Add-on package.
- Your base bundle limits the total volume usage of the add-on package in the following ways:
  - If the volume allowance of your add-on package is less than the base bundle, then your add-on package can only handle the volume allocated for the add-on package.
  - When the life term of an add-on package extends beyond the base bundle, and the base bundle expires, the add-on package's volume allowance is reduced to zero until you add a new base bundle.
  - The total volume is cumulative when multiple base bundles of the same type are active within the same time interval.

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

- 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

How GigaVUE-FM Tracks Volume-Based License Usage

GigaVUE-FM applies the following methods to track the license usage for each GigaVUE V Series Node:

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only applications with active licenses.
- When a license expires, you are notified with an audit log. For more information, 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 are not undeployed.
- For releases prior to 6.4:
  - The Monitoring Sessions using the corresponding license are undeployed, but not deleted from the database.
  - Any undeployed monitoring sessions are redeployed when you renew a license or newly import the same.

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

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 reflect the data volume flowing through the V Series Nodes, with the usage statistics of all licensed applications that run on these nodes.

GigaVUE Cloud Suite uses volume-based licensing (VBL), available as monthly subscription licenses. In the Volume-based Licensing (VBL) scheme, specific applications on the V Series Nodes are entitled to a specified amount of total data volume over the term of the license.

Distributing the license to individual nodes becomes irrelevant for Gigamon accounting purposes. GigaVUE-FM monitors overall consumption across all nodes and tracks individual application usage and overages.

Related Information

- Contact Sales: For purchasing licenses with the Volume-Based License (VBL) option.
- For more information, refer to the Data Sheet for the required GigaVUE Cloud Suite.

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 SKUs are named such that the number indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE indicates a daily volume allowance of 250 Terabytes (250T) for the CoreVUE bundle.

Bundle Replacement Policy

Refer to the following notes:

- You can only upgrade to a higher bundle.
- You cannot have two different base bundles at the same time. However, you can have multiple base bundles of the same type.
- As soon as you upgrade to a higher bundle, the existing lower bundles are automatically deactivated.

Add-on Packages

GigaVUE-FM allows you to add 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.

The following add-on SKUs are available:

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

- VBL-50T-ADD-5GC
- VBL-250T-ADD-5GC
- VBL-2500T-ADD-5GC
- VBL-25KT-ADD-5GC

Rules for add-on packages:

- An active base bundle is required to use an Add-on package.
- Your base bundle limits the total volume usage of the add-on package in the following ways:
  - If the volume allowance of your add-on package is less than the base bundle, then your add-on package can only handle the volume allocated for the add-on package.
  - When the life term of an add-on package extends beyond the base bundle, and the base bundle expires, the add-on package's volume allowance is reduced to zero until you add a new base bundle.
  - The total volume is cumulative when multiple base bundles of the same type are active within the same time interval.

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

- 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

How GigaVUE-FM Tracks Volume-Based License Usage

GigaVUE-FM applies the following methods to track the license usage for each GigaVUE V Series Node:

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only applications with active licenses.
- When a license expires, you are notified with an audit log. For more information, 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 are not undeployed.
- For releases prior to 6.4:
  - The Monitoring Sessions using the corresponding license are undeployed, but not deleted from the database.
  - Any undeployed monitoring sessions are redeployed when you renew a license or newly import the same.

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

Activate Volume-Based Licenses

To activate Volume-Based Licenses,

1. On the left navigation pane, select  .
2. Go to **System > Licenses**.
3. From the top navigation bar, select the **VBL** from the **Activation** drop-down.
4. Select **Activate Licenses**. The **Activate License** page appears.
5. Select **IP Address** or **Hostname** to include this information. If you exclude the IP Address or Hostname, identify the chassis or GigaSMART card by its ID when activating.
6. Download the fabric inventory file that contains information about GigaVUE-FM.
7. Select **Next**. For details, refer to the What is a Fabric Inventory File section in *GigaVUE Licensing Guide*
8. Select **Gigamon License Portal**.
9. On the portal, upload the Fabric Inventory file.
10. Select the required license and select **Activate**. A license key is provided.
11. Record the license key or keys.
12. Return to GigaVUE-FM and select **Choose File to** upload the file.

Manage Volume-Based Licenses

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

View active Volume-Based License

To view active Volume-Based License (VBL):

1. On the left navigation pane, click  .
2. Go to **System > Licenses**.
3. 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, select the column setting configuration option to enable the Entitlement ID field.

View Inactive Volume-Based License

To view inactive Volume-Based License (VBL):

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

   This page lists the following information about the inactive Volume-Based Licenses.

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, select the column setting configuration option and enable these fields.

Activate Volume-Based Licenses

To activate Volume-Based Licenses,

1. On the left navigation pane, select  .
2. Go to **System > Licenses**.
3. From the top navigation bar, select the **VBL** from the **Activation** drop-down.
4. Select **Activate Licenses**. The **Activate License** page appears.
5. Select **IP Address** or **Hostname** to include this information. If you exclude the IP Address or Hostname, identify the chassis or GigaSMART card by its ID when activating.
6. Download the fabric inventory file that contains information about GigaVUE-FM.
7. Select **Next**. For details, refer to the What is a Fabric Inventory File section in *GigaVUE Licensing Guide*
8. Select **Gigamon License Portal**.
9. On the portal, upload the Fabric Inventory file.
10. Select the required license and select **Activate**. A license key is provided.
11. Record the license key or keys.
12. Return to GigaVUE-FM and select **Choose File to** upload the file.

NOTE: If a VBL is deactivated after a bundle upgrade, you cannot create or edit Monitoring Sessions that include applications from the deactivated VBL during the grace period. You should manually deactivate the upgraded license during the grace period to move the inactive lower bundle license back to active status.

For 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

Get Started with GigaVUE Cloud Suite for OpenStack Deployment

This chapter describes how to configure GigaVUE-FM fabric manager, UCT-V Controllers, GigaVUE V Series Proxy, and GigaVUE V Series Nodes in your OpenStack Cloud (Project). Refer to the following sections for details:

- License Information
- Before You Begin
- Install and Upgrade GigaVUE-FM

Before You Begin

This section describes the requirements and prerequisites for configuring the GigaVUE Cloud Suite for OpenStack. Refer to the following section for details.

- Supported Hypervisor for OpenStack
- Supported Compute Requirements for OpenStack
- Network Requirements
- Virtual Network Interface Cards (vNICs)
- Security Group for OpenStack
- Key Pairs
- Prerequisites for OVS Mirroring
- GigaVUE-FM Version Compatibility
- Default Login Credentials for GigaVUE Fabric Components

Supported Hypervisor for OpenStack

The following table lists the hypervisor with the supported versions for UCT-V.

Hypervisor	Supported Versions
KVM	**UCT-V**—Pike through Stein releases **OVS Mirroring**—Rocky and above, RHOSP 16.2 and 17.1, Kolla-ansible

Supported Compute Requirements for OpenStack

In OpenStack, flavors set the vCPU, memory, and storage requirements for an image. Gigamon recommends that you create a flavor on your choice that matches or exceeds the supported requirements listed in the following table.

Compute Instances	vCPU	Memory	Disk Space	Description
UCT-V	2 vCPU	4GB	N/A	Available as rpm or Debian package. Instances can have a single vNIC or dual vNICs configured for monitoring the traffic.
UCT-V Controller	2 vCPU	4GB	10GB	Based on the number of agents being monitored, multiple controllers will be required to scale out horizontally.
GigaVUE V Series Node	4 vCPU	4GB	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	10GB	Based on the number of GigaVUE V Series nodes being monitored, multiple controllers will be required to scale out horizontally.
GigaVUE-FM	4 vCPU	16GB	80GB	GigaVUE-FM must be able to access the controller instance for relaying the commands. Use a flavor with a root disk of minimum 40GB and an ephemeral disk of minimum 41GB.

NOTE: A single UCT-V Controller can manage up to 500 UCT-Vs. For more than 500 UCT-Vs, you must add an additional UCT-V Controller to scale up accordingly.

The instance size of the GigaVUE V Series Node is configured and packaged as part of the qcow2 image file.

Network Requirements

The following table lists the recommended requirements to setup the network topology.

Network	Purpose
Management	Identify the subnets that GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers.
Data	Identify the subnets that receives the mirrored tunnel traffic from the monitored instances. In data network, if a tool subnet is selected then the V Series node egress traffic on to the destinations or tools.

NOTE: If you are using IPv6 in the tenant network, then it is recommended to use SLAAC or stateless DHCPv6 for dynamic address assignment.

Virtual Network Interface Cards (vNICs)

OpenStack Cloud Instances with UCT-V can be configured with one or more vNICs.

- **Single vNIC**—If there is only one interface configured on the instance with the UCT-V, the UCT-V sends the mirrored traffic out using the same interface.
- **Multiple vNICs**—If there are two or more interfaces configured on the instance with the UCT-V, the UCT-V monitors any number of interfaces. It provides an option to send the mirrored traffic out using any one of the interfaces or using a separate, non-monitored interface. When multiple interfaces are added to the controller, floating IP is used to make the first interface as management interface.

NOTE: vNICs are only applicable if the UCT-V is installed on the instances being monitored. It is not applicable for OVS Mirroring or OVS Mirroring +DPDK.

Security Group for OpenStack

A security group defines the virtual firewall rules for your instance to control inbound and outbound traffic. When you launch GigaVUE-FM, GigaVUE V Series Proxies, GigaVUE V Series Nodes, and UCT-V Controllers in your project, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

The following table lists the Network Firewall / Security Group requirements for GigaVUE Cloud Suite:

NOTE: When using dual stack network, open the below mentioned ports for both IPv4 and IPv6.

GigaVUE FM

The following table specifies the inbound and outbound communication parameters—protocols, ports, and CIDRs—required for GigaVUE-FM to support secure access, registration, certificate exchange, and control-plane communication with associated components.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	443	Administrator Subnet	Allows GigaVUE-FM to accept Management connection using REST API. Allows users to access GigaVUE-FM UI securely through an HTTPS connection.
Inbound	TCP	22	Administrator Subnet	Allows CLI access to user-initiated management and diagnostics.

Inbound (This is the port used for Third Party Orchestration)	TCP	443	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-V Controller using REST API.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Node using REST API when GigaVUE V Series Proxy is not used.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Proxy using REST API.
Inbound	TCP	443	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-C Controller using REST API.
Inbound	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive traffic health updates from GigaVUE V Series Nodes.
Inbound	TCP	5671	UCT-V Controller IP	Allows GigaVUE-FM to receive statistics from UCT-V Controllers.
Inbound	TCP	9600	UCT-V Controller	Allows GigaVUE-FM to receive certificate requests from UCT-V Controller.
Inbound	TCP	9600	GigaVUE V Series Proxy	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Proxy.
Inbound	TCP	9600	GigaVUE V Series Node	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Node.
Inbound	TCP	5671	UCT-V Controller IP	Allows GigaVUE-FM to receive statistics from UCT-C Controllers.
Inbound	UDP	2056	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive Application Intelligence and Application Visualization reports from GigaVUE V Series Node.

Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	9900	UCT-V Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic with UCT-V Controller.
Outbound (optional)	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Proxy.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Node.
Outbound	TCP	8443	UCT-C Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic to UCT-C Controller.
Outbound	TCP	80	UCT-V Controller IP	Allows GigaVUE-FM to send ACME challenge requests to UCT-V Controller.
Outbound	TCP	80	GigaVUE V Series Node	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Node.
Outbound	TCP	80	GigaVUE V Series Proxy	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Proxy.
Outbound	TCP	443	Any IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.

UCT-V Controller

The following table defines the network communication parameters—protocols, ports, and CIDRs—required for UCT-V Controller to interact with GigaVUE-FM and UCT-V components, supporting registration, diagnostics, certificate exchange, and control-plane operations including third-party orchestration..

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate control and management plane traffic with GigaVUE-FM.

Inbound	TCP	9900	UCT-V or Subnet IP	Allows UCT-V Controller to receive traffic health updates from UCT-V.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows UCT-V Controller to receive the ACME challenge requests from GigaVUE-FM.
Inbound	TCP	8300	UCT-VSubnet	Allows UCT-V Controller to receive the certificate requests from the UCT-V.
Inbound (This is the port used for Third Party Orchestration)	TCP	8892	UCT-V Subnet	Allows UCT-V Controller to receive the registration requests and heartbeat from UCT-V.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows UCT-V Controller to send the registration requests to GigaVUE-FM using REST API.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
Outbound (This is the port used for Third Party Orchestration)	TCP	9600	GigaVUE-FM IP	Allows GigaVUE-FM to receive certificate requests from the UCT-V Controller.
Outbound	TCP	9902	UCT-V Subnet	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs for UCT-Vs with version greater than 6.10.00.
Outbound	TCP	8301	UCT-V Subnet	Allows ACME validation flow from UCT-V Controller to UCT-V.

UCT-V

The following table outlines UCT-V Controller's network communication requirements with GigaVUE-FM, detailing essential ports, protocols, and CIDRs for registration, diagnostics, certificate exchange, and orchestration traffic.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9902	UCT-V Controller IP	Allows UCT-V to receive control

				and management plane traffic from UCT-V Controller.
Inbound	TCP	8301	UCT-V Controller IP	Allows UCT-V to receive the ACME challenge requests from the UCT-V Controller.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	UDP (VXLAN)	VXLAN (default 4789)	GigaVUE V Series Node IP	Allows UCT-V to tunnel VXLAN traffic to GigaVUE V Series Nodes.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	GigaVUE V Series Node IP	Allows UCT-V to tunnel L2GRE traffic to GigaVUE V Series Nodes.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	GigaVUE V Series Node IP	Allows UCT-V to securely transfer the traffic to the GigaVUE V Series Node.
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V to send traffic health updates to UCT-V Controller.
Outbound (This is the port used for Third Party Orchestration)	TCP	8892	UCT-V Controller IP	Allows UCT-V to receive the registration requests and heartbeat to UCT-V Controller.
Outbound	TCP	8300	UCT-V Controller IP	Allows UCT-V to receive ACME validation flow from UCT-V Controller.

GigaVUE V Series Node

The following table outlines GigaVUE V Series Node's network communication requirements, detailing protocols, ports, and CIDRs necessary for tunneling, management, diagnostics, and secure data transfer across connected components

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8889	GigaVUE-FM IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE-FM.
Inbound	TCP	8889	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	UDP (VXLAN)	VXLAN (default 4789)	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive VXLAN tunnel traffic to UCT-V.

Inbound	IP Protocol (L2GRE)	L2GRE	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive L2GRE tunnel traffic to UCT-V.
Inbound	UDPGRE	4754	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from UDPGRE Tunnel.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Node to receive the ACME challenge requests from GigaVUE-FM.
Inbound	TCP	80	GigaVUE V Series Proxy IP	Allows UCT-V to receive the ACME challenge requests from the GigaVUE V Series Proxy.
Inbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	UCT-V subnet	Allows to securely transfer the traffic to GigaVUE V Series Nodes.
Inbound (Optional - This port is used only for configuring AWS Gateway Load Balancer)	UDP (GENEVE)	6081	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from AWS Gateway Load Balancer.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM.
Outbound	UDP (VXLAN)	VXLAN (default 4789)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	UDP	2056	GigaVUE-FM IP	Allows GigaVUE V Series Node to send Application Intelligence and Application Visualization reports to GigaVUE-FM.
Outbound	UDP	2055	Tool IP	Allows GigaVUE V Series Node to send NetFlow Generation traffic to an external tool.
Outbound	UDP	8892	GigaVUE V Series Proxy	Allows GigaVUE V Series Node to send certificate request to GigaVUE V Series Proxy IP.
Outbound	TCP	514	Tool IP	Allows GigaVUE V Series Node to

				send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	• echo request • echo reply	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE-FM when GigaVUE V Series Proxy is not used.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	Tool IP	Allows to securely transfer the traffic to an external tool.

Giga VUE V Series Proxy(Optional)

The following table defines GigaVUE V Series Proxy's network communication parameters, listing essential protocols, ports, and CIDRs for registration, certificate exchange, diagnostics, and control-plane traffic with GigaVUE-FM and V Series Nodes.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Proxy to receive the ACME challenge requests from the GigaVUE-FM.
Inbound	TCP	8300	GigaVUE V Series Node	Allows GigaVUE V Series Proxy to receive certificate requests from GigaVUE V Series Node for the configured params and provides the certificate using those parameters.
Inbound	TCP	8892	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.

Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate control and management plane traffic with GigaVUE V Series Node.

UCT-C Controller - deployed in Kubernetes worker mode

The following table outlines UCT-C Controller's network communication parameters in Kubernetes worker mode, specifying TCP ports and CIDRs required for management, statistics exchange, and secure connectivity with GigaVUE-FM.

UCT-C Controller deployed inside Kubernetes worker node				
Direction	**Protocol**	**Port**	**Source CIDR**	**Purpose**
Inbound	TCP	8443 (configurable)	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-C Controller.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	5671	Any IP address	Allows UCT-C Controller to send statistics to GigaVUE-FM.
Outbound	TCP	443	GigaVUE-FM IP	Allows UCT-C Controller to communicate with GigaVUE-FM.

Ports for Backward Compatibility

Ensure to open these ports for backward compatibility when GigaVUE-FM is running version 6.10 or later, and the fabric components are on (n-1) or (n-2) versions.

UCT-V Controller

The following table specifies the communication parameters required for third-party orchestration, detailing the TCP ports and CIDRs used by UCT-V Controller to manage registration and control-plane traffic with UCT-V components.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests from

(This is the port used for Third Party Orchestration)				UCT-V.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs.

GigaVUE V Series Node

The following table specifies the outbound communication requirement for GigaVUE V Series Node, detailing the protocol, port, and source CIDR used to send registration and heartbeat messages to the GigaVUE V Series Proxy during third-party orchestration.

Direction	Protocol	Port	Source CIDR	Purpose
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE V Series Proxy when GigaVUE V Series Proxy is used.

GigaVUE V Series Proxy(Optional)

The following table specifies the optional inbound communication parameter for GigaVUE V Series Proxy, detailing the protocol, port, and source CIDR required to receive security parameter requests from GigaVUE V Series Node during third-party orchestration.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive security parameter requests from GigaVUE V Series Node.

The following table list the Network Firewall or Security Group requirements when using OVS Mirroring.

Direction	Protocol	Port	CIDR	Purpose
UCT-V OVS Controller				
Inbound	TCP	9900	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-V OVS Controllers

Direction	Protocol	Port	CIDR	Purpose
UCT-V OVS Module				
Inbound	TCP	9901	UCT-V OVS Controller IP	Allows UCT-V OVS Controllers to communicate with UCT-V OVS Modules

NOTE: The Security Group Rules table lists only the ingress rules. Make sure the egress ports are open for communication. Along with the ports listed in the Security Group Rules table, make sure the suitable ports required to communicate with Service Endpoints such as Identity, Compute, and Cloud Metadata are also open.

Key Pairs

A key pair consists of a public key and a private key. You must create a key pair and select the name of this key pair when you launch the UCT-V Controllers, GigaVUE V Series nodes, and GigaVUE V Series Controllers from GigaVUE-FM. Then, you must provide the private key to connect to these instances. For information about creating a key pair, refer to OpenStack documentation.

Prerequisites for OVS Mirroring

This section is only applicable if you wish to use OVS Mirroring as your traffic acquisition method. The following items are required to deploy a UCT-V OVS module:

- An existing OpenStack cloud environment should be available with admin project and login credentials to create a monitoring domain.
- A user with OVS access is required to enable OVS-Mirror. The user can be an admin or can be a user with a custom role that has the permissions and the ability to list projects.
- A working GigaVUE-FM with latest build.

OVS-Mirror Requirements

Operating System	OVS Versions	OpenStack Version	Operating System Version
Ubuntu	2.9.8, 2.13.8	4.0.2, 5.5.1	20.04
Red Hat OpenStack platform	2.15.5	16.2, 17.1	Red Hat Enterprise Linux 8.4, Red Hat Enterprise Linux 9.2 (Plow)

OpenStack Cloud Environment Requirements

- ML2 mechanism driver: Open vSwitch.
- You must have the following role privileges as shown in the table for the respective files to enable OVS mirroring:

File	Command
/etc/nova/policy.json	"os_compute_api:os-hypervisors": "role:gigamon", "os_compute_api:servers:detail:get_all_tenants": "role:gigamon", "os_compute_api:servers:index:get_all_tenants": "role:gigamon", "os_compute_api:servers:allow_all_filters":"role:gigamon", "os_compute_api:os-extended-server-attributes":"role:gigamon"
/etc/keystone/policy.json	"identity:list_projects": "role:admin or role:gigamon", "identity:list_user_projects": "role:admin or role:gigamon or rule:owner", "identity:list_users": "role:admin or role:gigamon"
/etc/neutron/policy.json	"context_is_advsvc": "role:advsvc or role:gigamon", "get_subnet": "rule:admin_or_owner or rule:shared or role:gigamon", "get_network": "rule:admin_or_owner or rule:shared or rule:external or rule:context_is_advsvc", "update_floatingip": "rule:admin_or_owner or role:gigamon", "get_floatingip": "rule:admin_or_owner or role:gigamon", "get_security_groups": "rule:admin_or_owner or role:gigamon", "get_security_group": "rule:admin_or_owner or or role:gigamon", "get_port": "rule:context_is_advsvc or rule:admin_owner_or_network_owner", "get_port:binding:vif_details":"rule:admin_only or rule:context_is_gigamon"

- Here are the APIs and commands required for OVS mirroring

OpenStack CLI command	Supported API/Action	Description
openstack hypervisor list	GET /os-hypervisors	Should list all hypervisors in the domain.
openstack server list --all -- host <hostname>	GET /servers	Should list all the servers on a specified host
openstack server list-all	GET /servers	Should list servers of all projects in the domain.
openstack project list	GET /v3/projects	Should list all projects in the domain.
openstack project list - user <user with custom role>	GET /v3/projects	Should list all projects that a specified user (user specified in GigaVUE-FM config) is associated with
openstack user show <userName>	GET /v3/users	Should list all users by username
openstack subnet list	GET /subnets	Should list all subnets for all projects in the

OpenStack CLI command	Supported API/Action	Description
		domain.
openstack network list	GET /network	Should list all networks for all projects in the domain.
openstack floating ip list	GET /floatingips	Should list all floating ips for all projects in the domain.
openstack floating ip set-port <portid> <floating ip>	PUT /floatingips/{floatingip_ID}	Used to attach floating ip to fabric nodes.
openstack security group list	GET /security-groups	Should list security groups for all projects in the domain
openstack security group show <security group id>	GET /security-groups/{security_group_id}	Should list details of specified security group
openstack port list	GET /ports	Should list ports for all projects in the domain
openstack port show <portID>	GET /ports/{portID}	Should list port details including bridge name.
openstack server create	POST /servers	Launch fabric nodes
openstack server <action> <serverName>	POST /servers/{server_id}/action	stop/start/reboot fabric nodes
openstack server delete <serverName>	DELETE /servers/{serverID}	Delete fabric nodes
openstack server set	PUT /servers/{serverID}/metadata	Update visibility node metadata
openstack flavor list	GET /flavors	Get list of flavors
openstack availability zone list	GET /os-availability-zone	Get list of availability zones
openstack keypair list	GET /os-keypairs	Get list of keypairs

If the OpenStack CLI command **`openstack hypervisor list`** does not return a reachable IP for the hypervisors that are being monitored, you must manually enter a reachable IP for each hypervisor in OpenStack CLI using project properties. For each hypervisor you will need to add a key value pair property in the following format:

- key: value
- key: must be in the form gigamon-hv-<hypervisorID>
- value: reachable IP for hypervisor

For example: **`openstack project set --property gigamon-hv-1=1.2.3.4 project-name`**

GigaVUE-FM Version Compatibility

GigaVUE-FM version 6.13.00 supports the latest version (6.13.00) of GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, and UCT-V, as well as (n-2) versions. For better compatibility, we recommend to use the latest version of fabric components with GigaVUE-FM.

Default Login Credentials for GigaVUE Fabric Components

You can login to the GigaVUE V Series Node, GigaVUE V Series proxy, and UCT-V Controller by using the default credentials.

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

Install and Upgrade GigaVUE-FM

You can install and upgrade the GigaVUE-FM fabric manager on cloud or on-premises. You can also upgrade GigaVUE-FM deployed in OpenStack environment.

- Cloud—To install GigaVUE-FM inside your OpenStack environment, you can simply launch the GigaVUE-FM instance in your Project. For installing the GigaVUE-FM instance, refer to Install GigaVUE-FM on OpenStack

NOTE: You cannot upgrade your 5.7.00 or lower versions of the GigaVUE-FM instance deployed in OpenStack environment to GigaVUE-FM 5.8.00 or higher versions. You must perform a fresh installation of GigaVUE-FM 5.8.00 or higher versions.

- 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.

Configure Role-Based Access for Third Party Orchestration

Before deploying the fabric components using a third party orchestrator, we must create users, roles and the respective user groups in GigaVUE-FM. You can use the user group to create a token for registration data, which helps deploy fabric components in your orchestrator.

Refer to following topics for more detailed information on how to add users, create roles and user groups:

- Users
- Role
- User Groups

Users

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
    - **Name:** Actual name of the user

- **Username**: User name configured in GigaVUE-FM
- **Email**: Email ID of the user
- **Password/Confirm Password**: Password for the user.
- **User Group:** Select the desired User Group to associate the user.

