Gigamon®

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

GigaVUE Cloud Suite

Product Version: 6.10

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
6.10	1.0	03/07/2025	The original release of this document with 6.10.00 GA.

Contents

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

This guide describes how to deploy the GigaVUE Cloud Suite in any of the cloud platforms available in the market.

Topics:

Overview of Third Party Orchestration

You can use your own orchestration system to deploy the GigaVUE fabric components instead of using GigaVUE-FM to deploy your fabric components. The third-party orchestration feature allows you to deploy GigaVUE fabric components using your own orchestration system. These fabric components register themselves with GigaVUE-FM using the information provided by the user. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

The GigaVUE Cloud Suite for third party Orchestration consists of the following components:

- GigaVUE-FM fabric manager (GigaVUE-FM)
- UCT-Vs
- UCT-V Controllers
- GigaVUE V Series Proxy
- GigaVUE V Series Nodes

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

In the third-party orchestration deployment option, you are responsible for the following:

- Installing and launching GigaVUE-FM from the supported cloud or enterprise platform.
- Launching the fabric components in your platform.
- Registering the fabric components to GigaVUE-FM.

The images of the components are available in the Gigamon Customer Portal and the images for public clouds are available in the respective market place.

NOTE: Contact Gigamon Technical Support team if the existing Gigamon images for a specific cloud platform is not compatible.

NOTE: You are responsible for deleting the fabric components from the platform when visibility for the platform is no longer required.

For information about installing GigaVUE-FM in your enterprise data center, refer to the *GigaVUE-FM Installation and Upgrade Guide*.

Components for Third Party Orchestration

The following table provides a brief description of the components that can be deployed using the third-party orchestration:

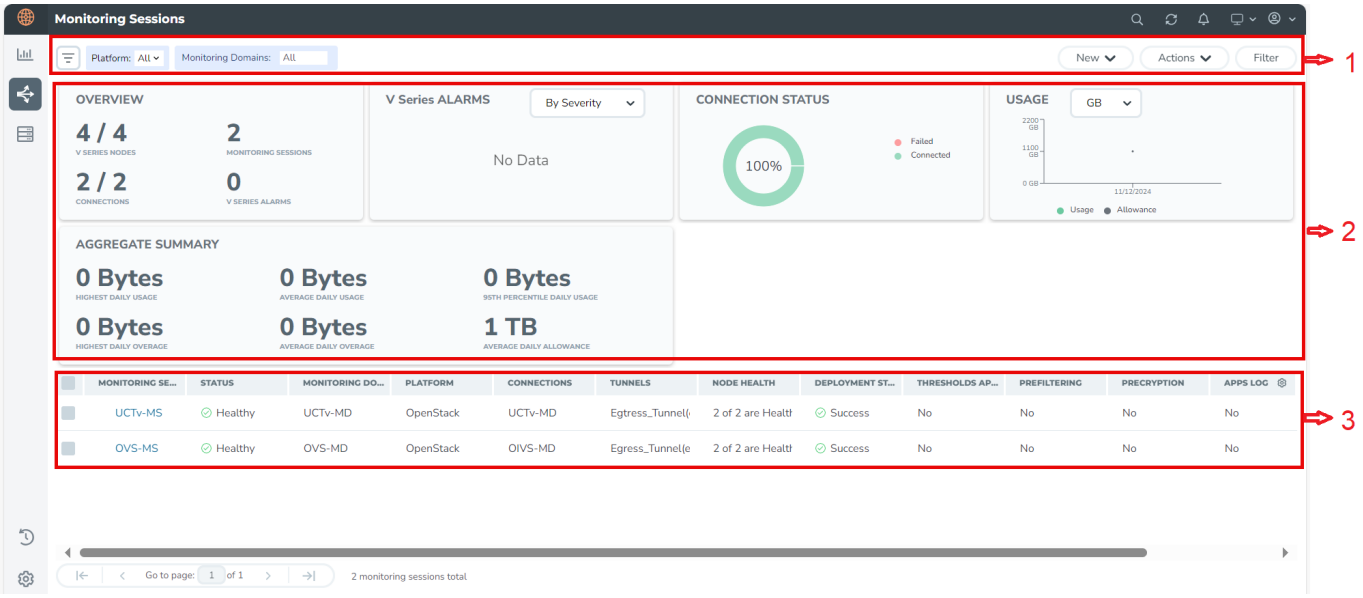
Component	Description
GigaVUE-FM fabric manager (GigaVUE-FM)	GigaVUE-FM is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud. You are responsible for launching GigaVUE-FM from your end on the supported cloud or enterprise platforms.
UCT-V (earlier known as G-vTAP Agent)	UCT-V is an agent that is installed in your Virtual Machine (VM). This agent mirrors the selected traffic from the VMs to the GigaVUE® V Series node. The UCT-V is offered as a Debian (.deb), Redhat Package Manager (.rpm) or windows package. Refer to Install UCT-Vs.