  GigaVUE-FM prompts for your password.

4. Click **Ok**. The new user is added.

Role

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

NOTE: A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

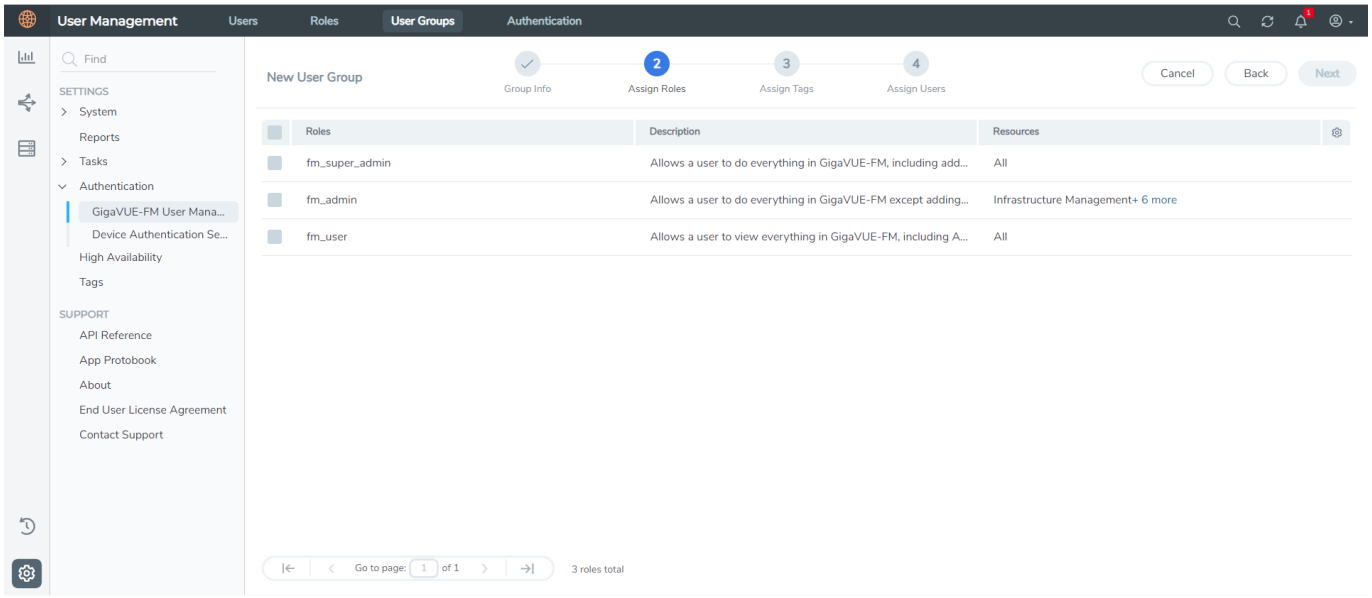
1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

User Groups

A user group consists of a set of roles and set of tags associated with users in that group. You can associate a new user to one or more groups.

To create a new user group,

1. Go to **Settings**, and then select **Authentication> GigaVUE-FM User Management >User Groups**.
2. Select **New Group.**



3. In the Wizard, perform the following steps.

   a. Select **Next** to progress forward and **Back** to navigate backward.

   b. In the **Group Info** tab, enter the following details:

   - **Group Name**
   - **Description**

   c. In the **Assign Roles** tab, select the role that you want to assign to the user group.

   d. In the **Assign Tags** tab, select the required tag key and tag value.

   e. In the **Assign Users** tab, select the required users.

   f. Select **Apply** to save the configuration.

NOTE: Select **Skip and Apply** to skip this step and proceed without adding users.

The new user group is added to the Summary list view.

Select the ellipses to perform the following operations:

- **Modify Users:** Edit the details of the users.
- **Edit:** Edit an existing group.

What to do Next:

Log in to GigaVUE-FM using the newly created user credentials and create tokens. For details, refer to Configure Tokens .

Configure Tokens

You must configure tokens for registering GigaVUE Fabric Components using Third Party Orchestration and registering UCT-V with GigaVUE-FM.

This feature verifies the identity of a user for accessing the GigaVUE-FM REST APIs by generating tokens.

GigaVUE-FM allows you to generate a token only if you are an authenticated user and based on your privileges in accessing the GigaVUE-FM. You can copy the generated tokens from the GUI, which can be used to access the REST APIs. Token inherits the Role-Based Access (RBAC) privilege (read or write) of the user groups assigned to a particular user.

GigaVUE-FM enables the generation of multiple tokens and associates them with the corresponding user groups. If you have GigaVUE-FM Security Management privileges with write access, you can revoke other users' tokens but not view the created tokens.

Prerequisite

You must create user groups in GigaVUE-FM. For details, refer to

Rules and Notes

- Authentication using a token is an additional mechanism to access GigaVUE-FM REST APIs, and it does not replace the existing GigaVUE-FM authentication mechanism.
- Only authenticated users can create tokens.
- The token expires or becomes invalid under the following circumstances:
    - Based on the configured value for expiry:
        - Default value: 30 days
        - Maximum value: 105 days
    - Deleting a related user group that exists as part of the token leads to deletion of the corresponding token.
    - A password change for the user(local) deletes the corresponding token.
    - A change in the authentication type deletes all the tokens.
- During the back up and restoration of GigaVUE-FM, previously generated tokens are not available.
- In FMHA role changeover, active GigaVUE-FM tokens are active.
- For basic authentication, activities such as creating, revoking, and reviewing of Token APIs are restricted.
- For expired or invalid tokens, you notice the error code 401 on GigaVUE-FM REST API access.

This section explains about the following:

Create Token

GigaVUE-FM allows you to create a token or multiple tokens if required.

To create a token, follow these steps:

1. Go to , select **Authentication** > **GigaVUE-FM User Management**. The **User Management** page appears.
2. In the **User Management** page, select **Tokens**.

NOTE: If you are a user with write access, then you can view a drop- down list under **Tokens**. Select **Current User Tokens** to create a token.

3. Select **New Token**.
4. Enter a name for the new token in the **Name** field.
5. Enter the days until the token is valid in the **Expiry** field.
6. Select the user group for which you are privileged to access GigaVUE-FM from the **User Group** drop-down list.
7. Select **OK** to generate a new token.

The generated token appears on the **Tokens** page. You can copy and use the generated token to authenticate the GigaVUE-FM REST APIs.

Copy and Paste a Token

1. Select the token that you want to copy.
2. Select **Actions>Copy Token.**

   The token is copied.
3. Paste the copied token in the required areas.

NOTE: You cannot view the generated token. You can only copy and paste the generated token.

Revoke Tokens

You can revoke tokens that other users create.

Prerequisite: Write access in GigaVUE-FM Security Management.

To revoke tokens,

1. Go to , select **Authentication** > **GigaVUE-FM User Management**.
2. In the **User Management** page, select **Tokens**.
3. From the drop-down, select **Token Management**. You can view the created tokens.
4. Select the token that you want to revoke.
5. Select **Action> Revoke**.

Export Token

GigaVUE-FM allows you to export selected or all the tokens in CSV and XLSX format.

- To export a token, select the token, select the **Export Selected** drop-down list box, and then select the **CSV** or **XLSX** format as per requirement.
- To export all the tokens, select the token, select the **Export All** drop-down list box, and then select the **CSV** or **XLSX** format as per requirement.

Deployment Options for GigaVUE Cloud Suite for OpenStack

This section provides a detailed information on the multiple ways in which GigaVUE Cloud Suite for OpenStack can be configured to provide visibility for physical and virtual traffic. There are four different ways in which GigaVUE Cloud Suite for OpenStack can be configured based on the traffic acquisition method and the method in which you want to deploy fabric components. Refer to theBefore You Begin topic for minimum requirements and prerequisites. For more detailed information and work flow refer the following topics:

- Deploy GigaVUE Fabric Components using OpenStack
- Deploy GigaVUE Fabric Components using GigaVUE-FM
  - Traffic Acquisition Method as UCT-V
  - Traffic Acquisition Method as OVS Mirroring
  - Traffic Acquisition Method as Customer Orchestrated Source

Deploy GigaVUE Fabric Components using OpenStack

GigaVUE-FM allows you to use OpenStack as an orchestrator to deploy GigaVUE fabric nodes and then use GigaVUE-FM to configure the advanced features supported by these nodes. Refer the following table for the step-by-step instructions.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on OpenStack	Install GigaVUE-FM on OpenStack
2	Install UCT-Vs **Note**: When using OpenStack as your orchestration system you can only use UCT-V.	For Linux: Linux UCT-V Installation For Windows: Windows UCT-V Installation
3	Create a Monitoring Domain **Note**: • Ensure that the **Use FM to Launch Fabric** toggle button is disabled. • Select **UCT-V** as the **Traffic Acquisition Method**.	Create Monitoring Domain
4	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in OpenStack
5	Create Monitoring session	Create a Monitoring Session (OpenStack)
6	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Deploy GigaVUE Fabric Components using GigaVUE-FM

If you wish to deploy your fabric components using GigaVUE-FM, it can done is three ways based on the traffic acquisition method you chose.

Traffic Acquisition Method as UCT-V

Follow instruction in the below table if you wish to use UCT-V as your traffic acquisition method. In this case the traffic from the Virtual Machines are acquired using the UCT-Vs and it is sent to the V Series nodes.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on OpenStack	Install GigaVUE-FM on OpenStack
2	Install UCT-Vs	For Linux: Linux UCT-V Installation For Windows: Windows UCT-V Installation
3	Create a Monitoring Domain **Note**: • Ensure that the **Use FM to Launch Fabric** toggle button is enabled. • Select **UCT-V** as the **Traffic Acquisition Method**.	Create Monitoring Domain
4	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in GigaVUE-FM
5	Create Monitoring session	Create a Monitoring Session (OpenStack)
6	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as OVS Mirroring

Follow instruction in the below table if you wish to use OVS Mirroring as your traffic acquisition method. Open vSwitch Mirroring extention is deployed on the hypervisor where the Virtual Machines you wish to monitor are located. Refer to the Prerequisites for OVS Mirroring topic for OpenStack cloud requirements before using OVS Mirroring as your traffic acquisition type.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on OpenStack	Install GigaVUE-FM on OpenStack
2	Install UCT-V OVS Modules	Install UCT-V OVS Mirroring Module
3	Create a Monitoring Domain **Note**: • Ensure that the **Use FM to Launch Fabric** toggle button is enabled. • Select OVS Mirroring as the **Traffic Acquisition Method**.	Create Monitoring Domain
4	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in GigaVUE-FM
5	Create Monitoring session	Create a Monitoring Session (OpenStack)

Step No	Task	Refer the following topics
6	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as Customer Orchestrated Source

Follow instruction in the below table if you wish to use Customer Orchestrated Source as your traffic acquisition method. In this case you can use tunnels as a source where the traffic is directly tunneled to V Series nodes without deploying UCT-Vs or UCT-V Controllers.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on OpenStack	Install GigaVUE-FM on OpenStack
2	Create a Monitoring Domain **Note**: • Ensure that the **Use FM to Launch Fabric** toggle button is enabled. • Select **Customer Orchestrated Source** as the **Traffic Acquisition Method**.	Create Monitoring Domain
3	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in GigaVUE-FM
4	Create Monitoring session	Create a Monitoring Session (OpenStack)
5	Create Ingress and Egress Tunnel Endpoints	Create Ingress and Egress Tunnels (OpenStack)
6	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Deploy GigaVUE Cloud Suite for OpenStack

This chapter describes how to connect, launch, and deploy fabric components of GigaVUE Cloud Suite for OpenStack in your OpenStack environment.

Refer to the following sections for details:

- Upload Fabric Images
- Install UCT-V
- Pre-Configuration Checklist for OpenStack
- Create Monitoring Domain
- Configure GigaVUE Fabric Components in GigaVUE-FM
- Configure GigaVUE Fabric Components in OpenStack
- Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack

Upload Fabric Images

First, you must fetch the images from Gigamon Customer Portal using FTP, SCP, or other desired methods and copy it to your cloud controller. After fetching the images, you must source the credentials file and then upload the qcow2 images to Glance.

For example, you can source the credentials file with admin credentials using the following command:

$ source admin_openrc.sh

To upload the qcow2 images to Glance, use the following commands:

GigaVUE-FM - **glance image-create --disk-format qcow2 --visibility public --container-format bare --progress --name fm-6.13-uefiSec-boot --file gfm-6.13.qcow2**

GigaVUE-FM with UEFI Boot - **glance image-create --disk-format qcow2 --visibility public --container-format bare --property hw_firmware_type=uefi --progress --name fm-6.13-uefiSec-boot --file gfm-6.13.qcow2**

GigaVUE-FM with UEFI secure Boot - **glance image-create --disk-format qcow2 --visibility public --container-format bare --property hw_firmware_type=uefi --property os_secure_boot=required --progress --name fm-6.13-uefiSec-boot --file gfm-6.13.qcow2**

> **NOTE:** UEFI secure boot is supported on RHSOP 17.01 version and above. UEFI secure boot is not supported on Wallaby.

Refer to the below table for the OpenStack flavors and the versions that support UEFI and UEFI secure boot:

OpenStack Flavor	Version	UEFI	UEFI Secure boot
kolla Ansible	Wallaby	Yes	No
Rhosp	17.01	Yes	Yes
Rhosp	16.2	No	No

UCT-V OVS Controller - **glance image-create --disk-format qcow2 --visibility public --container-format bare --progress --name gigamon-gigavue-uctv-ovs-cntlr-6.13 --file gigamon-gigavue-uctv-ovs-cntlr-6.13.qcow2**

UCT-V Controller - **glance image-create --disk-format qcow2 --visibility public --container-format bare --progress --name gigamon-gigavue-uctv-cntlr-6.13 --file gigamon-gigavue-uctv-cntlr-6.13.qcow2**

GigaVUE V Series Node - **glance image-create --disk-format qcow2 --visibility public --container-format bare --progress --name gigamon-gigavue-vseries-node-6.13 --file gigamon-gigavue-vseries-node-6.13.qcow2**

While uploading images to OpenStack, the names of the image files should be of the following format:

- gigamon-gigavue-vseries-node-6.13
- gigamon-gigavue-vseries-proxy-6.13
- gigamon-gigavue-uctv-cntlr-6.13
- gigamon-gigavue-uctv-ovs-cntlr-6.13

> **NOTE:** Always use '-' after the build number when providing designation details. For example, "**gigamon-gigavue-uctv-ovs-cntlr-buildNumber-**". Failure to follow this pattern will result in controller's deployment failure.

Upload Images using OpenStack Horizon Dashboard:

To upload the qcow2 using OpenStack Horizon Dashboard:

1. Log into Horizon.
2. From the Horizon GUI, select the appropriate project, and select **Compute > Images**.
3. Click **Create Image**. In the dialog box, provide the following details:

a. Name - Enter a descriptive name for the image

b. Image Source - Select File and browse to the location of the .qcow2 image file

c. Format - Select QCOW2

d. Visibility - Set as required (e.g., Public or Private)

4. Click **Create Image**. The image will be uploaded and listed in the **Images** page.

Refer to Install GigaVUE-FM on OpenStack to launch GigaVUE-FM instance using Horizon Dashboard.

Install GigaVUE-FM on OpenStack

To launch the GigaVUE-FM instance inside the cloud:

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

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

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

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

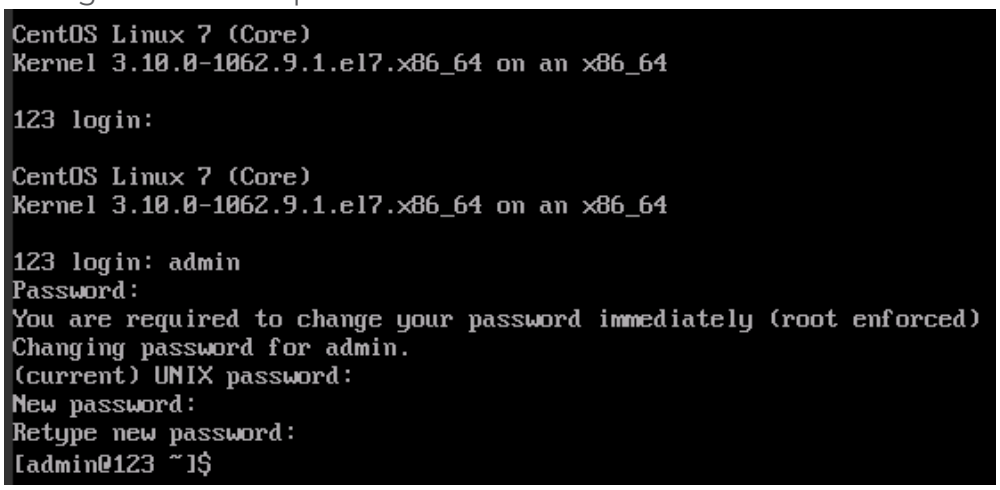
Parameter	Attribute
IP Address	Floating IP address of the instance
Port to be associated	Port for the GigaVUE-FM instance

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

Initial GigaVUE-FM Configuration

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

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



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

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

Install UCT-V

UCT-V is the primary Gigamon monitoring module that you install on your Virtual Machines (VMs). UCT-V mirrors the selected traffic from a source interface to a destination mirror interface. UCT-V encapsulates the mirrored traffic using GRE or VXLAN tunneling and then forwards to the GigaVUE V Series Node.

NOTE: Install UCT-V only when the UCT-V is your traffic acquisition method.

The Workflow

- A UCT-V can consist of multiple source interface and a single destination interface.
- UCT-V collects the network packets from the source interface and sends to the destination interface.
- From the destination interface, the packets traverse through the L2GRE, VXLAN tunnel interface, or Secure Tunnels to the GigaVUE V Series Node.

You can configure a source interface with one or more Network Interfaces. While configuring a source interface, specify the traffic direction to monitor: ingress, egress, or both.

NOTE: For environments with both Windows and Linux or just windows UCT-V, VXLAN tunnels in the UCT-V Controller specification is required.

Supported Platforms

UCT-V is compatible with the following platforms when used withGigaVUE-FM:

- AWS
- Azure
- OpenStack

UCT-V is compatible with the following platforms when used with Third Party Orchestration:

- AWS
- Azure
- OpenStack

- VMware ESXi
- VMware NSX-T

Refer to the following sections for more information:

- Supported Operating Systems for UCT-V
- Linux UCT-V Installation
- Windows UCT-V Installation
- Install UCT-V OVS Mirroring Module

Supported Operating Systems for UCT-V

Supported Operating System for UCT-V[1] is 6.5.00, 6.6.00, 6.7.00, 6.8.00, 6.9.00, 6.10.00, 6.11.00, 6.12.00, 6.13.00

The table below lists the validated and supported versions of the Operating Systems for UCT-V.

Operating System	Supported Versions
Ubuntu/Debian	Versions 16.04 through 22.04
CentOS	Versions 7.5 through 9.0
RHEL	Versions 7.5 through 9.4
Windows Server	Versions 2012 through 2022 **Note**: Ensure the **send buffer size** of the network adapters is set to 128 MB for optimal performance and to minimize traffic disruption.
Rocky OS	Versions 8.4 through 8.8

GigaVUE-FM version 6.13 supports UCT-V version 6.13 as well as (n-2) versions. We recommend to use the latest version of UCT-V with GigaVUE-FM for better compatibility.

Linux UCT-V Installation

You can install UCT-V on various Linux distributions using Debian or RPM packages.

Refer to the following sections:

- Single Network Interface Configuration
- Multiple Network Interface Configuration
- Loopback Network Interface Configuration
- Linux Network Firewall Requirements
- Install Linux UCT-Vs
- Register Linux UCT-V

[1]From Software version 6.4.00, G-vTAP is renamed to UCT-V.

Single Network Interface Configuration

A single network interface card (NIC) serves as both the source and destination interface. UCT-V, with a single network interface configuration, enables you to monitor both ingress and egress traffic from the same NIC. The system uses the same interface to send monitored traffic.

Example

Consider a single interface eth0 in the monitoring instance. In the UCT-V configuration, you can configure eth0 as both source and destination, and also specify monitoring for both ingress and egress traffic. The monitored traffic from eth0 is mirrored and sent using the same eth0 interface.

NOTE: Using a single NIC as the source and destination can lead to increased latency when sending traffic.

Sample Configuration

Example of the UCT-V configuration file for a single NIC configuration:

Grant permission to monitor ingress and egress traffic at iface

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst
```

Multiple Network Interface Configuration

In a multiple NIC configuration, UCT-Venables you to configure two NICs, one for the source and another for the destination.

Example

Consider two NICs, eth0 and eth1, in the monitoring instance.

In the UCT-V configuration, you can configure:

- eth0 as the source interface, and specify to monitor egress traffic.
- eth1 as the destination interface.

  Then, the mirrored traffic from eth0 is sent to eth1. From eth1, the traffic is sent to the GigaVUE V Series Node.

Sample: Example of the UCT-V configuration file for a dual NIC configuration:

Grant permission to monitor ingress and egress traffic at iface

```
# 'eth0' to monitor and 'eth1' to transmit the mirrored packets
# eth0 mirror-src-ingress mirror-src-egress
```

```
# eth1 mirror-dst
```

Loopback Network Interface Configuration

UCT-V supports the ability to tap and mirror the loopback interface. You can tap the loopback interfaces on the workload that carries application-level traffic inside the Virtual Machine. The loopback interface is always configured as bidirectional traffic, regardless of the configurations provided in the configuration file.

Example—Configuration example to monitor ingress and egress traffic at interface lo and use the same interface to send out the mirrored packets.

```
# lo mirror-src-ingress mirror-src-egress mirror-dst
```

Linux Network Firewall Requirements

If Network Firewall requirements or security groups are configured in your environment, you must open the following ports for the virtual machine. For details, refer to Network Firewall Requirement for GigaVUE Cloud Suite.

Direction	Port	Protocol	CIDR	Purpose
Inbound	9902	TCP	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller

You can use the following commands to add the Network Firewall rule.

```
sudo firewall-cmd --add-port=9902/tcp
sudo firewall-cmd --runtime-to-permanent
```

Install Linux UCT-Vs

You must have sudo/root access to edit the UCT-V configuration file. Establish an SSH connection to the virtual machine and ensure you have permission to execute the sudo command.

You may need to modify the network configuration files for dual or multiple network interface configurations to ensure that the extra NIC/Network interface initializes at boot time.

Prerequisites

- UCT-V is a standalone service. By default, most modern Linux operating systems come pre-installed with all the necessary packages for the UCT-V to function without additional configuration.
- Before registering Linux UCT-V, you should generate token and place it in the **/etc/gigamon-cloud.conf** configuration file. For more information, refer to Configure Tokens.

You can install the UCT-Vs either from Debian or RPM packages using one of the following options:.

- Install Linux UCT-Vs using Installation Script
- Install Linux UCT-Vs using Manual Configuration

Refer to the following sections for more detailed information and step-by-step instructions.

Install Linux UCT-Vs using Installation Script

Using installation script, you can complete installation.

Perform the following steps:

1. **To install UCT-V from Ubuntu/Debian:**
    a. Download the UCT-V**6.13.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
    b. Copy this package to your instance and Install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.13.00-amd64.deb
    $ sudo dpkg -i gigamon-gigavue-uctv-6.13.00-amd64.deb
    ```

2. **To install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS:**
    a. Download the UCT-V**6.13.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
    b. Copy this package to your instance and install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.13.00-x86_64.rpm
    $ sudo rpm -i gigamon-gigavue-uctv-6.13.00-x86_64.rpm
    ```

3. Use the command given below to perform pre-check, installation, and configuration functionalities.

```
sudo uctv-wizard
```

NOTE: The installation script is not provided with the Debian or RPM packages. You can use the script (installation_wizard.sh/uctv-wizard) only after the UCT-V is installed.

Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	sudo uctv-wizard pre-check	Checks the status of the required packages and firewall requirements. • If any package is missing, it displays an appropriate message with the missing package details. • If installation includes all the packages, it displays a success message indicating that UCT-V is ready for configuration.
pkg-install	sudo uctv-wizard pkg-install **NOTE:** The uctv-wizard install command requires access to a repository, either public (internet-based) or local, that hosts prerequisite packages for installation. If no repository is accessible, you must manually install the required packages. Refer to Linux UCT-V Installation.	Displays the missing package and version details. To proceed with the installation, you can choose between the following: If you wish to skip the prompts and proceed with the system update, enter your option as **y**. The console interface installs the missing packages and restarts the UCT-V service. Enter **N** if you wish to install it manually. For details, refer to Linux UCT-V Installation.
configure	sudo uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** location). If available, UCT-V uses that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. If you wish to skip the prompts to add the

Options	Use Command	Description
		required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. Enter **N** if you wish to configure manually. For details, refer to Linux UCT-V Installation section.
uninstall	sudo uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- Use the command below to view all the log messages generated from uctv-wizard. These log messages are stored at **/var/log/uctv-installation.log**

  ```
  sudo vi /var/log/uctv-installation.log
  ```

- Use the command below to know the usage descriptions for the individual operations.

  ```
  sudo uctv-wizard help
  ```

Linux UCT-V Installation Scenarios

1. **Zero Touch Installation** - When using a cloud-integrated script to deploy UCT-V in a virtual machine, no interference is required as the script installs and configures everything automatically.
2. **One Touch Installation** - When using .deb or .rpm packages with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.
3. **Two Touch Installation** - When using .deb or .rpm packages with missing prerequisite packages, the platform displays a warning message about the missing packages. You need to install the missing packages using the **sudo uctv-wizard pkg-install** command.

Install Linux UCT-Vs using Manual Configuration

- Install UCT-V from Ubuntu/Debian Package
- Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

1. Download the UCT-V**6.13.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance.

3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.13.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.13.00-amd64.deb
```

4. Modify the file **/etc/uctv/uctv.conf** to configure and register the source and destination interfaces.
The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

> **NOTE:** When you have an active, successful monitoring session deployed, any modification to the UCT-V config file made after the initial setup requires a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress mirror-dst
```

Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-dst
```

Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-src-ingress mirror-src-egress mirror-dst
```

Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

```
# eth0   mirror-src-ingress
# eth1   mirror-src-egress
# eth2 mirror-dst
```

Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

```
# lo mirror-src-ingress mirror-src-egress
# eth0 mirror-dst
```

> **NOTE:** Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.
6. Restart the UCT-V service.

```
$ systemctl restart uctv.service
```

The UCT-V status is displayed as running. Verify the status using the following command:

```
$ systemctl status uctv.service
```

Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

To install from an RPM (.rpm) package on a RedHat, CentOS, or other RPM-based system:

1. Download the UCT-V**6.13.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance.
3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.13.00-x86_64.rpm
$ sudo rpm -i gigamon-gigavue-uctv-6.13.00-x86_64.rpm
```

4. Modify the **/etc/uctv/uctv.conf** file to configure and register the source and destination interfaces.
   The following example registers the eth0 as the mirror source for both ingress and egress traffic and registers eth1 as the destination for this traffic as follows:

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-dst
   ```

   Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

   ```
   # eth0   mirror-src-ingress
   # eth1   mirror-src-egress
   # eth2 mirror-dst
   ```

   Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

   ```
   # lo mirror-src-ingress mirror-src-egress
   # eth0 mirror-dst
   ```

   NOTE: Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.
6. Restart the UCT-V service.
   ```
   $ sudo service uctv restart
   ```

The UCT-V status is displayed as running. Verify the status with the following command:

```
$ sudo service uctv status
```

Notes:

- When UCT-V fails to start due to a "**start-limit-hit**" (caused by repeated restarts within 10 minutes), you should correct the underlying issue first. To clear the failure and allow UCT-V to restart, run the following command:

  ```
  sudo systemctl reset-failed uctv.service
  ```

- After installing UCT-V, refer to Deploy Fabric Components using Generic Mode for platform specific information to configure UCT-V using Third Party Orchestration.

Post Deployment Check:

After installing UCT-V, you can perform the following to verify the version of UCT-V:

1. Enter the command:

   ```
   sudo uctvl uctv-show
   ```

2. Manually execute the following command:

   ```
   export LD_LIBRARY_PATH=/usr/lib/uctv/ssl-lib64/
   ```

Register Linux UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine in two ways:

1. **GigaVUE-FM Orchestration**: Perform the following steps:

   a. Log in to the UCT-V.

   b. Create a local configuration file and enter the following user data. **/etc/gigamon-cloud.conf** is the local configuration file in the Linux platform.

   ```
   Registration:
       token: <Enter the token created in GigaVUE-FM>
   ```

   c. Restart the UCT-V service.

   Linux platform:

   ```
   $ sudo service uctv restart
   ```

   For more details on how to create tokens, refer to .

2. **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of the user to register with GigaVUE-FM. You can register UCT-V toGigaVUE-FM using Third Party Orchestration with the following two modes:
   - Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
   - Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

NOTE: If you have already configured gigamon-cloud.conf file in the /tmp directory, you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and completes the registration process.

Windows UCT-V Installation

Windows UCT-V allows you to select the network interfaces by subnet/CIDR and modify the corresponding monitoring permissions in the configuration file. This options helps you get granular control over the monitored and mirrored traffic.

Refer to the following sections for the Windows UCT-V installation:

- Windows Network Firewall Requirements
- Install Windows UCT-Vs
- Register Windows UCT-V

Windows Network Firewall Requirements

If your environment uses network firewall rules or security groups, you must open specific ports for the virtual machine. For details, refer to Network Firewall Requirement for GigaVUE Cloud Suite.

Notes:

- After installing UCT-V, ensure the following TCP ports are configured:
  - Port 8301 (Inbound)
  - Port 8300 (Outbound)
- You can configure the ports using the following PowerShell commands. Make sure to run PowerShell as **Administrator**:

  1. New-NetFirewallRule -DisplayName "GigaVUE UCT-V (http01_challenge_port)" -Group "Virtual Tap" -Direction "Inbound" -Program "C:\Program Files (x86)\Uctv\step.exe" -LocalPort "8301" -Protocol "TCP" -Action

  2. New-NetFirewallRule -DisplayName "GigaVUE UCT-V (pki_ra_port)" -Group "Virtual Tap" -Direction "Outbound" -Program "C:\Program Files (x86)\Uctv\uctvd.exe" -LocalPort "8300" -Protocol "TCP" -Action Allow

Install Windows UCT-Vs

Rules and Notes:

- VXLAN is the only tunnel type supported for Windows UCT-V.
- Loopback Interface is not supported for Windows UCT-V.
- Before registering Windows UCT-V, generate a token and place it in the **C:\ProgramData\uctv\gigamon-cloud.conf** configuration file. Refer to Configure Tokens.

You can install the UCT-Vs with MSI package using one of the following options:

- Install Windows UCT-Vs using Installation Script
- Install Windows UCT-Vs using Manual Configuration

> The Windows UCT-V MSI is a self-contained package that includes all necessary dependencies. However, during set up, it automatically installs the following components:
>
> - **Visual C++ Redistributable 2019 (x86)**
> - **Npcap (v1.81 OEM)**
>
> Before installing the Windows Agent, ensure that Npcap is not already present on the system. If an existing version of Npcap is present, uninstall it manually to avoid conflicts and ensure compatibility with the version bundled in the UCT-V.

Refer to the following sections for more detailed information and instructions.

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V **`6.13.00`** MSI package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator**.
   The UCT-V service starts automatically.

3. Use the command below to perform pre-check, adapter setup, adapter restore, and configuration functionalities.

   ```
   uctv-wizard
   ```

   Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	uctv-wizard pre-check	Checks the network adapter properties and firewall requirements. It notifies the user if the network adapter's send buffer size is smaller than the required size for the Windows UCT-V and if any firewall rules need to be added. **NOTE:** We recommend to Increase the send buffer size of network adapters to 128 MB during the UCT-V installation to optimize performance and minimize traffic disruption.
adapter-setup	uctv-wizard adapter-setup	Checks the compatible network adapters, increases the send buffer size and restarts the service. Before changing the buffer size, the existing configuration is saved as a backup. You can choose between the following: • If you wish to skip the prompts for changing the buffer size of compatible network adapters, enter the option as **y**. • Enter **N** if you wish to set it up manually. For details, refer to Windows UCT-V Installation.
adapter-restore	uctv-wizard adapter-restore	Using this command, you can restore the backup copy of the network adapter buffer size configuration saved in the in the **uctv-wizard adapter-setup** step. **NOTE:** You need to manually restart the network adapters for changes to take effect immediately. You can choose between the following: • If you wish to skip the prompts for restoring the buffer size of the compatible network adapters, enter the option as **y**. • Enter **N** if you wish to restore it

Options	Use Command	Description
		manually. For details, refer to Windows UCT-V Installation.
configure	uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** location). If available, UCT-V will use that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. • If you wish to skip the prompts to add the required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. • Enter **N** if you wish to configure manually. For details, refer to Windows UCT-V Installation.
uninstall	uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- The log messages generated from uctv-wizard are stored at **/C:\ProgramData\uctv\uctv-installation.txt**
- Use the command below to know the usage descriptions for the individual operations.

```
uctv-wizard help
```

Windows UCT-V Installation Scenarios

1. **Zero Touch Installation**: When using a cloud integrated script to deploy UCT-V in a virtual machine, zero interference is required as the script installs and configures everything automatically.
2. **One Touch Installation**: When using a .msi package with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V**6.13.00** MSI package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator**. The UCT-V service starts automatically.

3. Modify the file **C:\ProgramData\Uct-v\uctv.conf** to configure and register the source and destination interfaces.

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Following are the rules to modify the UCT-V configuration file:
   - Interface is selected by matching its CIDR address with config entries.
   - For the VMs with single interface *(.conf file modification is optional)*:
     - if neither mirror-src permissions is granted to the interface, both mirror-src-ingress and mirror-src-egress are granted to it.
     - mirror-dst is always granted implicitly to the interface.
   - For the VMs with multiple interfaces:
     - mirror-dst is granted explicitly in the config file. Only the first matched interface is selected for mirror-dst, all other matched interfaces are ignored.
     - if none interfaces is granted any mirror-src permission, all interfaces are granted mirror-src-ingress and mirror-src-egress.

   Example 1—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the same interface to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24  mirror-src-ingress mirror-src-egress mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the interface 192.168.2.0/24 to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24   mirror-src-ingress mirror-src-egress
   192.168.2.0/24   mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress
    2001:db8:abcd:ef01::2/64 mirror-dst
   ```

4. Save the file.

5. Restart the Windows UCT-V using one of the following actions:
   - From the command prompt, run **sc stop uctv** and **sc start uctv**.
   - From the Windows Task Manager, restart the UCT-V.

You can verify the status of the UCT-V in the Service tab of the Windows Task Manager.

NOTE: After installing UCT-V, refer to Deploy Fabric Components using Generic Mode for platform specific information to configure UCT-V using Third Party Orchestration.

Register Windows UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine in two ways:

1. **GigaVUE-FM Orchestration**: Refer to the following steps:

   a. Log in to the UCT-V.

   b. Create a local configuration file and enter the following user data. **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.

   ```
   Registration:
       token: <Enter the token created in GigaVUE-FM>
   ```

   c. Restart the UCT-V service.

   Windows platform: Restart from the Task Manager Service

   For more details on how to create tokens, refer to Configure Tokens.

2. **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of user to register with GigaVUE-FM.
   UCT-V can register with GigaVUE-FM using Third Party Orchestration in one of the following two modes:
   - Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
   - Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

NOTE: If you have already configured gigamon-cloud.conf file in the directory (C:\Users\<username>\AppData\Local), you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and complete the registration process.

Install UCT-V OVS Mirroring Module

This is applicable only if you are using UCT-V OVS module as the source of acquiring traffic. You must have sudo/root access to edit the UCT-V OVS module configuration file. Before installing the UCT-V OVS modules, you must have launched the GigaVUE-FM instance. UCT-V OVS module supports a maximum of 255 source interfaces per OpenStack node.

NOTE: After rebooting your workload VM, you must redeploy the respective Monitoring Sessions to restore the mirror traffic on the respective workload VM interfaces.

You can install theUCT-V OVS module either from Debian or RPM packages as follows:

- Install the UCT-V OVS Module from Ubuntu/Debian Package
- Install the UCT-V OVS Module from RPM package

Install the UCT-V OVS Module from Ubuntu/Debian Package

To install from a Debian package:

1. Download the latest version of UCT-V OVS Module Debian (.deb) package from the Gigamon Customer Portal.
2. Copy this package to OpenStack compute nodes. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue-uctv-ovs-agent_6.13.00_amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-ovs-agent_6.13.00_amd64.deb
```

3. Once the UCT-V OVS module package is installed, modify the file **/etc/uctv/uctv.conf** to configure and grant permission to monitor ingress and egress traffic and to transmit the mirrored packets.

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   ```
   br-int mirror-dst

   # Changes for OVS Mirroring
   # This Value will be used as local Ip in OVS Mirror Config
   tunnel-src 172.20.20.11
   # This Value will be used as Next Hop for Tunneled Packets
   tunnel-gw 172.20.20.1
   This Value will be used as local Ipv6 in OVS Mirror Config
   tunnel-src-v6 2001::161
   This Value will be used as Next Hop ipv6 addr for Tunneled Packets
   tunnel-gw-v6 2001::1
   # OVS Agent Mode, Values: auto|standard|dpdk|hw-offload
   ovs-agent-mode auto
   # VLAN Tag value (valid: 0-4094)
   ovs-vlan-tag 2020
   # Egress Interface for OVS Mirrored Traffic
   ovs-egress-if vlan2020
   ```

4. After modifying the UCT-V OVS config file, start the UCT-V service.

   ```
   $ sudo service uctv start
   ```

5. The UCT-V OVS module status will be displayed as running. Check the status using the following command:

   ```
   $ sudo service uctv status
   UCT-V is running
   ```

Install the UCT-V OVS Module from RPM package

To install from an RPM (.rpm) package on a Redhat, CentOS, or other RPM-based system:

1. Download the UCT-V OVS module RPM (.rpm) package from the Gigamon Customer Portal.
2. Copy this package to OpenStack compute nodes. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue-uctv-ovs-agent_6.13.00_x86_64.rpm
$ sudo rpm -ivh gigamon-gigavue-uctv-ovs-agent_6.13.00_x86_64.rpm
```

3. Once the OVS module package is installed, modify the file **/etc/uctv/uctv.conf** to configure and grant permission to monitor ingress and egress traffic and transmit the mirrored packets.

> **NOTE:** When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

```
# br-int mirror-dst

# Changes for OVS Mirroring
# This Value will be used as local Ip in OVS Mirror Config
tunnel-src 172.20.20.11
# This Value will be used as Next Hop for Tunneled Packets
tunnel-gw 172.20.20.1
This Value will be used as local Ipv6 in OVS Mirror Config
tunnel-src-v6 2001::161
This Value will be used as Next Hop ipv6 addr for Tunneled Packets
tunnel-gw-v6 2001::1
# OVS Agent Mode, Values: auto|standard|dpdk|hw-offload
ovs-agent-mode auto
# VLAN Tag value (valid: 0-4094)
ovs-vlan-tag 2020
# Egress Interface for OVS Mirrored Traffic
ovs-egress-if vlan2020
```

4. After modifying the UCT-V OVS config file, start the UCT-V service and verify its status.