Component	Description
Next generation UCT-V (earlier known as Next Generation G-vTAP Agent)	**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 agent to V Series node and in-turn reduces the V Series load. Next generation UCT-V gets activated only on Linux systems with a Kernel version above 5.4. Prefiltering allows you to filter the traffic at UCT-Vs before sending it to the V Series nodes. For prefiltering the traffic, GigaVUE-FM allows you to create a prefiltering policy template and the template can be applied to a monitoring session.
UCT-V Controller (earlier known as G-vTAP Controller)	UCT-V 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.
GigaVUE® V Series Proxy (optional)	GigaVUE® V Series Proxy manages multiple V Series nodes and orchestrates the flow of traffic from GigaVUE V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series nodes.
GigaVUE® V Series Node	GigaVUE® V Series Node is a visibility node that aggregates mirrored traffic from multiple UCT-Vs. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to GigaVUE Cloud Suite Cloud using GRE or VXLAN tunnels, provided the cloud platform supports

Cloud Overview Page (Third Party Orchestration)

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

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



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

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

Top Menu

The Top menu consists of the following options:

Options	Description
New	You can create a new Monitoring Session and new Monitoring Domain.
Actions	You can do the following actions using the **Action** button: **Edit** - Opens the edit page for the selected Monitoring Session. **Delete** - Deletes the selected Monitoring Session. **Clone** - Duplicates the selected Monitoring Session. **Deploy** - Deploys the selected Monitoring Session. **Undeploy** - Undeploys the selected Monitoring Session. **Apply Threshold** - Applies the threshold template created for monitoring cloud traffic health. Refer to *Monitor Cloud* section for details.
Filter	You can filter the Monitoring Session details based on a criterion or combination of criteria. For more information, refer to Filters.

Filters

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

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

Filter on the left corner

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

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

Filter on the right corner Filter

You can filter Monitoring Session and Monitoring Domain details based on a criterion or by providing multiple criteria as follows:

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

Viewing Charts

You can view the following charts on the overview page:

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

Overview

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

V Series Alarms

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

Connection Status

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

Usage

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

Aggregate Summary

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

Viewing Monitoring Session Details

You can view the following details in the overview table:

Details	Description
Monitoring Sessions	Name of the Monitoring Session. When you click the name of the session, you will be redirected to the platform specific Monitoring Session page.
Status	Health status of the Monitoring Session.
Monitoring Domain	Name of the Monitoring Domain to which the Monitoring Session is associated.
Platform	Cloud platform in which the session is created.
Connections	Connection details of the Monitoring Session.
Tunnels	Tunnel details related to the Monitoring Session.
Node Health	Health status of the GigaVUE V Series Node.
Deployment Status	Status of the deployment.

Details	Description
Threshold Applied	Specifies whether the threshold is applied or not.
Prefiltering	Specifies whether Prefiltering is configured or not.
Precryption	Specifies whether Precryption is configured or not.
APPS logging	Specifies whether APPS logging is configured or not.
Traffic Mirroring	Specifies whether Traffic Mirroring is configured or not.