```
$ systemctl start uctv.service
$ sudo service uctv status
UCT-V is running
```

- UCT-V OVS module is supported for OpenStack with container-based deployment.
  # Docker name to run the OVS Commands
  docker-name openvswitch_vswitchd
- When you are installing a self-signed RPM package, you must execute the following command to import the signing key into the RPM db.
  `sudo rpm --import /path/to/YOUR-RPM-GPG-KEY`

To upgrade UCT-V OVS module:

- You must backup the **/etc/uctv/uctv.conf** configuration file before upgrading the UCT-V OVS module and uninstall the old OVS modules.
- Follow the same installation procedure to upgrade the UCT-V OVS modules.
- After upgrading the UCT-V OVS module, copy and modify the **uctv.conf** file, stop the UCT-V, and start the UCT-V. Redeploy the Monitoring Session if required.
  `service uctv stop`
  `service uctv start`

Uninstall UCT-V

This section describes how to uninstall Linux UCT-V and Windows UCT-V.

Uninstallation Method

- Linux:
  - Uninstall the UCT-V in Ubuntu/Debian, RPM, Red Hat Enterprise Linux, and CentOS packages
  - Use the following command: **`sudo uctv-wizard uninstall`**
- Windows
  - Uninstall the UCT-V in the MSI package.
  - Use the following command: **`CMD uctv-wizard uninstall`**

NOTE: Uninstall command automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Upgrade or Reinstall UCT-V

You can upgrade UCT-V in your virtual machine using the following options:

- Upgrade UCT-V through GigaVUE-FM (Recommended Method)
- Upgrade UCT-V Manually

Refer to the below sections for detailed information and instructions.

Upgrade UCT-V through GigaVUE-FM (Recommended Method)

Upgrading UCT-V manually involves a series of steps to uninstall, install, and restart the service again. This upgrade method is applicable to both GigaVUE-FM Orchestration and Third Party orchestration. For a list of supported platforms, refer to Install UCT-V.

NOTE: This method is complicated if you need to upgrade UCT-Vs for a large number of VMs. However, you can upgrade UCT-V in the workload VM without any hands-on involvement through GigaVUE-FM.

Refer to the sections below for details and instructions:

1. Upload the UCT-V Images
2. Upgrade the UCT-V

Rules and Notes:

- Upgrade is allowed only to versions 6.9.00 or later. Ensure that the UCT-V Controller version is compatible with the version to which you are upgrading.
- Do not trigger system upgrades or other upgrades at the same time as the UCT-V upgrade.
- You should have Infrastructure Management permission to upgrade the UCT-Vs.
- Currently, you can upgrade the UCT-Vs to n+2 versions and any number of patch releases through GigaVUE-FM.
- Before you proceed with the upgrade, ensure that the UCT-Vs are in a healthy state.
- Make sure that a UCT-V is performing only one active job at a time. If the selected UCT-V is part of another job, you cannot trigger the immediate job using the same UCT-V.
- You must upload a compatible image type to upgrade the UCT-V; otherwise, the UCT-V is rejected for the upgrade job.
- Upgrade through GigaVUE-FM is not applicable to OVS Modules. For OVS tapping, you should upgrade the UCT-Vs manually.

Upload the UCT-V Images

Perform the following steps to upload UCT-V image files in GigaVUE-FM:

1. Go to **Inventory > Virtual** and select your cloud platform.
   The **Monitoring Domain** page appears.
2. Select the **UCT-V Upgrade** drop-down menu and select **Images**.
3. In the **Images** page, click **Upload**. The **Upload Internal Image Files** wizard appears.

4. Select **Choose File**, upload the UCT-V files from your local, and select **Ok**.

   Notes:
   - You can download the UCT-V image files from Gigamon software portal.
   - You can upload a maximum of 15 UCT-V files at a time.
   - The supported file formats are **.deb**, **.rpm**, and **.msi**.
   - Ensure that you do not change the file names. GigaVUE-FM does not accept the image files with modified names.
   - When the upload is in process, GigaVUE-FM does not allow uploading a file with similar type and version.

5. Verify if the uploaded UCT-V images is listed in the **Images** page.

Delete the file

You can delete one or multiple images.

1. In the **Images** page, select **Filter** to find the images based on Image Name, Version, and Image Type.
2. Select the required images.
3. From the Actions drop-down menu, select **Delete** or **Delete All**.

You can only delete those image files that are not associated with any tasks created for the upgrade process.

Upgrade the UCT-V

Follow the steps below to upgrade UCT-V in GigaVUE-FM:

1. In the **UCT-V Upgrade** drop-down menu, select **Dashboard** to view the UCT-V upgrade landing page.
   In the Dashboard page, you can view the upgrade status of individual UCT-Vs and the stages of the upgrade process (Fetch, Install, Verify). The page also displays the overall progress of the upgrade.
2. Select the required UCT-Vs, and from the **Actions** drop-down menu, select **Upgrade**. The **UCT-V Upgrade task** page appears.
3. Enter the task name.
4. In the **Image Version** drop-down menu, select the required version you want to upgrade to from the list of available image versions. You can choose to upgrade immediately or schedule a time for the upgrade to happen.
5. Select the required option in the **Time Selection** field. If you prefer to schedule the upgrade, enter the choice of your date and time in the respective fields.
   Do not schedule the upgrade for a time in the past.

6. Select **Create**.
   The image upgrade task is now created.

   Note:
   - You cannot edit the upgrade task once it is created.
   - You can only reschedule the scheduled task but cannot edit the UCT-V selected for the particular task.
   - In the event of the errors listed below, GigaVUE-FM displays a pop-up message with the list of UCT-Vs that are not compatible for upgrade. Select **Proceed** to ignore the unsupported UCT-Vs and upgrade the compatible ones, or sekect "**Edit**" to modify your changes. The errors include:
     - Controller version is not compatible with the upgrade version.
     - Inconsistency between the uploaded image file type and the selected UCT-V.

You can view the created task details (both immediate and scheduled) in the **UCT-V Upgrade > Jobs** section.

Notes:
- For better progress monitoring, it is recommended to split the upgrade task to a limited number, such as 50 or 100 UCT-Vs.
- When you create a new upgrade task for the same UCT-V, the status of any existing UCT-V changes to 'In Progress' until the latest task is completed. Once the upgrade for the existing tasks is successfully finished, you can create another task for that same UCT-V.

You can view the different stages of the upgrade process in UCT-V Upgrade Dashboard page. Each stage is marked with if it is successful and in case of failure. If the upgrade is successful, GigaVUE-FM updates the upgrade status as **Success** for the selected UCT-V.

Notes:
- The default wait time for the **Upgrade Status** to get updated is 15 minutes.
- The default wait time for the **Image Version** to get updated is 5 minutes.
- In case of failure, you can upgrade the failed instance manually.

Upgrade UCT-V Manually

To upgrade UCT-V manually on a virtual machine, delete the existing UCT-V and install the new version of UCT-V.

NOTE: Before deleting the UCT-V, take a backup copy of the **/etc/uctv/uctv.conf** configuration file. This step avoids reconfiguring the source and destination interfaces.

1. Uninstall the existing UCT-V. Refer to the *Uninstall UCT-V* section in the respective GigaVUE Cloud Suite Deployment Guide.
2. Install the latest version of the new UCT-V. Refer to the Linux UCT-V Installation and the Windows UCT-V Installation topics in the respective GigaVUE Cloud Suite Deployment Guides.
3. Restart the UCT-V service.
   - Linux platform:
     ```
     $ sudo service uctv restart
     ```
   - Windows platform: Restart from the Task Manager.

NOTE: When the openssl version on the UCT-V is upgraded, Monitoring Session needs to be redeployed

Pre-Configuration Checklist for OpenStack

The following table provides information that you would need while launching the visibility components using GigaVUE-FM. Obtaining this information will ensure a successful and efficient deployment of the GigaVUE Cloud Suite for OpenStack.

You can log in to GigaVUE-FM and use the CLI command: **ip host <controller-hostname> <ip-address of the controller>**. (For example: `ip host os-controller1 192.168.2.3`.) Then, add the connection to the OpenStack tenant.

In order for GigaVUE-FM to make a connection to an OpenStack tenant, GigaVUE-FM must be able to resolve the hostname of the OpenStack controller, even if using an IP address in the Identity URL. For example, if GigaVUE-FM is configured to use DNS, and that controller hostname is in the DNS, this will work, and no further configuration will be needed. If not, then you must add a host entry to GigaVUE-FM.

NOTE: If you are not using DNS, you must manually enter the host entry in /etc/hosts on GigaVUE-FM for the OpenStack Controller. On using DNS you can directly enter the host entry in GigaVUE-FM.

	Required Information
☐	Authentication URL
☐	Project Name

	Required Information
☐	Floating IP
☐	Region name for the Project
☐	Domain
☐	SSH Key Pair
☐	Networks
☐	Security groups

Integrate Private CA

You can integrate your own PKI infrastructure with GigaVUE-FM.
To integrate,

1. Generate a Certificate Signing Request (CSR).
2. Get a signature of the Certificate Authority (CA) on the CSR.
3. Upload it back to GigaVUE-FM.

Rules and Notes

- Always place the root CA in a separate file.
- When using multiple intermediate CAs, consider the following:
  - Include all intermediate CAs in a single file in the correct order.
  - Place the last intermediate CA in the chain at the top.
  - Place the preceding CAs in descending order.

Generate CSR

To create an intermediate CA certificate:

1. Go to  **> System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list, select **CSR**. The **Generate Intermediate CA Certificate** page appears.
3. Enter details in the following fields:

   - **Country:** Enter the name of your country.
   - **Organization**: Enter the name of your organization.
   - **Organization Unit:** Enter the name of the department or unit.
   - **Common Name**: Enter the common name associated with the certificate.

4. From the **Algorithm** drop-down list, select the desired encryption algorithm used to encrypt your private key.
5. Select **Generate CSR**.

The CSR is downloaded successfully.

Upload CA Certificate

Get the CSR signed from your Enterprise PKI or any public PKI and upload the signed intermediate CA certificate to GigaVUE-FM.

To upload the signed CA certificate to GigaVUE-FM:

1. Go to **> System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list, select **CA**. The **CA Certificate** page appears.
3. From the **Actions** drop-down list, select **Upload CA**. The **Upload CA** pop-up appears.
4. Next to **Intermediate CA,** select **Choose File** to upload the signed intermediate CA certificate.
5. Next to **Root CA,** select **Choose File** to upload the corresponding root or intermediate CA.

The **CA Certificate** page displays the uploaded CA certificate.

Adding Certificate Authority

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

The CA Certificate chain List page allows you to add the root CA for the devices.

To upload the CA Certificate chain using GigaVUE-FM, follow these steps:

1. Go to **Inventory > Resources > Security > CA List**.
2. Select **Add**, to add a new Custom Authority.
   The **Add Certificate Authority** page appears.
3. In the **Alias** field, enter the alias name of the CA Certificate chain Authority
4. Use one of the following options to enter the CA Certificate chain Authority:
   - **Copy and Paste**: In the **Certificate** field, enter the certificate.
   - **Install from URL**: In the **Path** field, enter the URL in the format: <protocol>://<username>@<hostname/IP address>/<file path>/<file name>. In the **Password** field, enter the password.
   - **Install from Local Directory**: Select **Choose File** to browse and select a certificate from the local directory.

5. Select **Save**.

Create Monitoring Domain

To create a monitoring domain in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > OpenStack**. The Monitoring Domain page appears.
2. On the Monitoring Domain page, click **New**. The **Monitoring Domain Configuration** page appears.

3. Enter or select the appropriate information to configure Monitoring Domain for OpenStack. Refer to the following table for field-level details.

NOTE: For the URL, User Domain Name, Project Domain Name, and Region field values, refer to the RC file downloaded from your OpenStack dashboard.

Field	Description
Monitoring Domain	A name for the monitoring domain. **Note**: You can only view and delete the existing configuration for V Series node 1. You cannot create and perform any other actions on the existing configuration for GigaVUE V Series node 1 as the features are deprecated from GigaVUE-FM fabric manager.
Alias	An alias used to identify the monitoring domain.
URL	The authentication URL is the Keystone URL of the OpenStack cloud. This IP address must be DNS resolvable. Refer to the OpenStack User Manual for more information on retrieving the authentication URL from the OpenStack. **Note**: To ensure the validity of OpenStack 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.
User Domain Name	The domain name of your OpenStack authentication domain. **Note**: • If you are using a separate domain for AUTH, enter that domain name as User Domain Name. • If you are not using a separate domain, you can use the same domain for User and Project Domain Name.
Project Domain Name	The domain name of your OpenStack project.
Project Name	The name of the project used for OpenStack authentication.
Region	The region where the Project resides. You can find your region by running one of these commands, depending on your OpenStack version. **keystone endpoint-list** or **openstack endpoint list** or looking at the RC file in OpenStack to view your credentials.
Username	The username used to connect to your OpenStack cloud. **Note**: If you are using OVS mirroring, you must belong to a role that meets the OpenStack minimum requirements for OVS Mirroring. Refer to OVS Mirroring Prerequisites for more information.
Password	The password of your OpenStack cloud.
Traffic	Select the type of component used to capture traffic for monitoring:

Field	Description
Acquisition Method	• **UCT-V:** If you select UCT-V as the tapping method, the traffic is acquired from the UCT-Vs installed on the VMs. You must configure the UCT-V Controller to monitor the UCT-Vs. • **OVS Mirroring:** If you select OVS Mirroring as your tapping method, the traffic is acquired from the UCT-Vs installed on the hypervisors. You must configure the UCT-V Controller to monitor the UCT-Vs. **Note**: For software release 6.7.00, only OVS Mirroring is supported on RHOSP 17.1 version. • Customer Orchestrated Source**:** If you selectCustomer Orchestrated Source as the tapping method, you can use tunnels as a source where the traffic is directly tunneled to V Series nodes without deploying UCT-Vs or UCT-V Controllers.
Projects to Monitor (Only for OVS Mirroring traffic acquisition method)	This field only appears for OVS Mirroring traffic acquisition method. • Click the **Get Project List** to view the list of projects. **Note**: The **Get Project List** button will only work if all the OpenStack credentials have been provided. Refer to OVS Mirroring Prerequisites. • Select projects that you want to monitor from the list. • You can click **Select None** to clear existing selections or **Select All** to add all available projects to the connection configuration.
Traffic Acquisition Tunnel MTU (Maximum Transmission Unit)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE Cloud Suite V Series node. • For GRE, the default value is 1450. • For VXLAN, the default value is 1400. However, the UCT-V tunnel MTU should be 50 bytes less than the default MTU size.

4. Click **Save**. The **OpenStack Fabric Launch Configuration** page appears. Refer to Configure GigaVUE Fabric Components in GigaVUE-FM for detailed information.

Notes:

- Ensure that all V Series Nodes within a single Monitoring Domain are running the same version. Mixing different versions in the same Monitoring Domain may lead to inconsistencies when configuring Monitoring Session traffic elements.
- Similarly, when upgrading a V Series Node, ensure that the GigaVUE-FM version is the same or higher than the V Series Node version.
- If GigaVUE-FM fails to connect to OpenStack, an error message is displayed specifying the cause of failure. The connection status is also displayed in Audit Logs, refer to About Audit Logs for more information.

Managing Monitoring Domain

You can view the details of the monitoring domain that are created in the list view. The list view details can be viewed based on:

- Monitoring Domain
- Connections Domain
- Fabric
- UCT-Vs

You can also filter the monitoring domain based on a specified criterion. In the monitoring domain page there are two filter options as follows:

- Right filter - Click the Filter button on the right to filter the monitoring domain based on a specific criterion.
- Left filter - Click the  to filter the monitoring domain based on the domain and connections. You can click **+** to create a new monitoring domain. This filter once applied also works even when the tabs are swapped.

To edit or delete a specific monitoring domain, select the monitoring domain, click the ellipses ⋯.

When you click a monitoring domain, you can view details of it in a split view of the window. In the split view window, you can view the details such as Configuration, Launch Configuration and V Series configuration.

Monitoring Domain

The list view shows the following information in the monitoring domain page:

- Monitoring Domain
- Connections
- Tunnel MTU
- Acquisition Method
- Centralized connection
- Management Network

NOTE: Click the  to select the columns that should appear in the list view.

Use the following buttons to manage your Monitoring Domain:

Button	Description
New	Use to create new connection
Manage Certificates	You can use this button to perform the following actions: • **Re-issue**- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments. • **Renew**- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime.

Button	Description
	Auto-renewal is performed based on the duration specified in the **Certificate Settings** page. Refer to Configure Certificate Settings for more details.
Actions	You can select a Monitoring Domain and then perform the following options: • **Edit Monitoring Domain**- Select a Monitoring Domain and then click **Edit Monitoring Domain** to update the configuration. • **Delete Monitoring Domain** - You can select a monitoring domain or multiple monitoring domains to delete them. • **Deploy Fabric** - -You can select a monitoring domain to deploy a fabric, you cannot choose multiple monitoring domains at the same time to deploy fabrics. This option is only enabled when there is No FABRIC (launch configuration) for that specific monitoring domain and GigaVUE-FM orchestration is enabled.. You must create a fabric in the monitoring domain, if the option is disabled • **Upgrade Fabric**-You can select a monitoring domain or multiple monitoring domains to upgrade the fabric. You can upgrade the V Series nodes using this option. • **Delete Fabric**- You can delete all the fabrics associated with the monitoring domain of the selected Fabric. • **Edit SSL Configuration** - You can use this option to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Filter	Filters the Monitoring Domain based on the list view options that are configured: • **Tunnel MTU** • **Acquisition Method** • **Centralised Connection** • **Management Subnet** You can view the filters applied on the top of the Monitoring Domain page as a button. You can remove the filters by closing the button.

Connections Domain

To view the connection related details for a monitoring domain, click the **Connections** tab.

The list view shows the following details:

- Connections
- Monitoring Domain
- Status
- Fabric Nodes
- Credential
- Region

Fabric

To view the fabric related details for a monitoring domain, click the **Fabric** tab.

The list view shows the following details:

- Connections
- Monitoring Domain
- Fabric Nodes
- Type
- Management IP
- Version
- Status - Click to view the upgrade status for a monitoring domain.
- Security groups

You can use the Actions button to perform the following actions:

- **Edit Fabric** - You can select one fabric or multiple fabrics of the same Monitoring Domain to edit a fabric. You cannot choose different fabrics of multiple Monitoring Domains at the same time and edit their fabric components.
- **Delete Fabric** - You can delete all the fabrics associated with the Monitoring Domain of the selected fabric.
- **Upgrade Fabric** - You can select a Monitoring Domain or multiple Monitoring Domains to upgrade the fabric. You can upgrade the GigaVUE V Series Nodes using this option.
- **Restart OVS Traffic** - You can restart the OVS traffic. You can view the **Restart OVS Traffic** option only when you enable the check box **OVS Agent Traffic when V Series unreachable** in **Advanced Settings**. For more information on settings, refer to Configure the OpenStack Settings.
- **Shut Down OVS Traffic** - You can shut down the OVS traffic. You can view the **Shut down OVS Traffic** option only when you enable the check box **OVS Agent Traffic when V Series unreachable** in **Advanced Settings**. For more information on settings, refer to Configure the OpenStack Settings.
- **Generate Sysdump** - You can select one or multiple GigaVUE V Series Nodes (Maximum 10) to generate the system files. The generation of sysdump takes a few minutes in a GigaVUE V Series Node. You can proceed with other tasks, and upon completion, the status appears in the GUI. These system files are helpful for troubleshooting.For more information, refer to Debuggability and Troubleshooting.

To view and manage the generated sysdump files, select the GigaVUE V Series Node and click the **Sysdump** tab in the lower pane.

To view the certificates associated with the fabric, select the fabric nodes and click the **Certificates** tab in the lower pane.

UCT-Vs

To view all the UCT-Vs associated with the available monitoring domains click the **UCT-Vs** tab.

The list view shows the following details:

- Monitoring Domain
- IP address
- Registration time
- Last hearbeat time
- Agent mode
- Status

When an UCT-V is uninstalled, it moves to the Unknown status. If it remains in this state for more than 24 hours, it is considered a stale entry and is automatically removed from GigaVUE-FM every day at 12:30 AM (system time), unless it is part of an active or scheduled upgrade.

Refer to Configure the OpenStack Settings, for information regarding **Settings**.

Configure GigaVUE Fabric Components in GigaVUE-FM

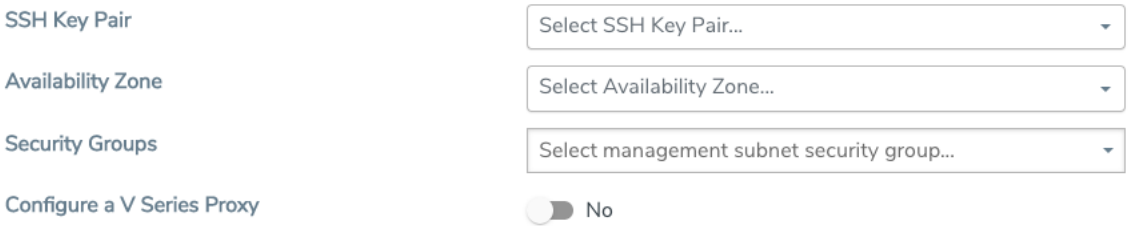
After configuring the Monitoring Domain, you will be navigated to the OpenStack Fabric Launch Configuration page. In the same **OpenStack Fabric Launch Configuration** page, you can configure the following fabric components:

- Configure UCT-V Controller
- Configure GigaVUE V Series Proxy
- Configure GigaVUE V Series Node

In the **OpenStack Fabric Launch Configuration** page, enter or select the required information as described in the following table.

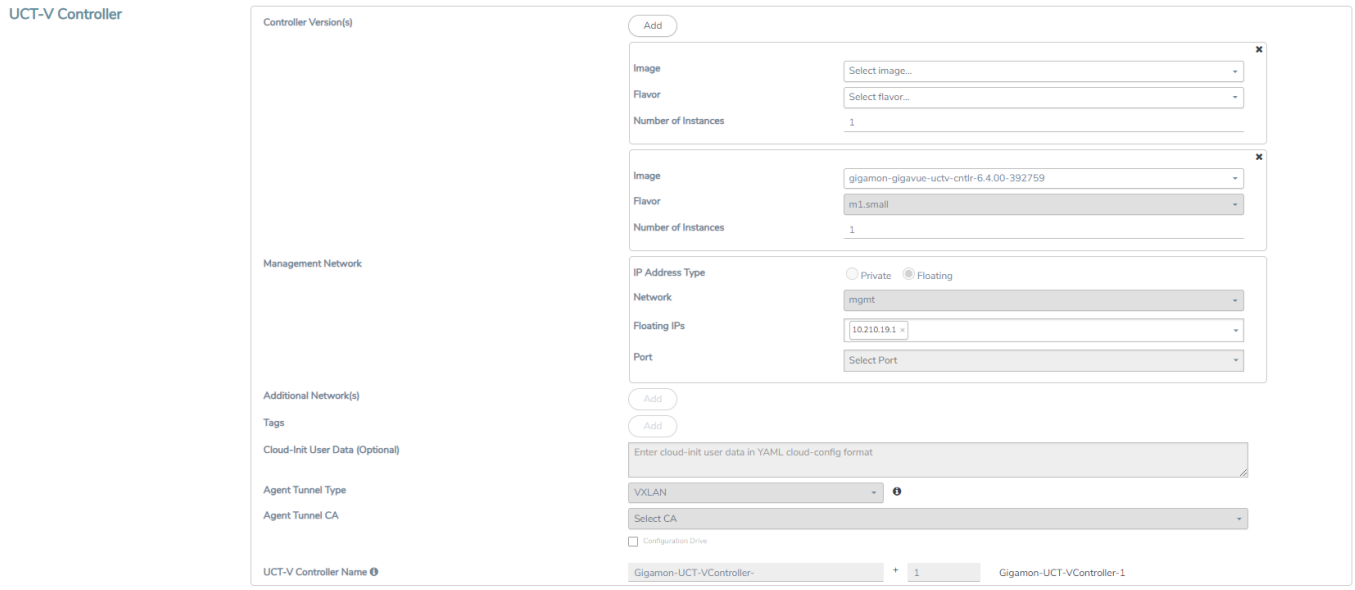
Fields	Description
SSH Key Pair	The SSH key pair for the UCT-V Controller. For more information about SSH key pair, refer to Key Pairs.
Availability Zone	The distinct locations (zones) of the OpenStack region.
Security Groups	The security group created for the UCT-V Controller. For more information, refer to Security Group for OpenStack .
Prefer IPv6	Enables IPv6 to deploy all the Fabric Controllers, and the tunnel between hypervisor to GigaVUE V Series Nodes using IPv6 address. If the IPv6 address is unavailable, it uses an IPv4 address. **Note**: This option can be enabled only when deploying a new GigaVUE V Series Node. If you wish to enable this option after deploying the GigaVUE V Series Node, then you must delete the existing GigaVUE V Series Node and deploy it again with this option enabled.
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.

Select **Yes** to configure a GigaVUE V Series Proxy.



Configure UCT-V Controller

A UCT-V Controller manages multiple UCT-Vs and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes. While configuring the UCT-V Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the UCT-Vs to the GigaVUE V Series nodes.



- Only if UCT-Vs are used for capturing traffic, then the UCT-V Controllers must be configured in the OpenStack cloud.
- A UCT-V Controller can only manage UCT-Vs that have the same version.

Enter or select the required information in the UCT-V Controller section as described in the following table.

Fields	Description
Controller Version(s)	The UCT-V Controller version that you configure must always have the same version number as the UCT-Vs deployed in the instances. For more detailed information refer GigaVUE-FM Version Compatibility Matrix. **Note**: If there is a version mismatch between the UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the agents in the instances. To add UCT-V Controllers: **a.** Under **Controller Versions**, click **Add**. **b.** From the **Image** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances. **c.** From the **Flavor** drop-down list, select a size for the UCT-V Controller. **d.** In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.
Management Network	This segment defines the management network that GigaVUE-FM uses to communicate with UCT-V Controllers, GigaVUE V Series Proxy, and GigaVUE V Series Nodes. **Network** - Select the management network ID. **Ports** - Select a port, you can choose a port related to the selected management network ID. **IP Address Type** The type of IP address GigaVUE-FM needs to communicate with UCT-V Controllers: o **Private**—A private IP can be used when GigaVUE-FM, the UCT-V Controller, or the GigaVUE V Series Proxy reside inside the same project. o **Floating**—A floating IP is needed only if GigaVUE-FM is not in the same project in the cloud or is outside the cloud. GigaVUE-FM needs a floating IP to communicate with the controllers from an external network.
Additional Network(s)	(Optional) If there are UCT-Vs on networks that are not IP routable from the management network, additional networks or subnets must be specified so that the UCT-V Controller can communicate with all the UCT-Vs. Click **Add** to specify additional networks (subnets), if needed. Also, make sure that you specify a list of security groups for each additional network. **Ports**: Select a port associated with the network.
Tag(s)	(Optional) The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-uctv-controllers. There is a specific UCT-V Controller Version for OVS Mirroring and OVS Mirroring + DPDK. To add a tag: a. Click **Add**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-uctv-controllers.

Fields	Description
Cloud-Init User Data (Optional)	Enter the cloud-init user data in cloud-config format.
Agent Tunnel Type	The type of tunnel used for sending the traffic from UCT-Vs to GigaVUE V Series nodes. The options are GRE, VXLAN, and Secure tunnels (TLS-PCAPNG).
Agent Tunnel CA	The Certificate Authority (CA) that should be used in the UCT-V Controller for connecting the tunnel.

Configure GigaVUE V Series Proxy

The fields in the GigaVUE V Series Proxy configuration section are the same as those on the UCT-V Configuration page. Refer to Configure UCT-V Controller for the field descriptions.

Configure GigaVUE V Series Node

Creating a GigaVUE V Series node profile automatically launches the V Series node. Enter or select the required information in the GigaVUE V Series Node section as described in the following table.

Prerequisites

Enable `Host pass through` by editing the *nova.conf* file and changing the *cpu_mode = host-passthrough*

Parameter	Description
Image	Select the GigaVUE V Series node image file.
Flavor	Select the form of the GigaVUE V Series node.
Management Network	For the GigaVUE V Series Node, the Management Network is what is used by the GigaVUE V Series Proxy to communicate with the GigaVUE V Series Nodes. Select the management network ID. **Ports**— Select a port, you can choose a port related to the selected management network ID. **Note**: When both IPv4 and IPv6 addresses are available, IPv6 address is preferred, however if IPv6 address is not reachable then IPv4 address is used.
Data Network	Click **Add** to add additional networks. This is the network that the GigVUE V Series node uses to communicate with the monitoring tools. Multiple networks are supported. • **Tool Subnet**—Select a tool subnet, this is the default subnet that the GigaVUE-FM use to egress traffic to your tools. This subnet must have proper connectivity to your endpoint. • **IP Address Type** ◦ **Private**—A private IP can be used when GigaVUE-FM, the UCT-V Controller, or the GigaVUE V Series Proxy, or the GigaVUE V Series node 2 reside inside the same project. ◦ **Floating**—A floating IP address specified here will be where V Series node 2x.x can be directly managed by GigaVUE-FM or can optionally managed by controllers. • **Network 1**—Select a network type. • **Ports** —Select a port associated with the network. **Note**: • For OVS Mirroring or OVS Mirroring + DPDK deployments, must select **Floating** in the Data Network section and then specify the IPs in the **Floating IPs** field. You can have multiple Floating IPs. • A network provider that is able to receive the monitored traffic may also be used here for OVS Mirroring and OVS Mirroring + DPDK. In this case, you would not need to provide a floating IP; but could select "private" and choose the provider network.

Parameter	Description
Tag(s)	(Optional) The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-uctv-controllers. To add a tag: a. Click **Add**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-uctv-controllers.
Cloud-Init User Data (Optional)	Enter the cloud-init user data in cloud-config format.
Min Instances	The minimum number of GigaVUE V Series nodes to be launched in OpenStack. The minimum number can be 1. • When you deploy an OVS Mirroring or OVS Mirroring + DPDK monitoring session, the V Series nodes will automatically be deployed based on the # of hypervisors being monitored. • When you deploy a UCT-V based monitoring session, the V Series nodes will automatically be deployed based on the # of VMs being monitored and the instance per V Series node ratio defined in the OpenStack Setttings page. **Note**: GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.
Max Instances	The maximum number of GigaVUE V Series nodes that can be launched in OpenStack.
V Series Node Name	(Optional) Enter the name of the V Series Node. The V Series Node name must meet the following criteria: o The entire name can be a minimum of 1 to a maximum of 128 characters. o The suffix must only be a numeral and it should range between 0 to 999999999. o When deploying multiple V Series Nodes, the suffix of the consecutive V Series Node name is updated successively. E.g., 000, 001, 002, 003, etc..

Click **Save** to save the OpenStack Fabric Launch Configuration.

To view the fabric launch configuration specification of a visibility node, click on a visibility node or proxy, and a quick view of the Fabric Launch Configuration appears on the Monitoring Domain page.

Setting MTU for OVS Mirroring

When using OVS (Open vSwitch) port mirroring, it's important to configure the MTU (Maximum Transmission Unit) of VM interfaces correctly to avoid packet fragmentation issues in the data path.

- If the original MTU is 1450, reduce it to 1376:
- Calculation: 1450 - (50 bytes VXLAN header + 24 bytes extra headroom)

- If the original MTU is 8950, reduce it to 8816 using the same logic.

For Example: In an OpenStack deployment with a default MTU of 1450, packets are fragmented at the VM based on this MTU. When mirrored via OVS with VXLAN tunneling (which adds ~50 bytes), the total packet size exceeds the path MTU, causing further fragmentation. This can lead to out-of-order IP frame delivery at the VseriesNode.

Configure GigaVUE Fabric Components in OpenStack

You can use your own OpenStack orchestration system to deploy GigaVUE fabric nodes and use GigaVUE-FM to configure the advanced features supported by these nodes. These nodes register themselves with GigaVUE-FM using the information provided by your OpenStack orchestration system. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM. Health status of the registered nodes are determined by the heartbeat messages sent from the respective nodes.

Recommended Instance Type

The following table lists the recommended instance type for deploying the fabric components:

Fabric Component	Machine type
GigaVUE V Series Node	m1.medium
GigaVUE V Series Proxy	m1.small
UCT-V Controller	m1.small

Keep in mind the following when deploying the fabric components using third party orchestration in integrated mode:

- Traffic Acquisition Tunnel MTU is set to the default value of 1500. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** and click Save.
- When you deploy the fabric components using 3rd party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in OpenStack.
- Create tokens in the **User Management** page in GigaVUE-FM. Refer to Configure Tokens for more detailed information.

- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For more details, refer to the Configure Role-Based Access for Third-Party Orchestration section in the 6.9 Documentation.

In your OpenStack dashboard, you can configure the following GigaVUE fabric components:

- Configure V Series Nodes and Proxy in OpenStack
- Configure UCT-V Controller in OpenStack
- Configure UCT-V in OpenStack

Configure V Series Nodes and Proxy in OpenStack

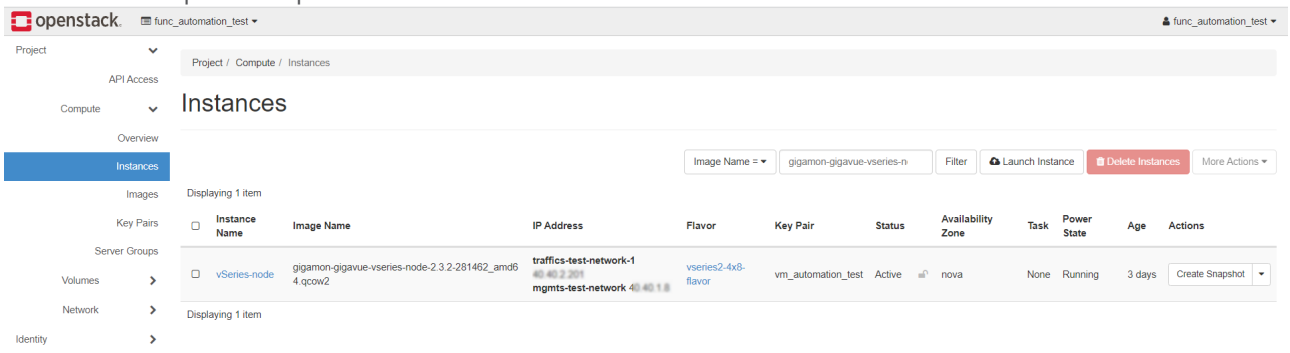
To configure V Series Nodes and V Series Proxy in OpenStack platform:

1. Before configuring GigaVUE fabric components through OpenStack, you must create a monitoring domain in GigaVUE-FM. Refer to Create Monitoring Domain for detailed instructions.
2. In the **Monitoring Domain Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you are going to configure the fabric components in OpenStack Orchestrator.
3. In your OpenStack environment, you can deploy V Series nodes or V Series proxy using the following methods:
   - Register V Series Nodes or V Series Proxy using OpenStack GUI
   - Register V Series Node or V Series Proxy using a configuration file

Register V Series Nodes or V Series Proxy using OpenStack GUI

To register V Series nodes or proxy using the user data in OpenStack GUI:

1. On the Instance page of OpenStack dashboard, click **Launch instance**. The Launch Instance wizard appears. For detailed information, refer to Launch and Manage Instances topic in OpenStack Documentation.



2. On the **Configuration** tab, enter the Customization Script as text in the following format and deploy the instance. The V Series nodes or V Series proxy uses this customization script to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteIP: <IP address of the GigaVUE-FM> or <IP address of the Proxy>
        remotePort: 443
```

- You can register your V Series node directly with GigaVUE-FM or you can use V Series Proxy to register your V Series node with GigaVUE-FM. If you wish to register V Series Node directly, enter the **`remotePort`** value as 443 or if you wish to deploy V Series Node using V Series Proxy then, enter the **`remotePort`** value as 8891.

Register V Series Node or V Series Proxy using a configuration file

To register V Series node or proxy using a configuration file:

1. Log in to the V Series Node or proxy.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following customization script.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteIP: <IP address of the GigaVUE-FM>
    remotePort: 443
```

NOTE: If you wish to register V Series node using V Series proxy then, enter the **`remotePort`** value as 8891.

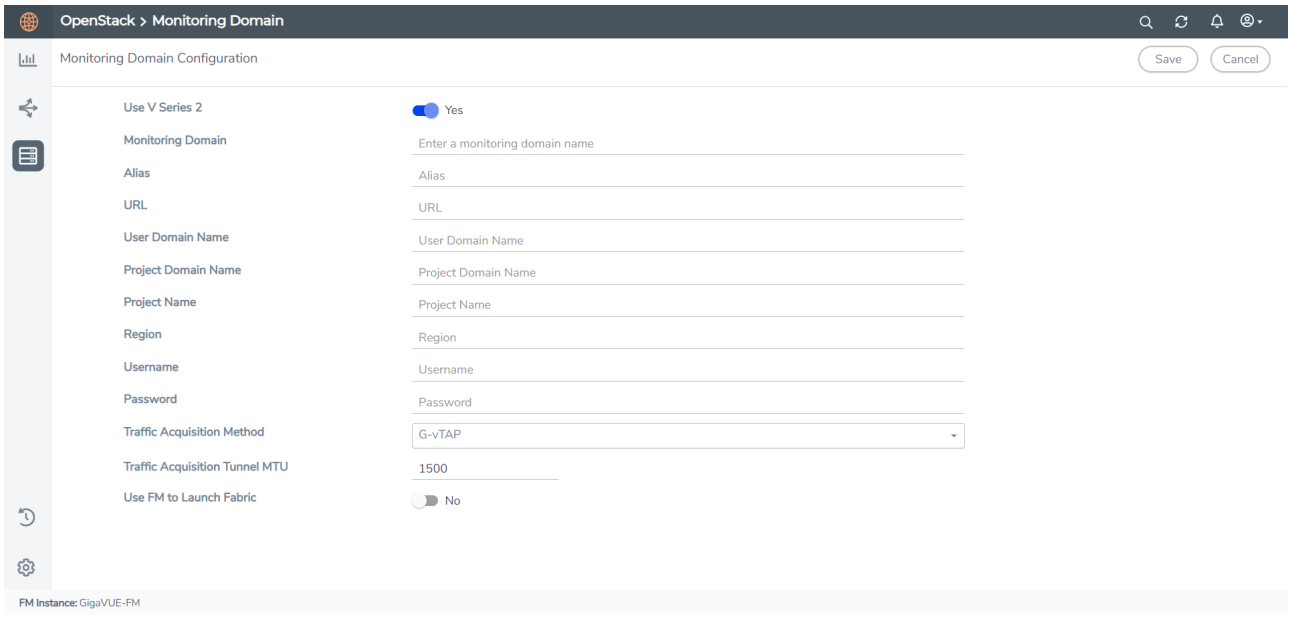
3. Restart the V Series node or proxy service.
   - V Series node:
     ```
     $ sudo service vseries-node restart
     ```
   - V Series proxy:
     ```
     $ sudo service vps restart
     ```

   The deployed V Series node or V Series proxy registers with the GigaVUE-FM. After successful registration the V Series node or proxy sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing ,the visibility node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the V Series node or proxy and if that fails as well then GigaVUE-FM unregisters the V Series node or proxy and it will be removed from GigaVUE-FM.

Configure UCT-V Controller in OpenStack

To configure GigaVUE fabric components in OpenStack platform:

1. Before configuring GigaVUE fabric components through OpenStack, you must create a monitoring domain in GigaVUE-FM. While creating the monitoring domain, select **UCT-V** as the Traffic Acquisition Method. Refer to Create Monitoring Domain for detailed instructions.
2. In the **Monitoring Domain Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you are going to configure the fabric components in OpenStack Dashboard.

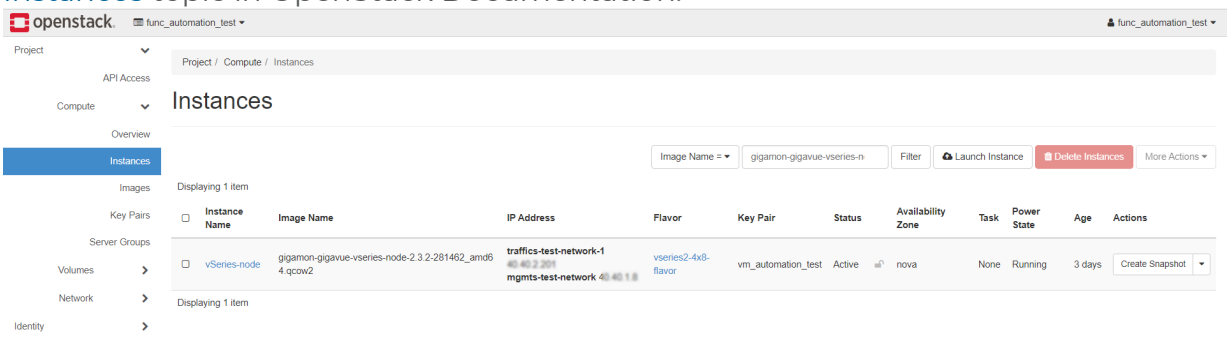


3. In your OpenStack environment, launch the UCT-V Controller using any of the following methods:
   - Register UCT-V Controller using OpenStack GUI
   - Register UCT-V Controller using a configuration file

Register UCT-V Controller using OpenStack GUI

To register UCT-V Controller using the user data in OpenStack GUI:

a. On the Instance page of OpenStack dashboard, click **Launch instance**. The Launch Instance wizard appears. For detailed information, refer to Launch and Manage Instances topic in OpenStack Documentation.



b. On the **Configuration** tab, enter the Customization Script as text in the following format and deploy the instance. The UCT-V Controller uses this customization script to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root
permissions: '0644' content: | Registration: groupName: <Monitoring Domain
Name> subGroupName: <Connection Name> token: <Token> remoteIP: <IP address of
the GigaVUE-FM> sourceIP: <IP address of UCT-V Controller> (Optional Field)
remotePort: 443
```

The UCT-V Controller deployed in OpenStack appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller using a configuration file

To register UCT-V Controller using a configuration file:

a. Log in to the UCT-V Controller.

b. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteIP: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional Field)
    remotePort: 443
```

c. Restart the UCT-V Controller service.

```
$ sudo service uctv-cntlr restart
```

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
```

```
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   $ sudo netplan apply

Configure UCT-V in OpenStack

UCT-V should be registered via the registered UCT-V Controller and communicates through PORT 8891.

NOTE: Deployment of UCT-V through a third-party orchestrator is supported on Linux and Windows platforms. Refer to Linux UCT-V Installation and Windows UCT-V Installation for detailed information.

To register UCT-V using a configuration file:

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to Linux UCT-V Installation and Windows UCT-V Installation.
2. Log in to the UCT-V.
3. Create a local configuration file and enter the following user data.

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteIP: <IP address of the UCT-V Controller 1>,
           <IP address of the UCT-V Controller 2>

    sourceIP: <IP address of UCT-V> (Optional Field)
    remotePort: 8891
```

   - If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:
     localInterface:<Interface to which UCT-V Controller is connected>

4. Restart the UCT-V service.
   - Linux platform:
     $ sudo service uctv restart
   - Windows platform: Restart from the Task Manager.

NOTE: You can configure more than one UCT-V Controller for a UCT-V, so that if one UCT-V Controller goes down, the UCT-V registration will happen through another Controller that is active.

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration the UCT-V sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, UCT-V status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V and if that fails as well then GigaVUE-FM unregisters the UCT-V and it will be removed from GigaVUE-FM.

Key Considerations for Upgrade

Consider the following when upgrading the GigaVUE-FM to 6.1.00 or higher version (when using third party orchestration to deploy fabric components):

When upgrading GigaVUE-FM to any version higher than 6.0.00, if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM is lower than or equal to 6.0.00, then, for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission.

For the user created in GigaVUE-FM,

- Username: **orchestration**
- Password: **orchestration123A!**.

  Verify that the username **orchestration** does not belong to another user in GigaVUE-FM.

After the upgrade, we recommend changing the password on the Users page. For details, refer to Configure Role-Based Access for Third Party Orchestration.

Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack

This chapter describes how to upgradeGigaVUE V Series Proxy and GigaVUE V Series Nodes. For more detailed information about UCT-V Controller, GigaVUE V Series Proxy and Node Version refer GigaVUE-FM Version Compatibility Matrix.

IMPORTANT NOTE:

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

- Create Token in GigaVUE-FM for UCT-V Installation and update it in the configuration file. Refer to Install UCT-Vfor more details.
- Create Tokens for deploying the Fabric Components using Third Party Orchestration. Refer to Configure Tokens for more details.

- Open the required ports in the cloud platform. Refer to Network Firewall Requirement for Cloud Suite] for more details.
- When using FMHA configuration, follow the steps given provided in the Configure Secure Communication between Fabric Components in FMHA section.

Refer to the following topic for more information:

- Prerequisite
- Upgrade UCT-V Controller
- Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

Prerequisite

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

Upgrade UCT-V Controller

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

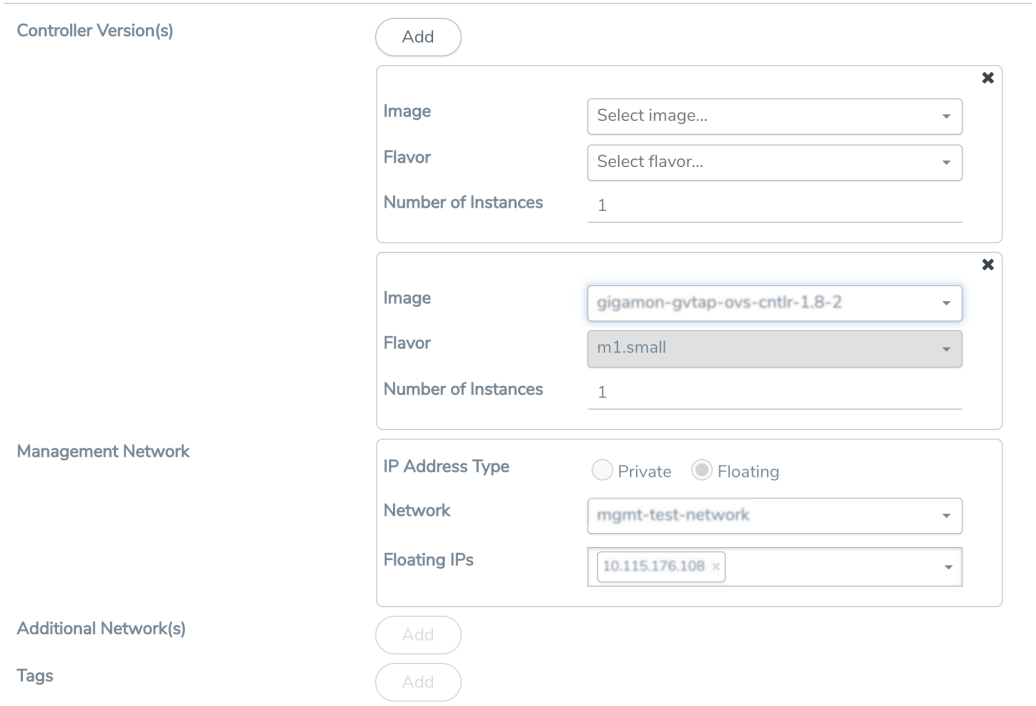
To change the UCT-V Controller version follow the steps given below:

To change UCT-V Controller version between different major versions

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

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

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



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

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

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

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

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

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

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

Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

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

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

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

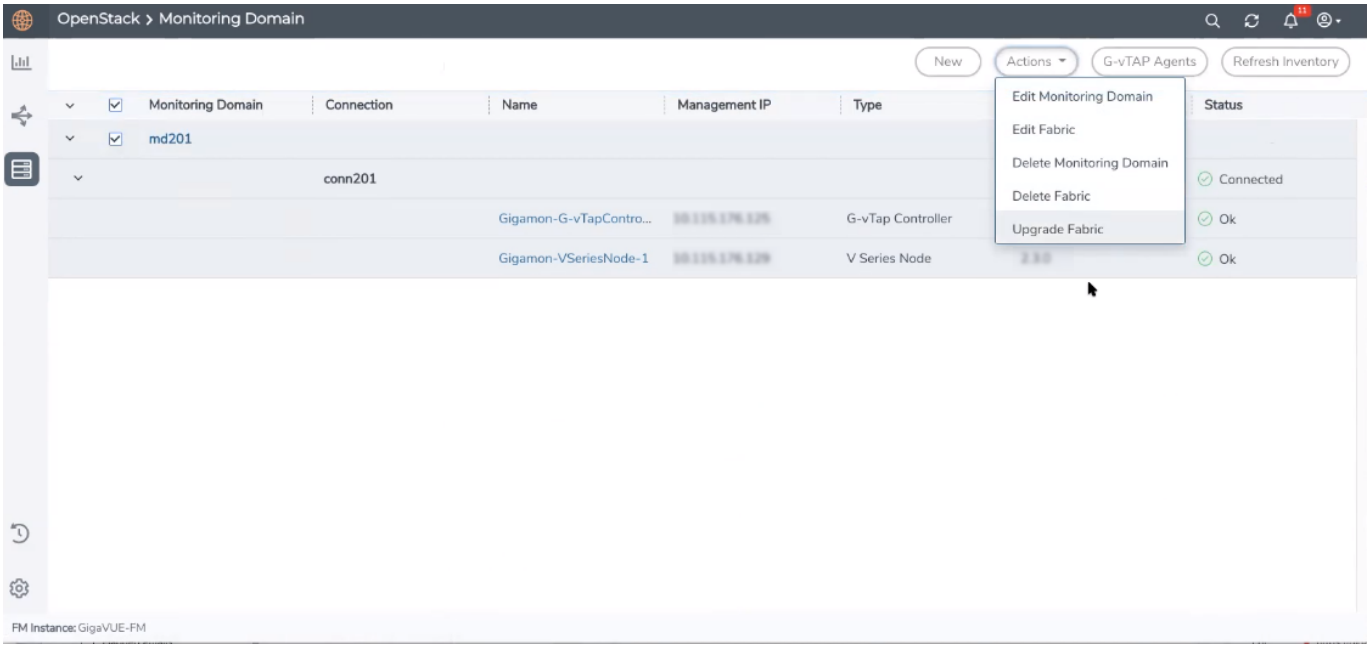
  For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series nodes in your project, you can upgrade all of them at once. First, the new version of GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes are launched. Then, the old version of V Series Proxy and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

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

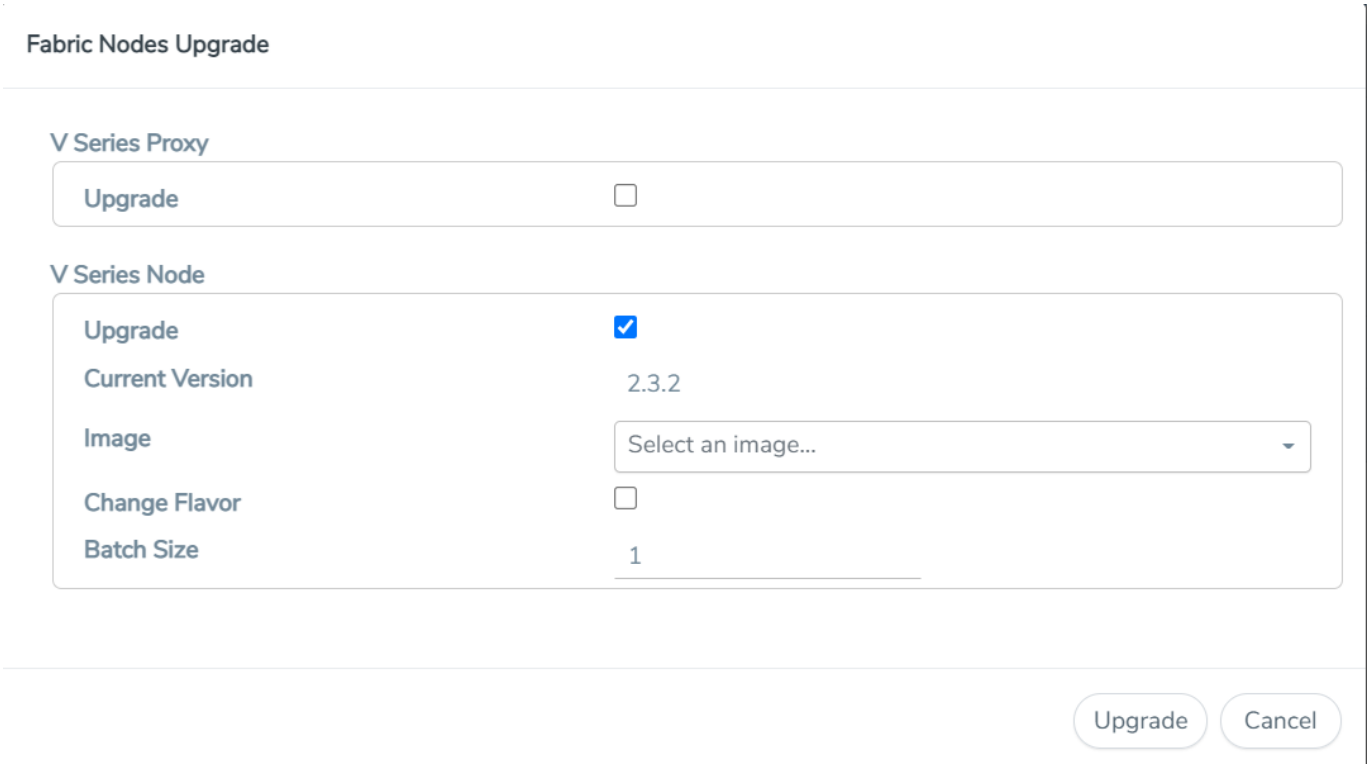
  For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

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

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



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



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

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

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

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

   The monitoring session is deployed automatically.

Configure Secure Communication between Fabric Components in FMHA

IMPORTANT: Before upgrading the Fabric Components to version 6.10 or later, complete the following steps after upgrading GigaVUE-FM to version 6.10 or later.

Follow these steps:

1. Access the active GigaVUE-FM via CLI.
2. Archive the stepCA directory using the following commands:
   ```
   sudo su
   cd /var/lib
   tar -cvf /home/admin/stepca.tar stepca
   ```
3. Set the permissions of the tar file using the following commands:
   ```
   chmod 666 /home/admin/stepca.tar
   ```
4. Copy the tar file to all standby instances in the **/home/admin/ directory** using scp:
   ```
   scp /home/admin/stepca.tar <standby-node>:/home/admin/
   ```
5. Download the **runstepca_fmha** script from the Community Portal.
6. Log in to the standby instance using CLI.
7. Copy the script in the standby instance in the **/home/admin directory** and execute it using the following command:
   ```
   sh /home/admin/runstepca_fmha
   ```

Configure Secure Tunnel (OpenStack)

The Secure tunnels can be configured on:

- Precrypted Traffic
- Mirrored Traffic

Precrypted Traffic

You can send the precrypted traffic through a secure tunnel. When secure tunnels for Precryption is enabled, packets are framed and sent to the TLS socket. The packets are sent in PCAPng format.

When you enable the secure tunnel option for regular and precrypted packets, two TLS secure tunnel sessions are created.

It is recommended always to enable secure tunnels for precrypted traffic to securely transfer the sensitive information.

For more information about PCAPng, refer to PCAPng Application.

Mirrored Traffic

You can enable the Secure Tunnel for mirrored traffic. By default, Secure Tunnel is disabled.

Refer to the following sections for Secure Tunnel Configuration:

- Configure Secure Tunnel from UCT-V to GigaVUE V Series Node in UCT-V
- Configure Secure Tunnel between GigaVUE V Series Nodes

Prerequisites

- While creating Secure Tunnel, you must provide the following details:
  - SSH key pair
  - CA certificate
- Port 11443 should be enabled in security group settings. Refer to Security Group for OpenStack for more detailed information on Network Firewall / Security Group.

Notes

- Protocol versions 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 with a version lower than 6.6.00, if the secure tunnel is enabled in the monitoring session, secure mirror traffic will be transmitted over IPv4, regardless of IPv6 preference.

Configure Secure Tunnel from UCT-V to GigaVUE V Series Node

To configure a secure tunnel in UCT-V, you must configure one end of the tunnel to the UCT-V and the other end to GigaVUE V Series node. You must configure the CA certificates in UCT-V and the the private keys and SSL certificates in GigaVUE V Series node. Refer to the following steps for configuration:

S.No	Task	Description
1.	Upload a CA	You must upload a Custom Certificate to UCT-V Controller to establish a connection with 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. Select **New** to add a new Custom Authority. The **Add Custom Authority** page appears. 3. Enter or select the following information. • Alias - Alias name of the CA. • File Upload - Choose the certificate from the desired location. 4. Select **Save**. For more information, refer to the section Adding Certificate Authority
2.	Upload an SSL Key	You must add an SSL key to GigaVUE V Series node. To add an SSL Key, follow the steps in the section Upload SSL Keys.
3	Enable the secure tunnel	You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE V Series node. To enable the secure tunnel feature follow these steps: **1.** In the Edit Monitoring Session page, click **Options**. The **Monitoring**

S.No	Task	Description
		Session options page appears. 2. Enable the **Secure Tunnel** button. You can enable secure tunnel for both mirrored and precrypted traffic. **Note**: When GigaVUE V Series is upgraded or deployed to 6.5 version, all the existing monitoring sessions will be redeployed, and individual TLS TEPs are created for each UCT-V agent in GigaVUE V Series node.
4.	Select the SSL Key	You must select the added SSL Key in GigaVUE V Series node Key while creating a monitoring domain configuring the fabric components in GigaVUE-FM. To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM If the existing monitoring domain does not have a SSL key, you can add it by following the given steps: 1. Select the monitoring domain for which you want to add the SSL key. 2. Click the **Actions** drop down list and select **Edit SSL Configuration**. An **Edit SSL Configuration** window appears. 3. Select the CA in the **UCT-V Agent Tunnel CA** drop down list. 4. Select the SSL key in the **V Series Node SSL key** drop down list. 5. Click **Save**.
5.	Select the CA	You should select the added Certificate Authority (CA) in UCT-V Controller while creating the monitoring domain configuring the fabric components in GigaVUE-FM. To select the CA certificate, follow the steps in the sectionConfigure GigaVUE Fabric Components in GigaVUE-FM

Configure Secure Tunnel between GigaVUE V Series Nodes

You can create secure tunnel:

- Between two GigaVUE V Series Nodes.
- From one GigaVUE V Series Node to multiple GigaVUE V Series Nodes.

You must have the following details before you start configuring secure tunnels between two GigaVUE V Series Nodes:

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

To configure secure tunnel between two GigaVUE V Series Nodes, refer to the following steps:

<table>
<tr><th>S.No</th><th>Task</th><th>Description</th></tr>
<tr><td>1.</td><td>Upload a CA.</td><td>You must upload a CA Certificate to UCT-V Controller to establish 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 Adding Certificate Authority section.</td></tr>
<tr><td>2.</td><td>Upload an SSL Key.</td><td>You must add an SSL key to GigaVUE V Series node. To add an SSL Key, follow the steps in the section</td></tr>
<tr><td>3</td><td>Create a secure tunnel.</td><td>You should create a secure tunnel to establish a connection between the UCT-V and first GigaVUE V Series Node. To enable the secure tunnel feature follow these steps:
1. In the Edit Monitoring Session page, click Options. The Monitoring Session Options 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.</td><td>Select the SSL Key added in Step 2, while creating a monitoring domain and configuring the fabric components in GigaVUE-FM for the first GigaVUE V Series Node.
You must select the added SSL Key in the first GigaVUE V Series Node.
To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM</td></tr>
<tr><td>5.</td><td>Select the added CA certificate.</td><td>You should select the added Certificate Authority (CA) in UCT-V Controller while creating the monitoring domain. To select the CA certificate, follow the steps in the sectionConfigure GigaVUE Fabric Components in GigaVUE-FM</td></tr>
<tr><td>6</td><td>Create an Egress tunnel from the first GigaVUE V Series Node.</td><td>You must create an egress tunnel for traffic to flow out from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session. Refer to Create a Monitoring Session to know about Monitoring Session.

To create the egress tunnel, follow these steps:
1. After creating a new Monitoring Session, or click Actions > Edit on an</td></tr>
</table>

S.No	Task	Description
		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: • Alias - The name of the tunnel endpoint. • Description - The description of the tunnel endpoint. • Type - Select TLS-PCAPNG for creating egress secure tunnel • Traffic Direction - 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. 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. • IP Version - The version of the Internet Protocol. IPv4 and IPv6 are supported. • Remote Tunnel IP - Enter the interface IP address of the second GigaVUE V Series Node (Destination IP). 4. Click **Save**.
7.	Select the added SSL Key in the GigaVUE V Series Node	You must select the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in the second GigaVUE V Series Node. To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM
8	Create an ingress tunnel in the second GigaVUE V Series node.	You must create a ingress tunnel for traffic to flow in from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session for the second GigaVUE V Series Node. Refer to Create a Monitoring Session to know about monitoring session.

S.No	Task	Description
		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: • Alias - The name of the tunnel endpoint. • Description - The description of the tunnel endpoint. • Type - 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. • Traffic Direction- Choose **In** (Decapsulation) for creating an ingress tunnel that receives traffic from the first GigaVUE V Series Node. Select or enter the values as described in Step 6: • IP Version - The version of the Internet Protocol. IPv4 and IPv6 are supported. • Remote Tunnel IP - Enter the interface IP address of the first GigaVUE V Series Node (Destination IP). **4.** Click **Save**.

Viewing Status of Secure Tunnel

GigaVUE-FM allows you to view the status of secure tunnel connection in UCT-V. You can verify whether the tunnel is connected to the tool or GigaVUE V Series Node through the status.

To verify the status of secure tunnel,

1. Go to **Inventory > VIRTUAL > AWS**, and then select **Monitoring Domain**.
2. In the **Monitoring Domain** page, view the status.

   Tunnel status displays the status of the tunnel. The green color represents that the tunnel is connected and the red represents that the tunnel is not connected.