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

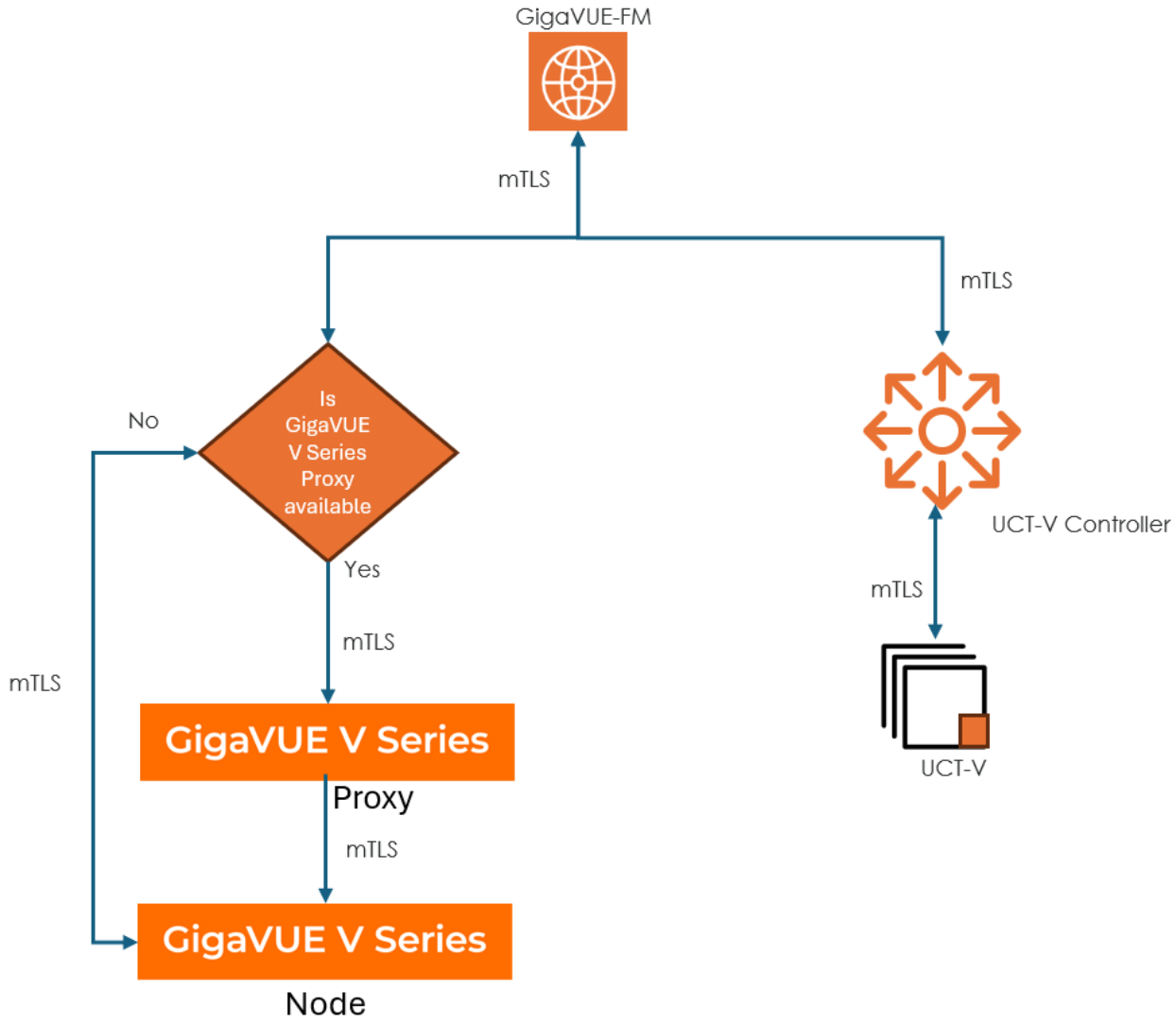
Introduction to Supported Features on GigaVUE Cloud Suite for Third Party Orchestration

GigaVUE Cloud Suite for Third Party Orchestration supports the following features:

- Precryption™
- Secure Tunnels
- Prefiltering
- Analytics for Virtual Resources
- Cloud Health Monitoring
- Customer Orchestrated Source - Use Case

Secure Communication between GigaVUE Fabric Components

The Secure Communication feature in GigaVUE-FM enhances security by enabling mutual Transport Layer Security (mTLS)-based authentication across GigaVUE Fabric Components. With this feature, each fabric component is assigned a properly signed certificate from a Certificate Authority (CA), ensuring authenticated, encrypted communication without relying on static credentials.



In the above diagram, 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 Proxy is available, then GigaVUE-FM first connects to the GigaVUE V Series Proxy, which then establishes an mTLS connection with the GigaVUE V Series Node. Separately, GigaVUE-FM also initiates an mTLS connection to the UCT-V Controller, which then establishes an mTLS connection with UCT-V. This structured flow ensures secure communication using mTLS-based authentication across all the fabric components.

GigaVUE-FM manages certificates by acting as the Public Key Infrastructure (PKI), ensuring a centralized and secure approach to certificate management.

GigaVUE-FM acts as the PKI

GigaVUE-FM acts as a private PKI, automatically issuing and managing certificates for all fabric components. GigaVUE-FM uses Step-CA to handle certificate issuance and renewal using the Automatic Certificate Management Environment (ACME) protocol in this method. This eliminates the need for external dependencies while ensuring secure, automated certificate management.