For configuring secure tunnel, refer to the **Configure Secure Tunnel** section.

Create Prefiltering Policy Template

GigaVUE-FM allows you to create a prefiltering policy template with one or more rules. You can configure a rule with one or more filters. A single monitoring session supports a maximum of 16 rules.

To create a prefiltering policy template,

1. Go to **Traffic > Resources > Prefiltering** and select **UCT-V**.

2. Select **New**.

3. In the **Template Name** field, enter the name of the template,

4. In the **Rule Name** field, enter the name of a rule.

5. Select one of the following options:

- Pass: Allows the traffic.
- Drop: Blocks the traffic..

NOTE: If no prefilter rules are defined, traffic is implicitly allowed. When rules are defined, an implicit drop rule applies. Traffic that does not match any specified rule is dropped.

6. Select one of the following options:

- **Bi-Directional:** Allows the traffic in both directions of the flow. A single Bi-direction rule requires 1 Ingress and 1 Egress rule.
- **Ingress:** Filters incoming traffic.
- **Egress:** Filters outgoing traffic.

NOTE: When using loopback interface in Linux UCT-V, you can use only Bi-directional.

7. Select a priority value from 1-8.

- 1: Select the value as 1 to pass or drop a rule in top priority.
- 2-8 Select the value as 2, 3, 4 to 8, where 8 indicates a rule with the least priority.

  Drop rules are added first based on the priority and then pass rules are added.

8. Select one of the following options as **Filter Type**:

- L3

- L4

9. Select one of the following options **Filter Name**:
   - ip4Src
   - ip4Dst
   - ip6Src
   - ip6Dst
   - Proto: Applies toboth ipv4 and ipv6.
10. Select one of the following options for **Filter Relation**:
    - Not Equal to
    - Equal to
11. In the **Value** field, enter the source or destination port.
12. Select **Save**.

NOTE: Select **+** to add more rules or filters or select **-** to remove a rule or a filter.

To enable prefiltering, refer to Monitoring Session Options.

Create Precryption Template for UCT-V

GigaVUE-FM allows you to filter packets during Precryption in the Data Acquisition at the UCT-V level. This filtering is based on L3/L4 5 tuple information (5-tuple filtering) and the applications running on the workload virtual machines.

Rules and Notes:

- Selective Precryption works with GigaVUE-FM and the fabric components version 6.8.00 or above.
- When a single UCT-V is associated with two different Monitoring Sessions with contrasting pass and drop rules, then instead of prioritizing a single rule, GigaVUE-FM passes all the traffic.
- Once the templates are associated with a Monitoring Session, the changes made in the template are not reflected in the Monitoring Session.

Refer to the section the following sections for more detailed information:

Create Precryption Template for Filtering based on Applications

The application filter allows you to select the applications for which you apply Precryption in the Monitoring Session Options page.

To create,

1. Step Go to **Traffic > Resources > Precryption**.

   The **Precryption Policies** page appear

2. Step Select the **APPLICATION** tab.
3. Select **Add**.

   The New Precryption Template page appears.

4. Select **csv** as the **Type**, if you wish to add applications using a .csv file.
   a. Download the sample .csv file and edit it.
   b. Save your .csv file.
   c. Select **Choose File** and upload the file.
5. Select **Manual** as the **Type** if you wish to add the applications manually.
6. Enter the **Application Name** select + icon to add more applications.
7. Select **Save**.

You can view the added applications in the **APPLICATION** tab.

You can delete a selected application or you can delete all the application using the **Actions** button.

Create Precryption Template for Filtering based on L3-L4 details

To create,

1. Go to **Traffic > Resources > Precryption**. The **Precryption Policies** page appears.
2. Select the **L3-L4** tab.

3. Perform the following steps:

   a. In the **Template** field, enter a name for the template.

   b. In the **Rule Name** field, enter a name for the rule.

   c. For **Action**, select one of the following options:

      - **Pass:** Passes the traffic.
      - **Drop:** Drops the traffic.

      > **NOTE:** In the absence of a Precryption rule, traffic is implicitly allowed. However, the defined rules include an implicit pass all rule. Should the traffic not conform to any of the specified rules, it is passed.

   d. For **Direction**, select one of the following options:

      - **Bi-Directional:** Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
      - **Ingress:** Filters the traffic that flows in.
      - **Egress:** Filters the traffic that flows out.

   e. In the **Priority** field, select one of the following values:

      - 1: Select to pass or drop a rule in top priority.
      - 2 to 8: Select to decide priority where 8 is used for setting a rule with the least priority.

      > **NOTE:** Drop rules are added based on the priority, and then pass rules are added.

f. Select **Filter Type** from the following options:

- L3:
- L4

> **NOTE:** You can use L4 Filter Type only with L3.

For L3, perform the following:

i. Select **Filter Name** from the following options:

- IPv4 Source
- IPv4 Destination
- IPv6 Source
- IPv6 Destination
- Protocol: It is common for both IPv4 and IPv6.

ii. Select **Filter Relation** from any one of the following options:

- Not Equal to
- Equal to

iii. Enter or Select the Value based on the selected **Filter Name**.

> **NOTE:** When using **Protocol** as **Filter Name**, select **TCP** from the drop-down menu.

For L4, perform the following:

i. Select the **Filter Name** from the following options:

- Source Port
- Destination Port

ii. Select the **Filter Relation** from any one of the following options:

- Not Equal to
- Equal to

iii. Enter the source or destination port value.

4. Select **Save**.

NOTE: Select **+** to add more rules or filters. Select **-** to remove a rule or a filter.

The template is successfully created. To enable Precryption, refer to Configure Monitoring Session Options (OpenStack) section.

You can delete a selected template or you can delete all the templates using the **Actions** button.

You can also edit a selected template using **Actions > Edit**.

Configure Monitoring Session

This chapter describes how to setup ingress and egress tunnel, maps, applications in a monitoring session to receive and send traffic to the GigaVUE V Series node. It also describes how to filter, manipulate, and send the traffic from the V Series node to monitoring tools.

Refer to the following sections for details:

Create a Monitoring Session (OpenStack)

You must a Create Monitoring Domain before creating a monitoring session.

GigaVUE-FM automatically collects inventory data on all target instances in your cloud environment. You can design your Monitoring Session to:

- Include or exclude the instances that you want to monitor.
- Monitor egress, ingress, or all traffic.

Target Instance

- When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds it to your Monitoring Session based on your selection criteria. Similarly, when an instance is removed, it updates the Monitoring Sessions.
- For the VPCs without UCT-Vs, targets are not automatically selected. In those cases, you can use Customer Orchestrated Source in the Monitoring Session to accept a tunnel from anywhere.

You can create multiple Monitoring Sessions within one 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. Select **New Monitoring Session** to open the New Monitoring Session configuration page.
3. In the configuration page, perform the following:
   - In the **Alias** field, enter the name of the Monitoring Session.
   - From the **Monitoring Domain** drop-down list, select the desired Monitoring Domain or select **Create New** to create a Monitoring Domain.
     For details, refer to the Create a Monitoring Domain section in the respective cloud guides.
   - From the **Connections** drop-down list, select the required connections to include as part of the Monitoring Domain.
   - From the **VPC** drop-down list, select the required VPCs to include as part of the Monitoring Domain.
   - Enable the **Distribute Traffic** option to identify duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring.Distributed Deduplication is only supported on GigaVUE V Series Node version 6.5.00 and later.
4. Select **Save**.
   The Monitoring Session Overview page appears.

Monitoring Session Page (OpenStack)

The following table outlines the Monitoring Session tabs in OpenStack, each enabling traffic analysis, configuration, and infrastructure visibility.

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. In the **Selection Status** section, you can view the VM status. The status indicates whether the VM is supported, not supported, selected, or not selected. When you hover over the status, a tooltip displays the reason for that status. **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 (OpenStack) 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 (OpenStack) 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 (OpenStack) section for details.
Topology	Displays the fabric and monitored instances based on the connections configured in your network. You can select a specific connection to explore its associated subnets and instances in the topology view, offering a clear visualization of the monitored network elements. Refer to Visualize the Network Topology (OpenStack).

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

NOTE: Ensure that the GigaVUE V Series Node and GigaVUE-FM are time synchronized or configure NTP time synchronization.

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:

- Create a new Monitoring Session
- Rename a Monitoring Session
- Hover over, click the check box of the required Monitoring Session(s) and perform bulk actions (Delete, Deploy, or Undeploy).

Configure Monitoring Session Options (OpenStack)

Configure Monitoring Session Options

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-d efined applications
- Enable Distributed De-duplication

TRAFFIC ACQUISITION

To navigate to **TRAFFIC ACQUISITION** tab,

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select the required Monitoring Session from the list view on the left pane and select the **TRAFFIC ACQUISITION** tab.

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

- Enable Prefiltering
- Enable Precryption

Enable Prefiltering

To enable Prefiltering:

1. In the **TRAFFIC ACQUISITION** page, go to **Mirroring > Edit Mirroring**.
2. Enable the **Mirroring** toggle button.
3. Enable **Secure Tunnel** option if you wish to use Secure Tunnels. Refer to the *Configure Secure Tunnel* section in the respective GigaVUE Cloud Suite Deployment Guide.
4. Select an existing Prefiltering template from the **Template** drop-down menu, or create a new template using **Add Rule** option and apply it. For details, refer to Create Prefiltering Policy Template.
5. Select the **Save as Template** to save the newly created template.
6. Select **Save** to apply the template to the Monitoring Session.

Enable Precryption

Consideration before you enable Precryption:

- To avoid packet fragmentation, 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, ensure that the versions of GigaVUE-FM and the fabric components are 6.6.00 or above.

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

To enable Precryption:

1. In the **TRAFFIC ACQUISITION** page, select **Precryption** tab and click **Edit Precryption**.
2. Enable the **Precryption** toggle button. Refer to Precryption™ topic in the respective cloud guides for details.

3. Apply Precryption to a few selective components based on the traffic:

   NOTE: If you wish to use Selective Precryption, ensure that the versions of GigaVUE-FM and the fabric components are 6.8.00 or above.

   Applications:

   a. Select the **APPLICATIONS** tab.
   The **Pass All Applications** is enabled by default. If you wish to use selective Precryption, disable this option.
   b. Select any one of the following options from **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.
   c. Select **Add**. The **Add Application** widget opens.
   d. Select **csv** as the **Type**, if you wish to add the applications using a .csv file.
   e. Select **Choose File** and upload the file.
   f. Select **Manual** as the **Type**, if you wish to add the applications manually.
   g. Enter the **Application Name** and select + icon to add more applications.
   h. Select **Save**.

   L3-L4

   You can select an existing Precryption template from the **Template** drop-down list, or you can create a new template and apply it. For details, refer to Create Precryption Template for UCT-V.

4. Enable the **Secure Tunnel** option 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 **Overview** tab and check the Traffic Acquisition Options.
- Select **Precryption**, 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 is 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 is all Zeros.

TRAFFIC PROCESSING

To navigate to **TRAFFIC PROCESSING** tab:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select the required Monitoring Session from the 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
- Tool Exclusion

Apply Threshold Template

To apply threshold:

1. In the **TRAFFIC PROCESSING** page, select **Thresholds** under **Options** menu.
2. You can select an existing threshold template from the **Select Template** drop-down list, or you can create a new template using **New Threshold Template** option and apply it.
   For more details on Threshold Template, refer to the Traffic Health Monitoring section.
3. Select **Save** to save the newly created template.
4. Select **Apply** to apply the template to the Monitoring Session.

NOTE: You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

You can also view the related details of the applied thresholds, such as Traffic Element, Metric, Type, Trigger Values, and Time Interval in the **Threshold** window. Select **Clear Thresholds** to clear the applied thresholds across the selected Monitoring Session.

Enable User Defined Applications

To enable user defined application:

1. In the **TRAFFIC PROCESSING** page, click **User Defined Applications** under **Options** menu.
2. Enable the **User-defined Applications** toggle button.
3. Add from the existing applications or create new User-Defined Application from the **Actions** drop-down. Refer to User Defined Application.

Enable Distributed De-duplication

In the TRAFFIC PROCESSING page, click **Distributed De-duplication** under **Options** menu. 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.

Notes:

- Distributed De-duplication is only supported on V Series version 6.5.00 and later.
- From version 6.9.00, Traffic Distribution option is renamed to Distributed De-duplication.

Tool Exclusion

Tool Exclusion helps prevent traffic loops by ensuring monitoring tools are not mistakenly selected as traffic targets during Automatic Target Selection (ATS). This feature is available only when the traffic acquisition method is VPC Traffic Mirroring.

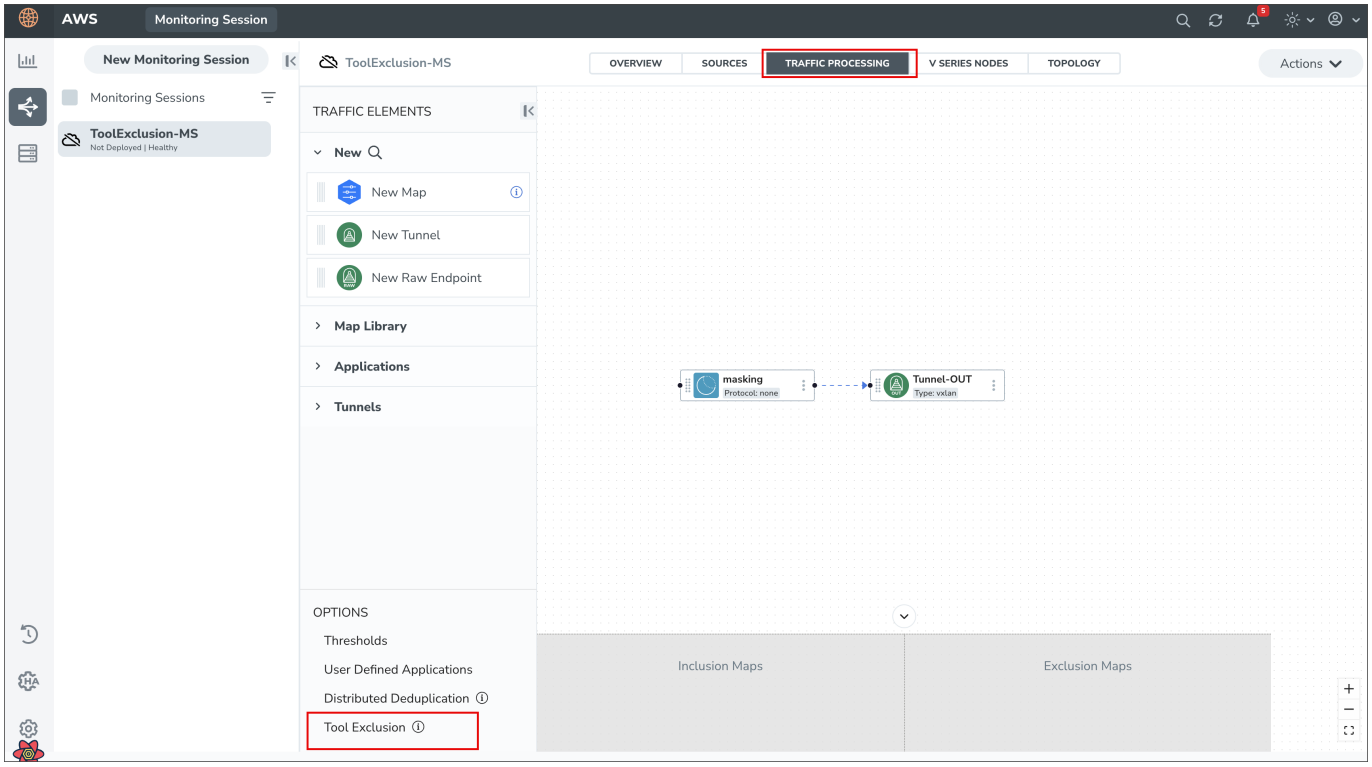
You can exclude tool instances using either of the following methods:

1. **Using AWS Tag Key**

   During deployment, apply the AWS tag key **GigamonExclude:Value** (Any Value) to any instance that acts as a monitoring tool. This tag ensures the system automatically excludes these instances from ATS.

2. **Using the Tool Exclusion Feature in UI**

   During deployment, if the same instance IP is configured as both source (ingress) and tool (egress),the system prompts you to manually identify and exclude tools. Also, you can use the **Tool Exclusion** option to include or exclude tools and targets manually.



Create Ingress and Egress Tunnels (OpenStack)

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

Notes:

- GigaVUE-FM lets you configure ingress tunnels in a Monitoring Session when you use the Traffic Acquisition Method UCT-V.
- The maximum number of links that can egress from any endpoint in V Series is four.

Create a new tunnel endpoint

To create,

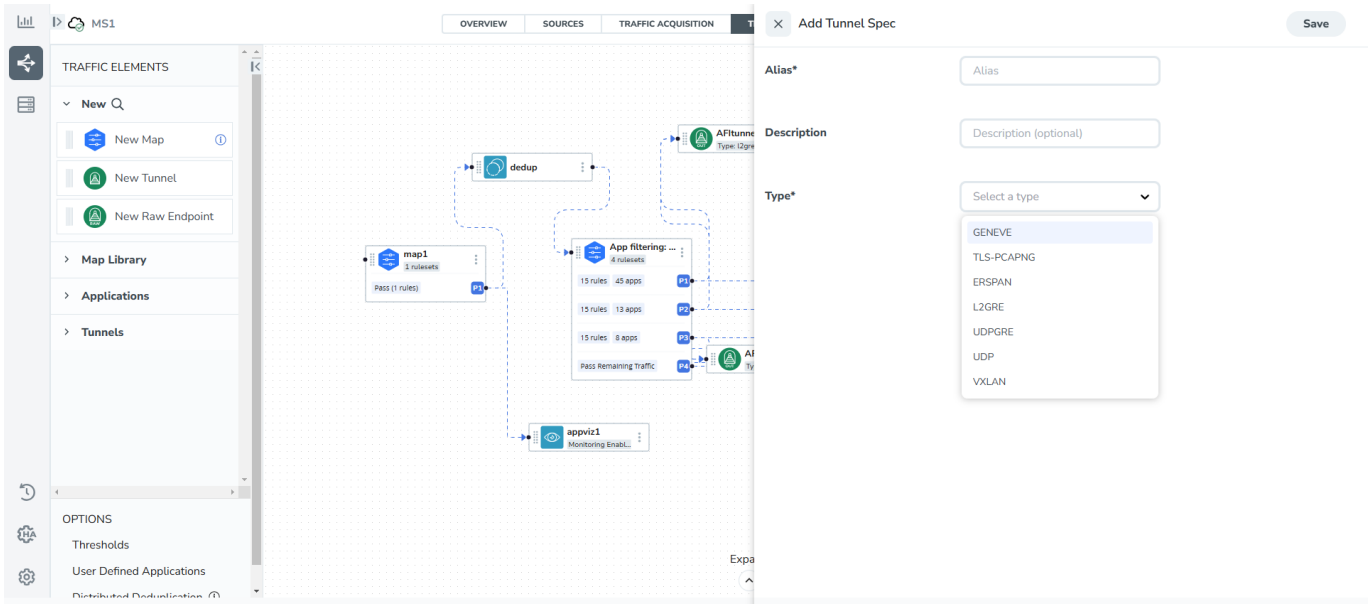
1. Perform one of the following and navigate to the **TRAFFIC PROCESSING** tab:
   - Create a new monitoring session
   - Select **Actions > Edit** on an existing monitoring session.

   The GigaVUE-FM Monitoring Session canvas page appears.

2. On the left pane of the canvas, select the icon to view the traffic processing elements.
3. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace.

   The **Add Tunnel Spec** quick view appears.
4. Enter the **Alias**, **Description**, and **Type** details.

   For details, refer to Details - Add Tunnel Specifications table.
5. Select **Save**.



To delete a tunnel, select the menu button of the required tunnel and select **Delete**.

Apply a threshold template to Tunnel End Points

1. Select the menu button of the required tunnel endpoint on the canvas and click **Details**.
2. In the quick view, go to the **Threshold** tab.

   For details on creating or applying a threshold template, refer to the Monitor Cloud Health topic in the respective Cloud guides.

You can use the configured Tunnel End Points 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. Select the numbers of tunnels displayed in the **OVERVIEW** tab to view the tunnel names and their respective **ADMIN STATUS** and **HEALTH STATUS**.

Table 1: Details - Add Tunnel Specifications

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 or down tools. Each egress tunnel configured on the GigaVUE V SeriesNode has an administrative state that enables GigaVUE-FM to halt the tunnel's traffic flow. GigaVUE-FM only disable the tunnels 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 options below 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 configure secure tunnels on your physical device conveniently. For details, refer to Secure Tunnels.		
In	Choose **In** (Decapsulation) for creating an ingress tunnel to 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 that is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	The port used to establish the connection 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 used to establish 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	

Field	Description
	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.
	Multi Tunnel	Enable the multi-tunnel flag to create multiple tunnels for flow distribution to the 5G-Cloud application. Refer to 5G-Cloud Ericson SCP Support. **Applicable Platforms**: OpenStack, Third Party Orchestration, VMware ESXi **Notes:** ▪ You can configure either a single-tep or multi-tep setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session. ▪ When you enable Multi-Tunnel on a VXLAN tunnel and set the number of tunnels, GigaVUE-FM automatically creates the additional VXLAN tunnel endpoints. Any later changes to the original VXLAN tunnel, such as disabling Multi-Tunnel or modifying Domain Tagging do not update these auto created endpoints. They continue to retain the configuration that existed at the time they were created.

Field	Description	
		To apply updated settings, you must delete the VXLAN TEP and the associated LB application, then recreate the LB and VXLAN TEP with the new configuration, and re-establish the link between them.
	Source L4 Port	The port from which the connection is 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 is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping. **NOTE:** This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to PCAPng Application for details.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an ingress tunnel to 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 routes the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Source L4 Port	The port from which the connection is 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 is 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.		

Field	Description	
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 . For details, refer to the Secure Tunnels.		
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 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.
	Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping. **NOTE:** This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to

Field	Description	
		PCAPng Application for details.
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 . For details, refer to Secure Tunnels section.		

Field	Description	
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 is 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 is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS 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 for a delay.

Field	Description	
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 helps network devices identify the higher or lower priority to handle traffic. 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 is 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 is 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.
	Selective Acknowledgments	Enable the receipt of acknowledgments.
	Sync Retries	Enter the number of times you can try the sync. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable the receipt of acknowledgments when there is a delay.
UDP:		

Field	Description	
Out	**L4 Destination IP Address**	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. For details, refer to Application Metadata Exporter.
	Source L4 Port	The port from which the connection is 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 is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.

Create Raw Endpoint (OpenStack)

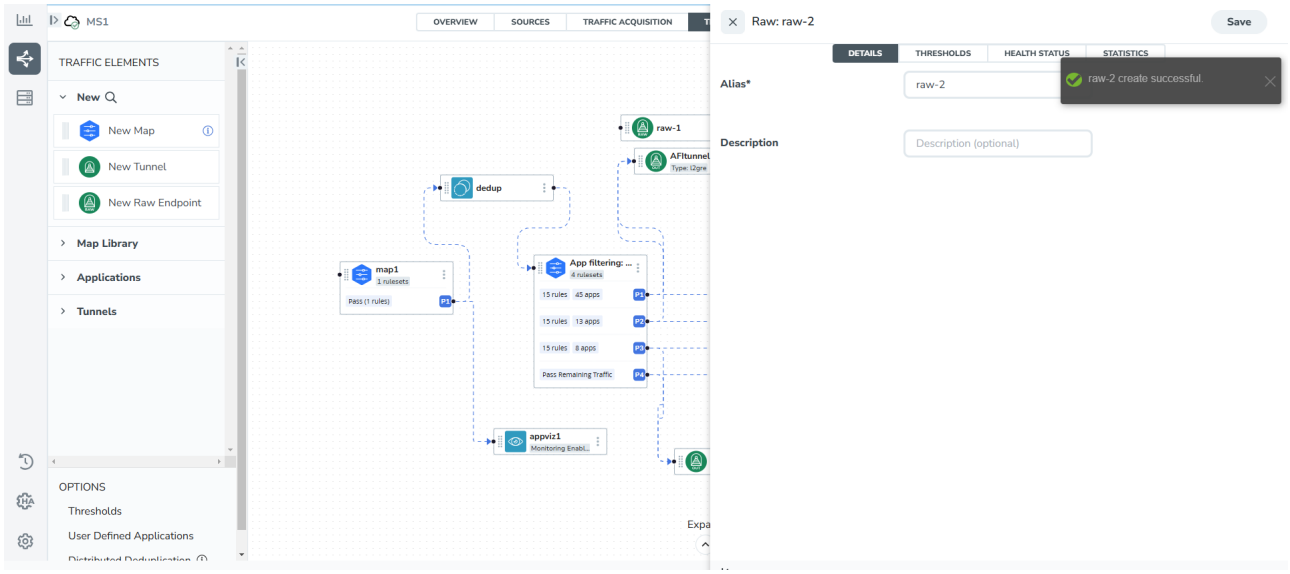
Raw End Point (REP) is used to pass traffic from an interface. REP is used to ingress data from a physical interface attached to GigaVUE V Series Nodes. You can optionally use this end point to send traffic to the applications deployed in the Monitoring Session.

NOTE: The maximum number of links that can egress from any endpoint in V Series is four.

To add Raw Endpoint to the Monitoring Session:

1. Drag and drop **New Raw Endpoint** from the **New** expand menu to the graphical workspace.
2. On the new raw endpoint icon, click the ⋮ menu button and select **Details**. The **Raw** quick view page appears.

3. Enter the Alias and Description details for the Raw End Point and click **Save**.



4. To deploy the Monitoring Session after adding the Raw Endpoint:
   a. Select **Deploy** from the **Actions** drop-down list on the **TRAFFIC PROCESSING** page. The **Deploy Monitoring Session** dialog box appears.
   b. Select the V Series Nodes for which you wish to deploy the Monitoring Session.
   c. 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.
   d. Select **Deploy**.
5. Select **Export** to download all or selected V Series Nodes in CSV and XLSX formats.

Create a New Map (OpenStack)

Terms to know before 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 is 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.

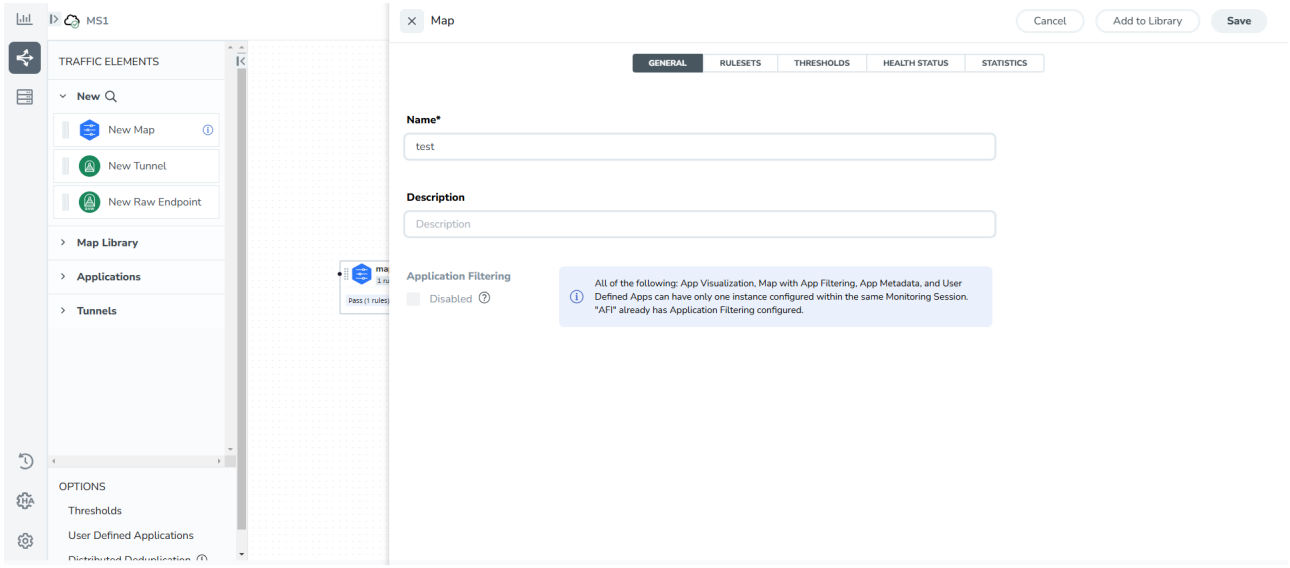
Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, 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 • VM Tag Source The traffic direction is as follows: • 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. **Note**: • 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. • Use the **GigamonNode** Tag to exclude any Gigamon devices from the target. • When using VM Name filter for selecting the Virtual Machines using Inclusion and Exclusion Maps, wild- cards in VM names are not supported. You must use the prefix of the Virtual Machine name.
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 are destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. For details, refer to "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide*.

To create a new map:

1. Drag and drop **New Map** from the **New** expand menu to the graphical workspace. The **Map** quick view appears.



2. On the new Map quick view, select the **General** tab and enter the required information as described below.
   a. Enter the **Name** and **Description** of the new map.
   b. Enable the **Application Filtering** 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.

   NOTE: 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

3. Select the **Rule Sets** tab.
   a. **To create a new rule set:**
      i. Select **Actions > New Ruleset**.
      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. Select **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.
4. Select **Save**.

Through the map, you can drop or pass packets 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. For details, refer to Example- Create a New Map using Inclusion and Exclusion Maps .

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

- To edit a map, select the menu button of the required map on the canvas and click **Details**, or select **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, select on the Thresholds tab. For more details on how to create or apply threshold templates, refer to Monitor Cloud Health.
- Hover over the rules and apps buttons on the map to view the rule and applications configured for the selected map. Select the rules and apps buttons to open the quick view menu for RULESETS.

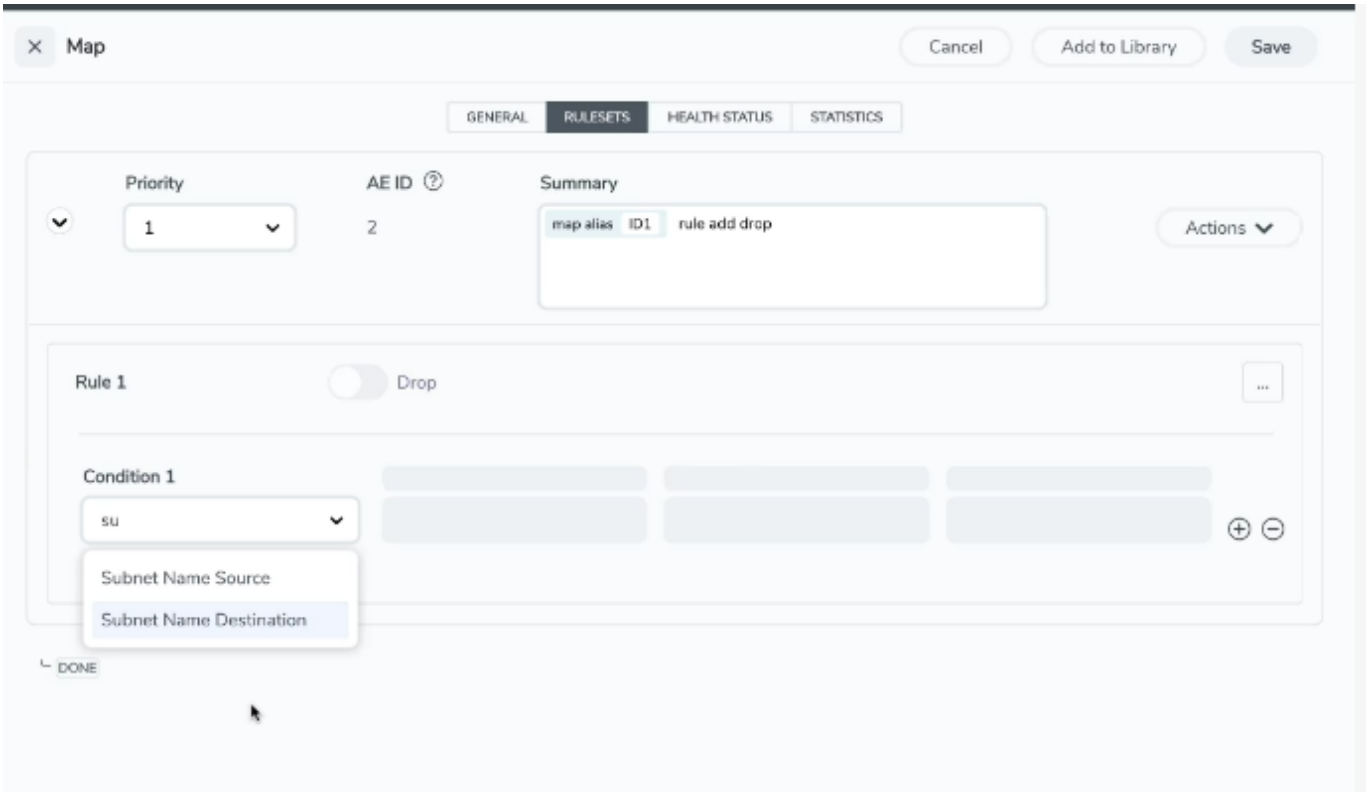
Example- Create a New Map using Inclusion and Exclusion Maps

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. Select 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** is 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** is excluded.

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

Starting from software release 6.8 version, to exclude a subnet, a provision to exclude interfaces based on subnet name is added in the Monitoring Domain as part of Exclusion Maps for OpenStack environment with Traffic Acquisition method as OVS mirroring. To add a subnet to the exclusion map, create an exclusion map and select the Subnet name (Subnet Name Source or Subnet Name Destination) in the ruleset.



Map Library

Map Library is available in the **TRAFFIC PROCESSING** canvas page. You can add and use the maps from the Monitoring Session.

To add a map,

1. From the **Monitoring Session** screen, select **TRAFFIC PROCESSING**.

   The GigaVUE-FMCanvas page appears.

2. From the page, select the desired map and save it as a template.
3. Select **Details**.

   The Application quick view appears.

4. Select **Add to Library** and perform one of the following:
   - From the **Select Group** list, select an existing group.
   - Select **New Group** to create a new one.
5. In the **Description** field, add details, and select **Save**.

The map is added to Map Library. You can use the added map for all the monitoring sessions.

Reusing a map

From the **Map Library**, drag and drop the saved map.

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 (OpenStack)

You can remap interfaces for individual GigaVUE V Series Nodes within a Monitoring Session.

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

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 the **V SERIES NODES** tab and select **Interface Mapping**.

   The **Deploy Monitoring Session** dialog box appears.

3. Select the GigaVUE V Series Nodes to which you wish to map the interface.

4. From the drop-down menu of the GigaVUE V Series Nodes, select the interfaces for the following deployed in the Monitoring Session:

   - REPs (Raw Endpoints)
   - TEPs (Tunnel Endpoints)

5. Select **Deploy**.

   NOTE: The updated mappings take effect when deployed.

Deploy Monitoring Session

You can deploy the Monitoring Session on all the nodes and view the report.

To deploy the Monitoring Session,

1. **Add components to the canvas**
   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. **Connect components**
   Perform the following steps after placing the required items in the canvas.

   a. Hover your mouse on the map

   b. Select the dotted lines

   c. Drag the arrow over to another item (map, application, or tunnel).

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

3. **(Optional) Review Sources**
   Select the SOURCES tab to view details about the subnets and monitored instances.

   The monitored instances and the subnets are visible in orange.

   Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method.

4. **Deploy the Monitoring Session**

   From the **Actions** menu, select **Deploy**.

   After successful deployment on all the V Series Nodes, the status appears as **Success** on the **Monitoring Sessions** page.

View the Deployment Report

You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab.

- When you select the **Status** link, the Deployment Report is displayed.
- When the deployment is incorrect, the Status column displays one of the following errors:
  - **Success:** Not deployed on one or more instances due to V Series Node failure.
  - **Failure:** Not deployed on all V Series Nodes or Instances.

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

The Monitoring Session Deployment includes two key configuration:

- Interface Mapping
- Tool Exclusion

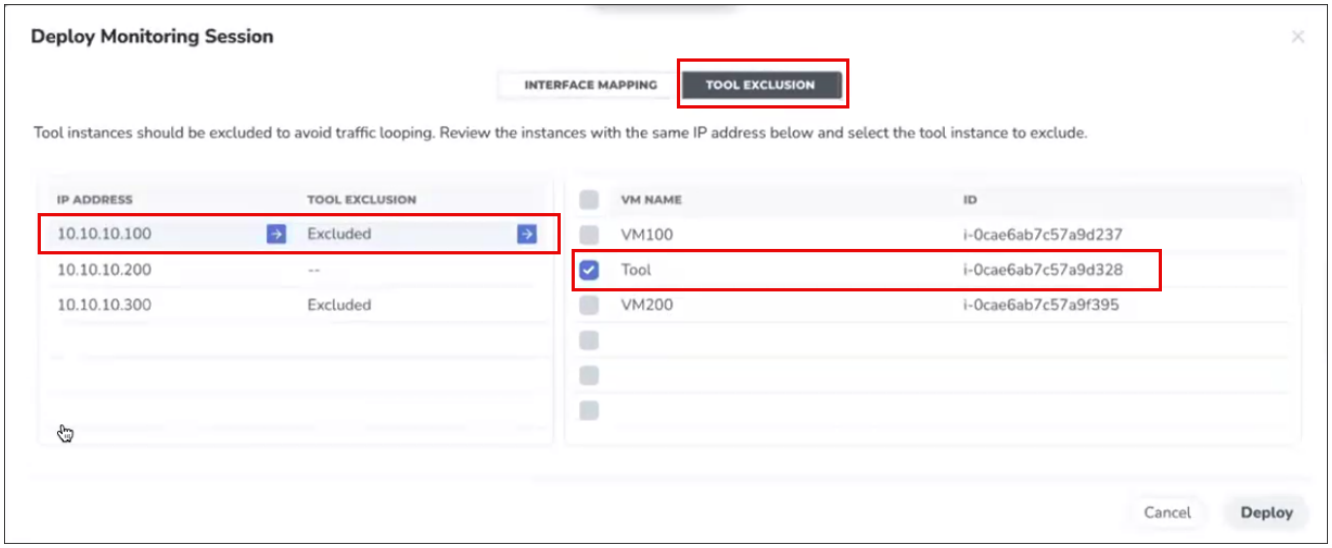
Interface Mapping

It allows to associate specific network interfaces (from monitored instances) with monitoring tools. This ensures that traffic from selected sources is accurately mirrored and routed for analysis. You can:

- Select interfaces from available instances.
- Map each interface to one or more monitoring tools.
- Apply filters or conditions to refine traffic selection.

Tool Exclusion

It excludes specific monitoring tools from receiving mirrored traffic during a monitoring session. This option is available only when the Traffic Acquisition method is set to **VPC Traffic Mirroring**.

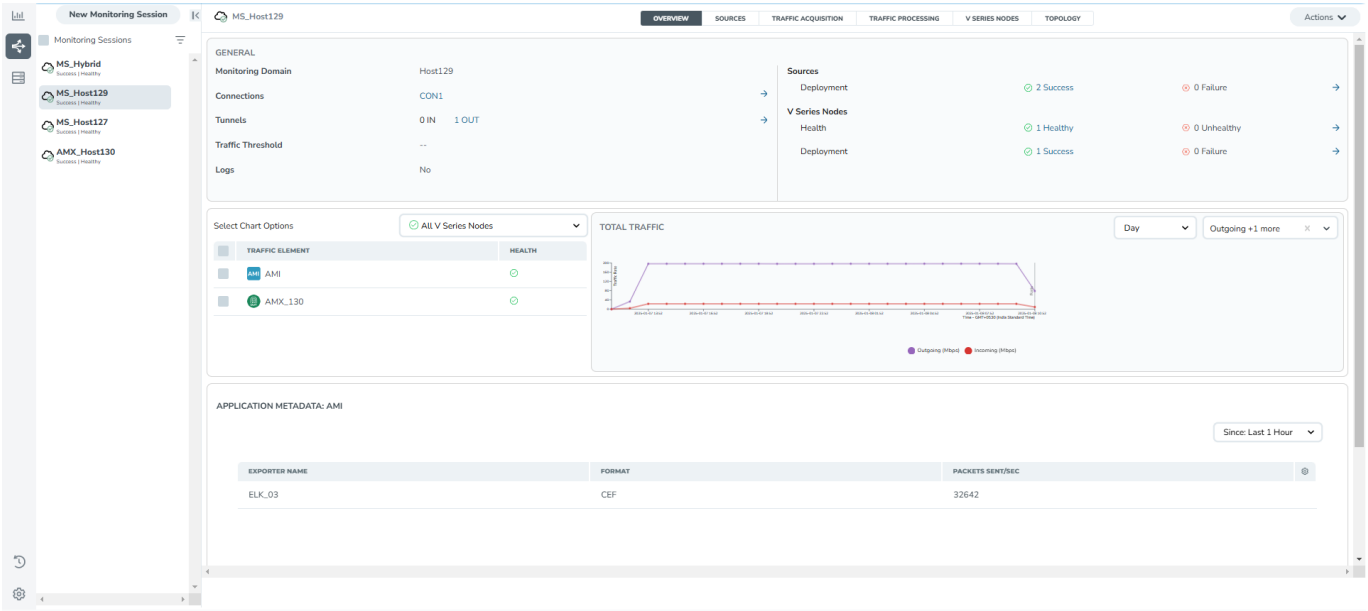


- Review the list of available monitoring tools.
- Select the tools to exclude from traffic flow.
- Confirm the exclusion before deploying the session.

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.

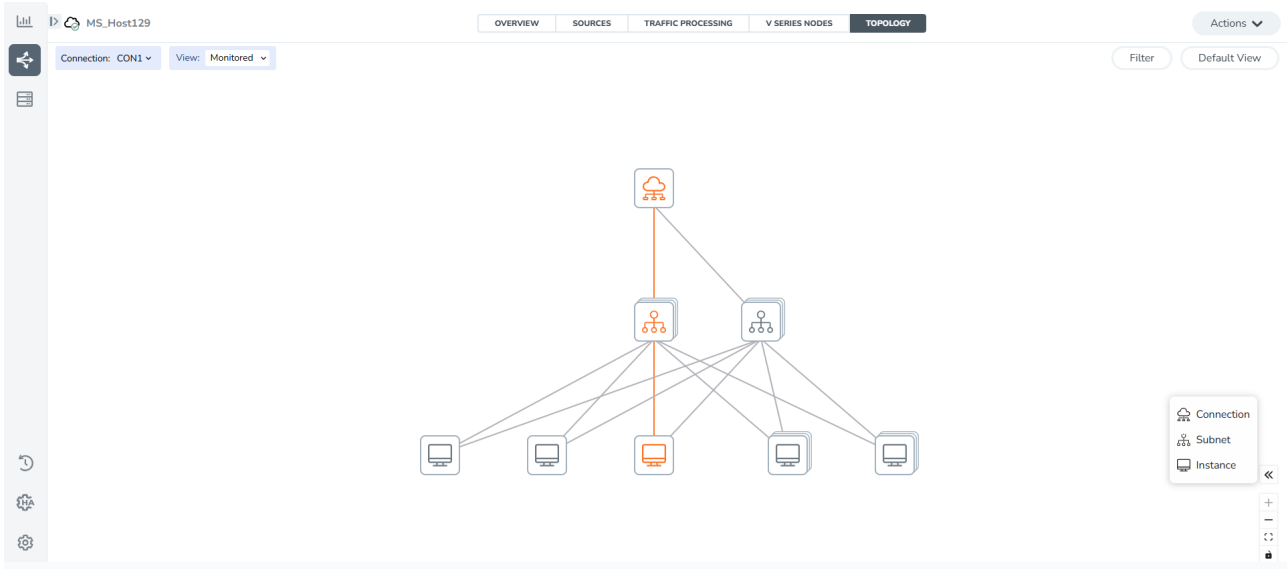
Visualize the Network Topology (OpenStack)

You can have multiple connections in GigaVUE-FM. Each connection can have multiple Monitoring Sessions configured within it. The Topology tab provides a visual representation of the monitored elements within a selected connection and Monitoring Session.

To view the topology in GigaVUE-FM:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Create a Monitoring Session or select an existing Monitoring Session,
3. Open the **TOPOLOGY** tab.
4. From the **Connection** list on the Topology page, select a connection.

   The topology view of the monitored subnets and instances in the selected session is displayed.
5. From **View,** select one of the following instance types:
   - Fabric
   - Monitored



6. (Optional) Hover over the subnet or VM group icons to view details such as the subnet ID, subnet range, and the total number of subnets and instances.
7. Select the subnet or VM group icons to explore the subnets or instances within the group.

In the Topology page, you can also perform the following:

- Use the **Filter** button to filter the instances based on the VM name, VM IP, OS Type, 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 monitored instances.
- Apply Navigation controls, such as:
  - Use the arrows at the bottom-right corner to move the topology page up, down, left, or right.
  - Use **+** or **-** icons to zoom in and zoom out of the topology view.
  - Select the **Fit View** icon to fit the topology diagram according to the width of the page.

Configure Precryption in UCT-V

GigaVUE-FM allows you to turn on or off the Precryption feature for a monitoring session.

To enable or disable the Precryption feature in UCT-V, refer to Create monitoring session.

Rules and Notes

- To avoid packet fragmentation, change the option precryption-path-mtu in the 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.
- Using IPv6 tunnels requires GigaVUE-FM and the fabric components version 6.6.00 or above.

To create a new monitoring session with Precryption, follow these steps:

1. On the left pane in GigaVUE-FM, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
   The **Monitoring Sessions** page appears.
2. Select **New** to open the **Create a New Monitoring Session** page.
3. Enter the appropriate information for the monitoring session:
   a. In the **Alias** field, enter the name of the monitoring session.
   b. In the **Monitoring Domain** field, enter the name of the monitoring domain that you want to select.
   c. In the **Connection** field, enter the desired connection(s) to include as part of the monitoring domain. You can select the connections required for the monitoring domain.
4. Select **Next**. The **Edit Monitoring Session** page appears with the new canvas.
5. Select **Options** button. The Monitoring Session options appear.
6. Select the **Precryption** tab.

7. Enable **Precryption**.
8. Select **Save**. The **Edit Monitoring Session** page appears. You can proceed to create map, tunnels, and add applications.

NOTE: We recommend enabling 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 information, refer to Secure Tunnel .

Validate Precryption connection

To validate the Precryption connection, follow these steps:

- Navigate to the **Monitoring Session** dashboard and check the Precryption option. The **yes** status indicates an active state.
- Select **Status** to view the rules configured.

Limitations

During precryption, the agent generates a TCP message and captures the payload in clear text. It probes the SSL connect and accept APIs to extract Layer 3 and Layer 4 (L3/L4) details from the packet. When the agent receives the SSL data on a specific interface, it sets the default gateway's MAC address as the destination MAC address for the TCP packet. If the gateway is misconfigured, the agent sets the destination MAC address to all zeros.

Monitor Cloud Health

GigaVUE-FM allows you to monitor the traffic and the configuration health status of each monitoring session and its components.

You can view:

- The overall health status of a monitoring session.
- The health status of individual components.

For details, refer to the following topics:

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

Configuration Health Monitoring

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

It supports specific 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	×	×	✓	×	×

Refer to the View Health Status section to view the configuration health status.

Traffic Health Monitoring

GigaVUE-FM monitors the traffic health of the entire Monitoring Session and each individual GigaVUE V Series Node in that session. It checks for issues like packet drops or traffic overflows.

When it detects a problem, GigaVUE-FM updates the health status of the related Monitoring Session. It monitors traffic health in near real-time.

The GigaVUE V Series Node tracks traffic levels. If traffic goes above or below the configured threshold, it alerts GigaVUE-FM. Then, GigaVUE-FM then uses this data to calculate traffic health.

If you deploy GigaVUE-FM and GigaVUE V Series Nodes in different cloud platforms, you must add the GigaVUE-FM public IP address as the Target Address in the Data Notification Interface on the Event Notifications page.

For details, refer to the section in the *GigaVUE Administration Guide* .

This feature supports GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

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

For instructions on creating and applying threshold templates across a Monitoring Session or an application, and viewing the traffic health status, refer to the following topics:

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

Consideration to configure 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 reapplies all the threshold policies associated with that Monitoring Session.
- Deleting the Monitoring Session clears all the threshold policies associated with that Monitoring Session.
- Threshold configuration is applied before deploying a Monitoring Session and remains even if the session is undeployed.
- 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. Refer to Create Threshold Templates and Apply Threshold Template sections for details on Threshold types and Threshold events.

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	1. Difference 2. Derivative	1. Over 2. Under

	8. Rx Errors		
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 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 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
AMX	1. Tx Packets 2. Rx Packets	1. Difference 2. Derivative	1. Over 2. Under

	3. Packets Dropped 4. Ingestor - Rx packets 5. Ingestor - Packets Dropped 6. Ingestor - Rx Octets 7. Ingestor - Octets Dropped 8. Ingestor - Records Dropped 9. Workload - Records Dropped 10. Workload - Req Auth Errors 11. Workload - Req Timedout Errors 12. Workload - Req Errors 13. Exporter - Avg File Size 14. Exporter - File Uploads 15. Exporter - File Uploads Errors 16. Enrichment - One Minute Percent		
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**.

   The **Threshold Templates** page appears.

2. Select **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	
Traffic Element	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. Select **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 these steps:

1. On the left pane in GigaVUE-FM, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. In the **TRAFFIC PROCESSING** tab, select **Options>Thresholds** menu.
3. From the **Select Template** drop-down list, select the template you wish to apply across the Monitoring Session.
4. Select **Apply**.

NOTE: You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

Apply Threshold Template to Applications

Applying threshold template across Monitoring Session does not overwrite the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it overwrites the existing threshold value for that particular application.

To apply the threshold template to a particular application in the Monitoring Session, follow these steps:

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

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

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a Monitoring Session, follow these steps:

1. On the left navigation pane in GigaVUE-FM, go to **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**,
3. Select **Clear Thresholds**.
4. On the **Clear Threshold** pop-up appears, select **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. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
2. Select a Monitoring Session and navigate to the **TRAFFIC PROCESSING** tab.
3. Select the application for which you wish to see the health status and select **Details**. The quick view page appears.
4. Select the **HEALTH STATUS** tab.

This displays the application's **Configuration Health**, **Traffic Health**, and the **Operational Health**, along with the thresholds applied to each.