Bring Your Own CA

Organizations with existing PKI infrastructure can import externally issued certificates into GigaVUE-FM. This method supports enterprise CA solutions while allowing seamless integration with Gigamon's secure communication framework.

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

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

- For public cloud platforms, if the public IP is revoked, you can issue a new certificate from GigaVUE-FM to remove the public IP from the certificate.

  NOTE: This is an optional configuration.

- When GigaVUE-FM and GigaVUE Fabric Components are deployed on different hosts, ensure that the hosts are time-synchronized with NTP configured and running.

- When applying the certificates, the GigaVUE Fabric Components may move to a Down state and automatically recover.

Precryption™

License: Requires **SecureVUE Plus** license.

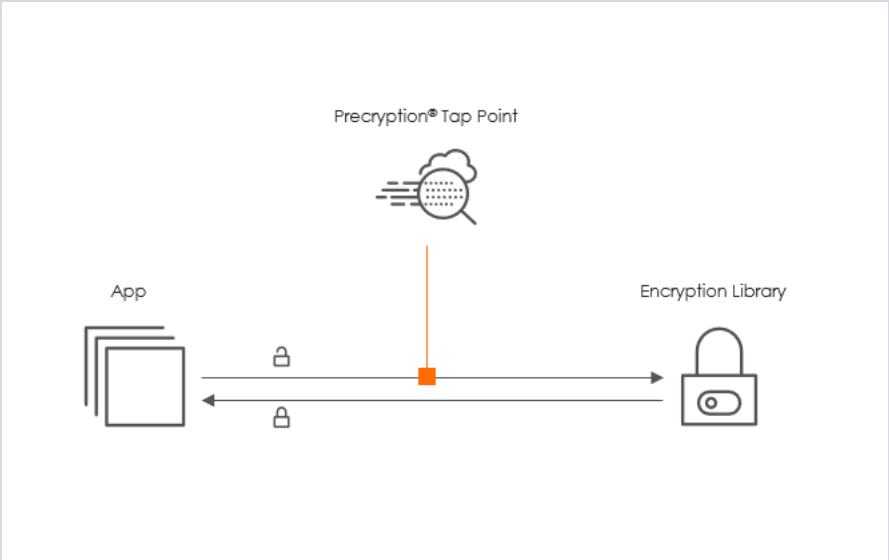
Gigamon Precryption™ technology[1] redefines security for virtual, cloud, and containerized applications, delivering plain text visibility of encrypted communications to the full security stack without the traditional cost and complexity of decryption.s

This section explains:

How Gigamon Precryption Technology Works

Precryption technology leverages native Linux functionality to tap, or copy, communications between the application and the encryption library, such as OpenSSL.

[1] **Disclaimer**: The Precryption feature allows users to acquire traffic after it has been decrypted. This traffic can be acquired from both virtual machine (VM) and container-based solutions, and is then sent to the V Series product for further processing. The Precryption feature provides an option to use encrypted tunnels for communication between the acquisition (via UCT-C or UCT-V) of unencrypted traffic and the traffic processing (at the V Series) which will better safeguard the traffic while in transit. However, if a user does not use the option for encrypted tunnels for communication, decrypted traffic will remain unencrypted while in transit between the point of acquisition and processing. Please note that this information is subject to change, and we encourage you to stay updated on any modifications or improvements made to this feature. By using this feature, you acknowledge and accept the current limitations and potential risks associated with the transmission of decrypted traffic.



In this way, Precryption captures network traffic in plain text, either before it has been encrypted or after it has been decrypted. Precryption functionality doesn't interfere with the message's actual encryption or transmission across the network. There's no proxy, retransmissions, or break-and-inspect. Instead, this plaintext copy is forwarded to the Gigamon Deep Observability Pipeline for further optimization, transformation, replication, and tool delivery.

Precryption technology is built on GigaVUE® Universal Cloud Tap (UCT) and works across hybrid and multi-cloud environments, including on-prem and virtual platforms. As a bonus, UCT with Precryption technology runs independently of the application and doesn't have to be baked into the application development life cycle.