NOTE: The secure tunnel status is refreshed 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 Operational Health Status of an Application

When you configure the Application Metadata Exporter to use **Kubernetes** as the workload platform, the V Series Node transmits failure and error events to GigaVUE-FM, which processes them and updates the node's health status on the Monitoring Session page. When interacting with Kubernetes workloads, the system may encounter errors while retrieving resources such as pods, services, nodes, or endpoints. Refer to Errors for additional error details.

Operational events for Exporter:

Refer below for message format and messages that indicate common issues that can occur during the operations:

Format: <Server Type>_<Message>

Server Types: CLOUD EXPORT, KAFKA

Message	Description
UPLOAD_MAX_TRIES_EXCEED	Upload retries exceeded the maximum limit **Example**: CLOUDEXPORTER_UPLOAD_MAX_TRIES_EXCEED
REACHABILITY_FROM_AMX_TO_TOOLS	AMX failed to reach the tool (Cloud Exporter server or Kafka server) **Example**: CLOUDEXPORTER_REACHABILITY_FROM_AMX_TO_TOOLS
NO_IP_ADDRESS	No IP address was configured on the interface **Example**: CLOUDEXPORTER_NO_IP_ADDRESS
EXPORTER_UPLOAD_ERROR	Upload to the exporter failed **Example**: CLOUDEXPORTER_EXPORTER_UPLOAD_ERROR

Operational events for Enrichment:

Refer below for message format and messages that indicate common issues that can occur during the operations:

Format: <Operation Type>_<Message>

Operation Types: GETSERVICES, GETPODS, GETNODES, GETENDPOINTSLICES, WATCHALL

Message	Description
K8S_AUTHORIZATION_FAILURE	The request was denied due to insufficient permissions **Example**: GETPODS_K8S_AUTHORIZATION_FAILURE
K8S_AUTHENTICATION_FAILURE	Authentication failed. Verify your credentials **Example**: GETPODS_K8S_AUTHENTICAION_FAILURE
K8S_UNHANDLED_ERROR	An unspecified error occurred. Check the error description

Message	Description
	Example: GETPODS_K8S_UNHANDLED_ERROR

View Health Status for Individual GigaVUE V Series Nodes

You can also 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, select the required Monitoring Session from the list view.
2. In the **Overview** tab, view the health status of the required GigaVUE V Series Node from the chart options.

View Application Health Status for Individual V Series Nodes

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

1. On the Monitoring Session page, select the required Monitoring Session from the list view.
2. On the Overview tab, select the GigaVUE V Series Node from the All V Series Nodes drop-down menu.

   The list view displays the list of applications for the selected GigaVUE V Series Node and the health status of each application.

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. For details, refer to Analytics.

Rules and Notes:

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

- 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.

For details, 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.

How to access the dashboards

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

The following table lists the various virtual dashboards:

Dashboard	Displays	*Visualizations*	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: • 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

Dashboard	Displays	*Visualizations*	Displays
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 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.

Dashboard	Displays	*Visualizations*	Displays
			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 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:	*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.

Dashboard	Displays	*Visualizations*	Displays
	• **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 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. 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.	*App Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	*Visualizations*	Displays
	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. 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 Bytes*	Displays received traffic vs transmitted traffic, in Bytes.
		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 OpenStack

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

- Configure the OpenStack Settings
- Role Based Access Control
- About Audit Logs
- About Events

Configure Certificate Settings

To configure certificate settings:

1. Go to **Inventory > VIRTUAL**.
2. Select your cloud platform.
3. Select **Settings > Certificate Settings**.
   The **Certificate Settings** page appears.
4. From the **Algorithm** drop-down list, select the algorithm that determines the cryptographic security of the certificate.

   NOTE: If selecting RSA 8192, the certificate generation may take longer due to the increased key size.
5. In the **Validity** field, enter the total validity period of the certificate.
6. In the **Auto Renewal** field, enter the number of days before expiration of the auto-renewal process should begin.
7. Select **Save**.

Configure the OpenStack Settings

To configure the OpenStack Settings:

1. Go to **Inventory > VIRTUAL > OpenStack,** and then click **Settings**.
2. Click the **Settings** drop-down, and then select **Advanced Settings**.
3. Click **Edit** to edit the Advanced Settings fields.

Refer to the following table for descriptions of the Settings fields.

Settings	Description
Refresh interval for VM target selection inventory (secs)	Specifies the frequency for updating the inventory of VMs in OpenStack.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for updating the inventory of GigaVUE fabrics in OpenStack.
Number of UCT-Vs per V Series Node (applicable only for UCT-V based connections)	Specifies the maximum number of instances that can be assigned to the V Series node.
Number of hypervisors per V Series Node (applicable only for OVS mirroring)	Specifies the maximum number of hypervisors that can be assigned to the V Series node.
Refresh interval for UCT-V inventory (secs)	Specifies the frequency for discovering the UCT-Vs available in the project. This is applicable for UCT-Vs only. **Note**: When you upgrade to version 6.5 or above, GigaVUE-FM resets the UCT-V Refresh Interval field to its default. To retain your custom value, you must manually reconfigure it.
OVS Mirror tunnel range start	Specifies the startup range value of the OVS mirror tunnel ID. This is applicable for UCT-V OVS modules only.
OVS Mirror tunnel range end	Specifies the closing range value of the OVS mirror tunnel ID. This is applicable for UCT-V OVS modules only.
Traffic distribution tunnel range start	Specifies the start range value of the tunnel ID.
Traffic distribution tunnel range end	Specifies the closing range value of the tunnel ID.
Traffic distribution tunnel MTU	Specifies the MTU value for the traffic distribution tunnel.
OVS Agent Traffic when V Series is down	Enable this option to stop the OVS module from sending the traffic to the V Series node. You can stop the traffic either manually or automatically. Refer to Shutdown or Restart of OVS traffic to know more about the manual or automatic shut down and restart.
Use UCT-V conf file	Enable this option to allow interface mirroring to follow the configuration defined in the file. Disable it to mirror traffic from all physical interfaces. **Note**: • When changing the UCT-V conf file option from **enabled to disabled**, ensure to undeploy the Monitoring Session and delete the Monitoring Domain. Once changed, you should create a new Monitoring Domain and configure the Monitoring Session.

Settings	Description
	• When changing the UCT-V conf file option from **disabled to enabled**, do the following: 1. Edit the uctv.conf file a. **Windows**: C:\ProgramData\Uctv\uctv.conf b. **Linux**: /etc/uctv/uctv.conf 2. Delete the skipConf file from the backup folder a. **Windows**: C:\ProgramData\Uctv\bak\skipConf b. **Linux**: /var/lib/uctv/bak/skipConf 3. Restart the UCT-V a. **Windows**: Restart from the Task Manager b. **Linux**: sudo service uctv restart
Un-Registration Timeout For FabricNode (secs)	Specify the unregistration wait time between 150 to 900 seconds to control how long GigaVUE-FM waits before removing an unhealthy node; the default is 150 seconds.
Reboot threshold limit for UCT-V Controller down	Specifies the number of times GigaVUE-FM tries to reach UCT-V Controller, when the UCT-V Controller moves to down state. GigaVUE-FM retries every 60 seconds.

- UCT-V OVS module supports a maximum of 255 source interfaces per OpenStack node.
- A maximum of 100 OpenStack connections are allowed for an OpenStack module.

Shutdown or Restart of OVS traffic

GigaVUE-FM allows you to stop or restart the traffic through OVS Mirroring based on the availability of V Series node.

GigaVUE-FM helps you to stop the traffic when the V Series node is unreachable or unrecoverable, and restart it when the GigaVUE V Series Node is reachable again in the following ways:

- Manual shutdown or restart of OVS traffic
- Automatic shutdown or restart of OVS traffic

Manual shutdown or restart of OVS traffic

The traffic sent from the OVS Mirroring Module can be manually stopped and started.

To shut down or restart the OVS traffic manually, follow these steps:

1. Go to **Inventory > VIRTUAL > OpenStack,** and then click **Settings**

2. Click the **Settings** drop-down, and then select **Advanced Settings**.
3. Enable the check box **OVS Agent Traffic when V Series is down**.
4. Click the **Fabric** tab.
5. Select the V Series node.
6. Click the **Actions** drop-down list and select **Shut down OVS Traffic** or **Restart OVS Traffic** as required.

NOTE: You can view the **Shut down OVS Traffic** or **Restart OVS Traffic** options only when you enable the check box **OVS Agent Traffic when V Series is down** in the Advanced Settings.

Automatic shutdown or restart of OVS traffic

When the GigaVUE Cloud Suite V Series node is deleted or changed to an unrecoverable state in the OpenStack platform, GigavUE-FM performs the action as explained in the following table:

V Series node Status in OpenStack	Action in GigaVUE-FM	Action in GigaVUE-FM when you enable the option
When a V Series node is deleted from the OpenStack platform	GigaVUE-FM automatically sets the status of that V Series node as terminated.	In the **Advanced Settings**, when the **OVS Agent Traffic when V Series is down** checkbox is enabled, GigaVUE-FM removes the source interfaces of OVS Mirroring module
When a V Series Node is changed to a stopped or shutoff state in Openstack	GigaVUE-FM Health monitoring module tries to start the V Series node. If unsuccessful after two attempts, GigaVUE-FM considers the V Series node to be unrecoverable.	In the **Advanced Settings**, when the **OVS Agent Traffic when V Series is down** checkbox is enabled, GigaVUE-FM removes the source interfaces of OVS Mirroring module.

V Series node Status in OpenStack	Action in GigaVUE-FM	Action in GigaVUE-FM when you enable the option
When a V Series node is in an active state and its connection to GigaVUE-FM is restored	GigaVUE-FM Health Monitoring module determines V Series Node is in a healthy state.	In the **Advanced Settings**, when the **OVS Agent Traffic when V Series is down** checkbox is enabled, GigaVUE-FM adds the source interfaces of the OVS Mirroring module and restarts the OVS traffic.

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 • Threshold Template • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps	• Create, Clone, and Deploy Monitoring Session • Create and Apply Threshold Template • Add Applications to Monitoring Session • Create Maps • View Statistics • Create Tunnel End Points
Third Party Orchestration: This includes the following resource: • Cloud Orchestration	Deploy the fabric components using Third Party Orchestration. Refer to Configure Role-Based Access for Third Party Orchestration for more details on how to create users, roles, and user groups for Third Party Orchestration.

NOTE: Cloud APIs are also RBAC enabled.

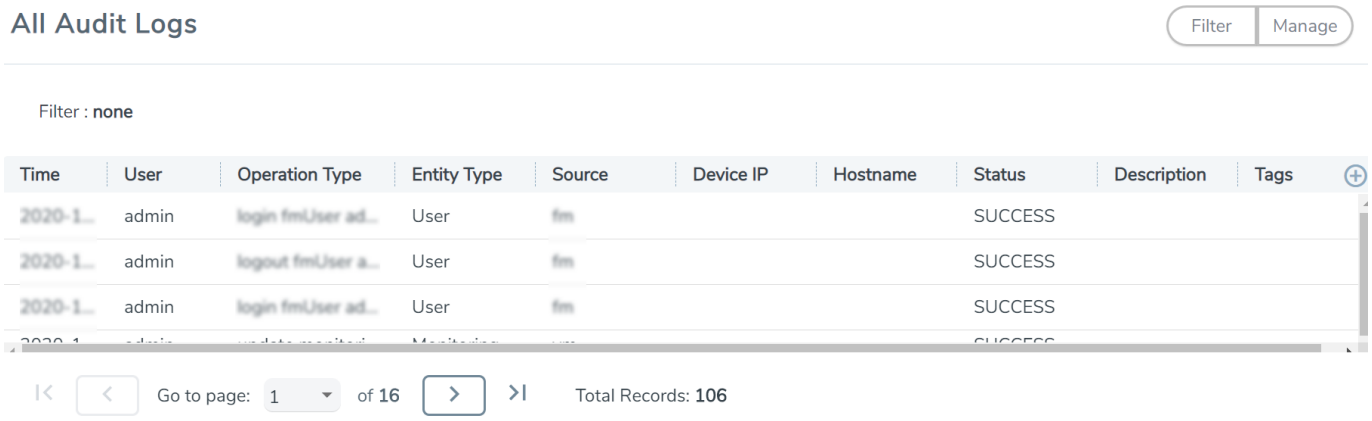
Refer to the *GigaVUE Administration Guide* for detailed information about Roles, Tags, User Groups.

About Audit Logs

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

Access Audit Logs

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



Parameters

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 the system logs. For example, ▪ Log in and Log out based on users. ▪ Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details about the usage either in GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	For failed status provides a brief update on the reason..

NOTE: Verify if the GigaVUE-FM time is set correctly to ensure accuracy of the captured trending data.

Filtering the audit logs

You can filter to view specific type of logs based on the following criteria:

- **When**: Displays logs that occurred within a specified time range.
- **Who**: Displays logs related to a particular user or users.
- **What**: Displays logs for one or more operations, such as Create, Read, and Update.

- **Where**: Displays logs for GigaVUE-FM or devices.
- **Result**: Displays logs for success or failure.

To filter the audit logs,

1. Select **Filter**.

   A quick view for Audit Log Filters displays.

2. Specify one 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. 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. Select **OK** to apply the selected filters to the **Audit Logs** page.

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 occurs at a specific point in time. Examples of events include:

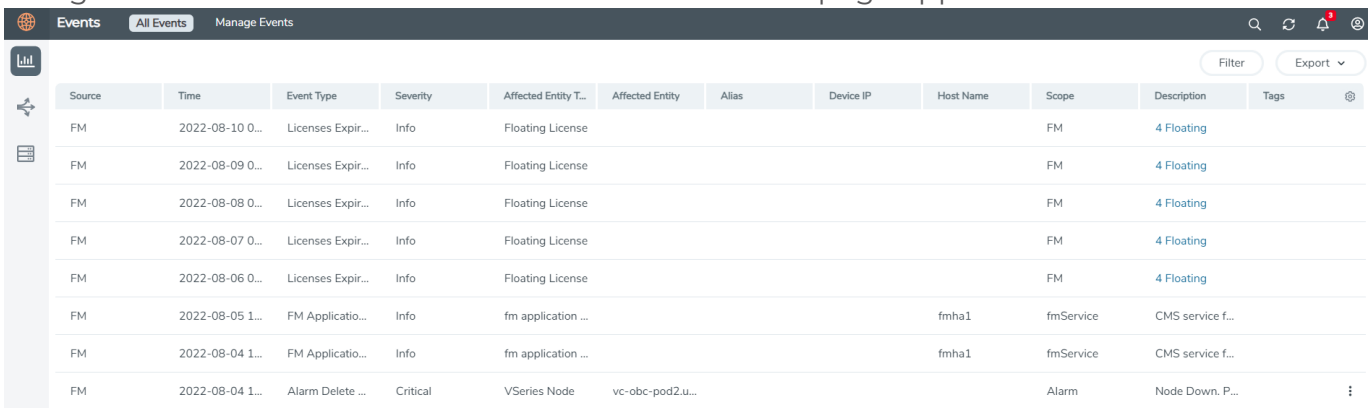
- Cloud provider License Expiry
- UCT-V Inventory Update Completed
- Cloud provider Connection Status Changed

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 is your cloud provider license expiry.

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

Access Event

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 are: ▪ FM - indicates the event that the GigaVUE-FM fabric manager flagged. ▪ VMM - indicates the event that the Virtual Machine Manager flagged. ▪ FM Health - indicates the event that the health status change of GigaVUE-FM flagged.
Duration	The timestamp when the event occurred or the duration of the event. **IMPORTANT:** Timestamps or the duration appear 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 categories: Domain, Node, Card, Port, Stack, Cluster, Chassis, GigaVUE-FM, GigaVUE-VM, and so on. For example, if an event generates a notification for port utilization low threshold, the scope is displayed as Physical Node.
Alarm Type	The type of events that generates the alarms. The types of alarms are 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 a power status change notification is displayed, the message is Info.
Event Status	The status of the event. The status is either Acknowledged or Unacknowledged.
Event Type	The type of event that generated the events. The types of events are 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 a 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 you cannot tag. 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 events,

1. Select **Filter**.

   The Filter quick view is displayed.

2. Select the filtering criteria, and then select **Apply Filter**.

   The result appears on the Events page.

Debuggability and Troubleshooting

Use the following information to help diagnose and resolve GigaVUE V Series Nodes issues.

Sysdumps

A sysdump is a log and system data package generated when a GigaVUE V Series Node experiences a crash (such as kernel, application, or hardware failure). These files are essential for debugging.

You cannot download sysdump files if the associated fabric component is deleted or unreachable.

Sysdumps—Rules and Notes

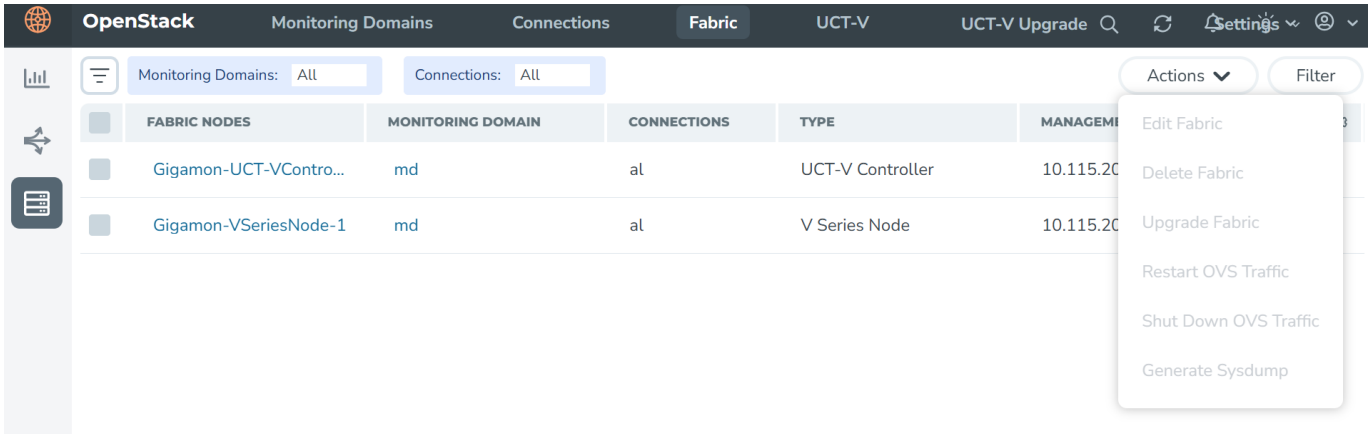
Consider the following points before you generate sysdumps:

- You can generate only one sysdump file at a time for a GigaVUE V Series Node.
- You cannot generate a sysdump file when generation of another sysdump file is in progress.
- The limit of sysdump files available per GigaVUE V Series Node is six. When you generate a seventh sysdump file, the file overwrites the first sysdump file.
- You can download only one sysdump file per GigaVUE V Series Node at a time.
- You can delete sysdump files in bulk for a GigaVUE V Series Node.
- To ensure efficient usage, the system limits the number of simultaneous sysdump generation requests to 10 GigaVUE V Series Nodes.
- GigaVUE V Series Node sysdumps are not stored in Fabric Manager but generated and stored on the GigaVUE V Series Node itself.

Generate a Sysdump File

To generate a sysdumps file:

1. Select the required node, and use one of the following options to generate a sysdump file:
   - Select **Actions > Generate Sysdump**.
   - In the lower pane, go to **Sysdump**, and select **Actions > Generate Sysdump**.
2. View the latest status, click **Refresh**.



Other Actions

- To download a sysdump file, select the file in the lower pane, and then click **Actions > Download**.
- To delete a sysdump file,
  1. Select the file in the lower pane.
  2. Select the desired sysdump file.

3. Select **Actions > Delete**.

- To bulk delete, select all the sysdump files, and then select **Actions > Delete All.**

FAQs - Secure Communication between GigaVUE Fabric Components (OpenStack)

This section addresses frequently asked questions about Secure Communication between GigaVUE Fabric Components and GigaVUE-FM. Refer to Secure Communication between GigaVUE Fabric Components section for more details.

1. **Is there a change in the upgrade process for GigaVUE-FM and GigaVUE V Series Node?**

   No. The upgrade process remains unchanged across all supported upgrade paths. You can upgrade your nodes without any additional steps. The upgrade results in the automatic deployment of the appropriate certificates based on the node versions

GigaVUE-FM	GigaVUE V Series Nodes	Custom Certificates Selected (Y/N)	Actual Node Certificate
6.10	6.10	Y	GigaVUE-FM PKI Signed Certificate
6.10	6.9 or earlier	Y	Custom Certificate
6.10	6.9 or earlier	N	Self-Signed Certificate

2. **What is the new authentication type used between GigaVUE-FM and the GigaVUE Fabric Components? Is backward compatibility supported?**

   Backward compatibility is supported, ensuring that fabric components running on version 6.9 or earlier remain compatible with GigaVUE-FM 6.10. The following authentication types are supported across different versions:

GigaVUE-FM	GigaVUE Fabric Components	Authentication
6.10	6.10	Tokens + mTLS Authentication (Secure Communication)
6.10	6.9 or earlier	User Name and Password

3. **What are the new ports that must be added to the security groups?**

   The following table lists the port numbers that must be opened for the respective fabric components:

Component	Port
GigaVUE-FM	9600
GigaVUE V Series Node	80, 8892
GigaVUE V Series Proxy	8300, 80, 8892
UCT-V Controller	8300, 80
UCT-V	8301, 8892, 9902 For more details, refer to Security Group for OpenStack.

4. **Is the registration process different for deploying the fabric components using Third-Party Orchestration?**

   Yes. Beginning with version 6.10, you must use tokens in the gigamon-cloud.conf file instead of the username and password. To generate the token in GigaVUE-FM, go to **Settings > Authentication > User Management > Token**. For more details, refer to Configure Tokens.

   Example Registration Data for UCT-V:

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteIP: <IP address of the UCT-V Controller 1, <IP address of the UCT-V Controller
2>
        sourceIP: <IP address of UCT-V> (Optional Field)
```

5. **Are there any changes to the UCT-V manual installation and upgrade process?**

   Starting from version 6.10, you must add tokens during manual installation and upgrades.

   - Create a configuration file named gigamon-cloud.conf with the token and place it in the /tmp directory during UCT-V installation
   - After installing UCT-V, you can add the configuration file in the /etc directory.

   Important! Without this token, UCT-V cannot register with GigaVUE-FM.

6. **Can I use my PKI infrastructure to issue certificates for the Fabric Components?**

   Direct integration of your PKI with GigaVUE-FM is not supported. However, you can provide your Intermediate Certificate Authority (CA) to sign the node certificate.

7. **What happens to the existing custom certificates introduced in the 6.3 release?**

   The custom certificate feature is not supported for the fabric components with version 6.10 or higher, even if a custom certificate is selected in the Monitoring Domain. However, this feature remains available for older versions.

   - When upgrading from version 6.9 or earlier with custom certificates upgrades to version 6.10, the system automatically generates and deploys certificates signed by GigaVUE-FM.
   - If deploying version 6.9 or earlier components from a 6.10 GigaVUE-FM, custom certificates are still applied.

8. **How to issue certificates after upgrading the fabric components to 6.10?**

   When the upgrade process begins, GigaVUE-FM transmits the certificate specifications to the new fabric components using the launch script. The fabric components utilize these specifications to generate their own certificates.

9. **Is secure communication supported in FMHA deployment?**

   Yes, it is supported. However, you must follow a few manual steps before upgrading the fabric components to 6.10. For details, refer to Configure Secure Communication between Fabric Components in FMHA.

   NOTE: This step is essential if you are using cloud deployments in FMHA mode and would like to deploy or upgrade the fabric components to version 6.10 or later.

Troubleshooting

This section provides the information needed to troubleshoot GigaVUE-FM integration with OpenStack.

OpenStack Connection Failed

The connFailed state indicates that the OpenStack connection has failed. Check the following troubleshoot tips to restore the connection:

- Verify if GigaVUE-FM is able to reach the OpenStack cloud controller.
- Check if the OpenStack cloud controller is DNS resolvable from GigaVUE-FM.
- Verify if the region name provided while launching the instance is accurate.
- Ensure that all the security group rules required for communication between GigaVUE-FM and OpenStack cloud controller OR GigaVUE-FM and DNS server are accurately setup.
- Check if the Compute Servers that the nova API returns are reachable from GigaVUE-FM. Refer to Handshake Alert: unrecognized_name.

Handshake Alert: unrecognized_name

When setting up the OpenStack connection in GigaVUE-FM, the GigaVUE-FM logs might show a handshake alert: unrecognized_name error. This error is related to a Server Name Indication (SNI) error. Starting with Java 7, the JDK does not ignore the unrecognized name warning. To resolve this issue, perform either of the following:

- Fix the configuration on the server where the error is occurring.
- Ignore the warning on the client side (GigaVUE-FM server) by using the Java system property **--Djsse.enableSNIExtension=false** while launching GigaVUE-FM.

Contact support for information on how to use the Java system property. However, this is not recommended for security reasons.

GigaVUE V Series Node or UCT-V Controller is Unreachable

If GigaVUE V Series node or UCT-V Controller is unreachable, verify the following:

- The correct version of the image is uploaded.
- The network is reachable.

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 6.13 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 6.13 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA400E Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide
GigaVUE Inline Solutions Guide(**NEW**) (previously included in the **GigaVUE Fabric Management Guide**)
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)

GigaVUE Cloud Suite 6.13 Hardware and Software Guides
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud TAP - Container Deployment Guide
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 contact Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The VÜE Community

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

Visit the VÜE Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, 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)