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. It provides East-West visibility into virtual, cloud, and container platforms. It delivers unobscured visibility into all encryption types, including TLS 1.3, without managing and maintaining decryption keys. IT organizations can now manage compliance, keep private communications private, architect the necessary foundation for Zero Trust, and boost 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:

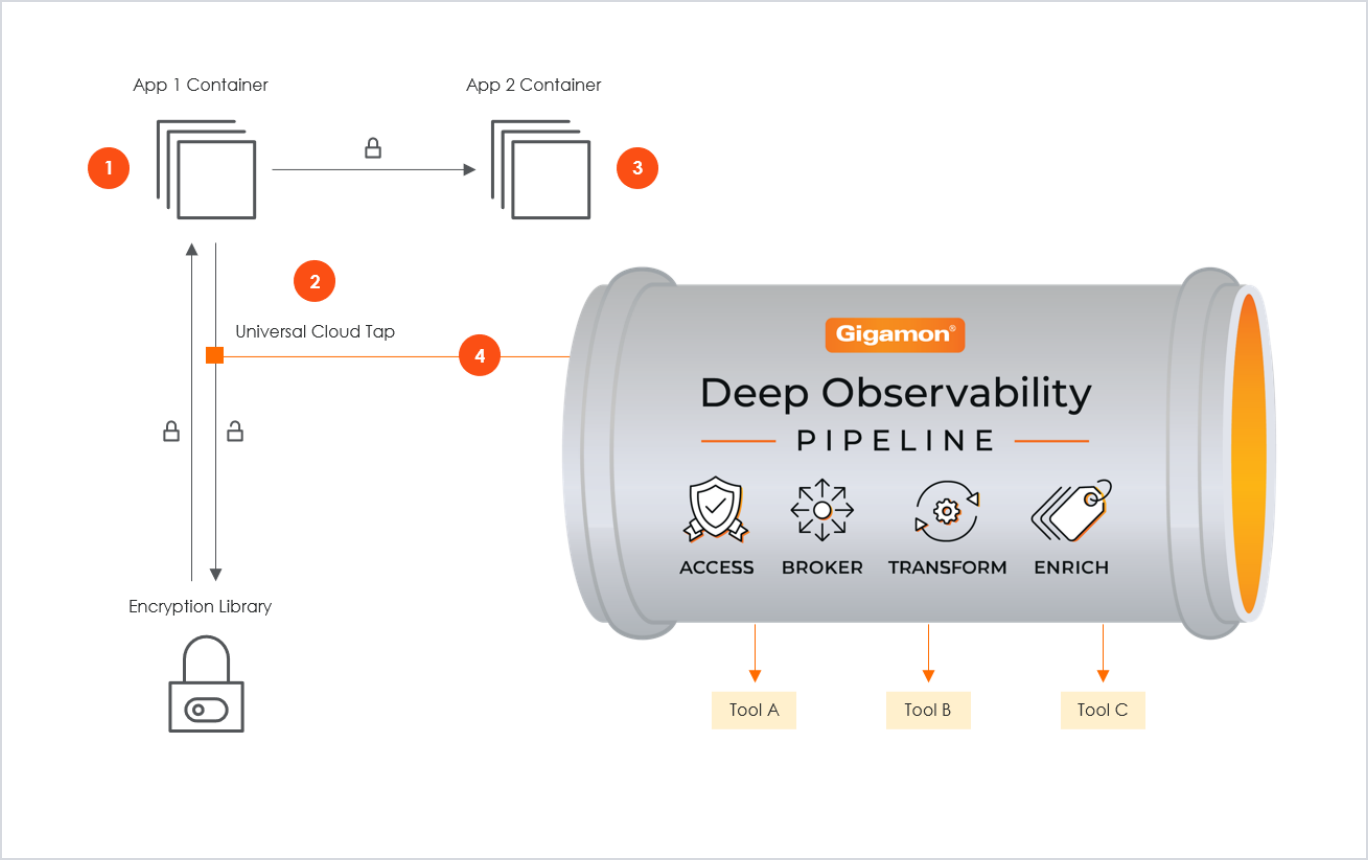
- Eliminate blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.
- Monitor application communications with an independent approach that enhances development team velocity.
- Extend security tools' visibility to all communications, regardless of encryption type.
- Achieve maximum traffic tapping efficiency across virtual environments.
- Leverage a 5–7x performance boost for security tools by consuming unencrypted data.
- Support a Zero Trust architecture founded on deep observability.
- Maintain 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:

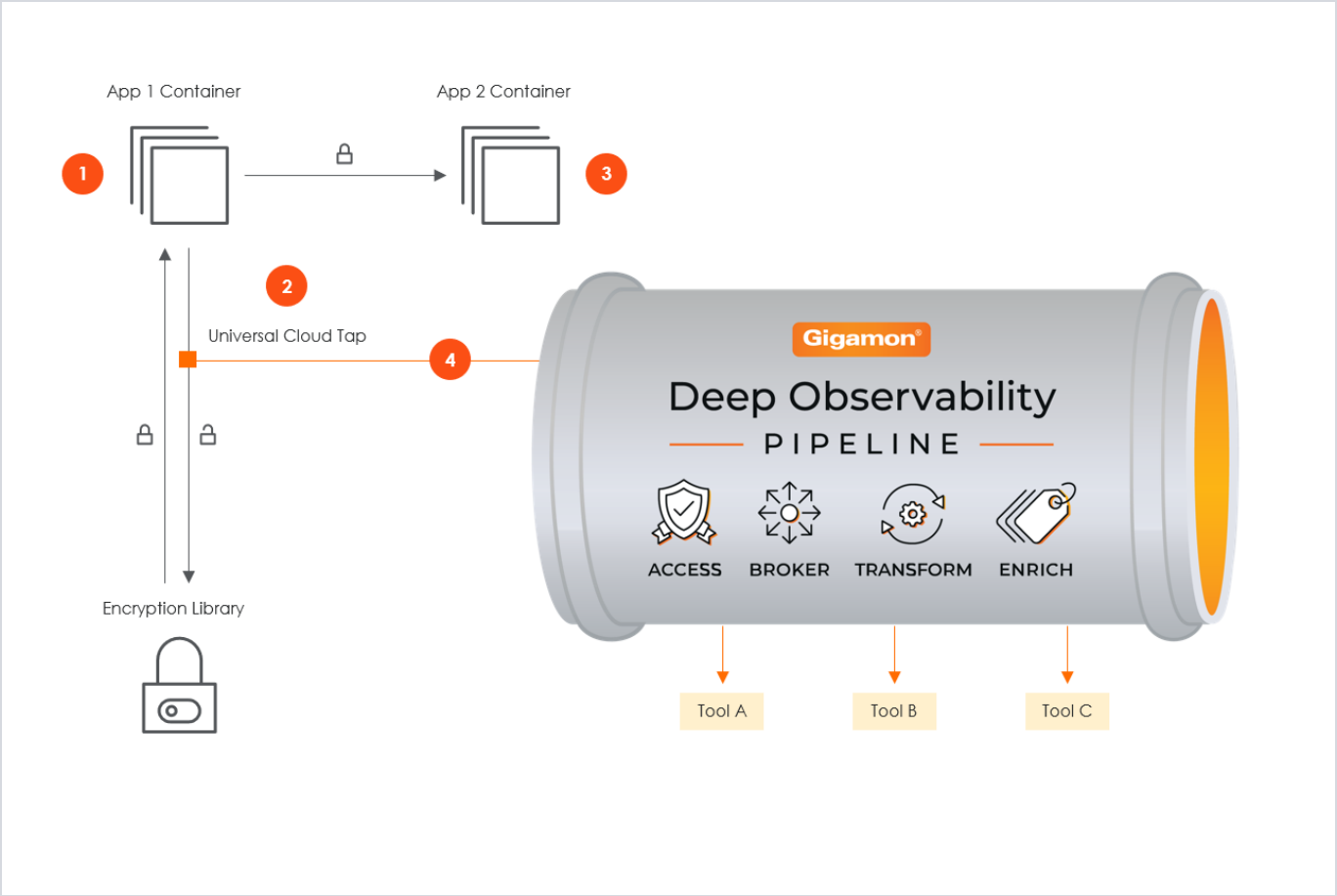
- Precryption Technology on Single Node
- Precryption Technology on Multi-Node

Precryption Technology on Single Node



1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption technology, gets a copy of this message before it's 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. Gigamon optimizes, transforms, and delivers data to tools without further decryption.

Precryption Technology on Multi-Node



1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption, gets a copy of this message before it's 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 V Series in the deep observability pipeline. There, they are further enriched, transformed, and delivered to tools without further decryption.

Supported Platforms

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

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)

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

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

Prerequisites

Deployment Prerequisites

- 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 precrypted packets from the worker pods whenever libssl calls are made from the worker pods.
- For GigaVUE-FM, you must add port 5671 in the security group to capture the statistics.
- Port 9900 should be enabled in security group settings on the UCT-V controller to receive the statistics information from UCT-V.
- For UCT-C, you must add port 42042 and port 5671 to the security group.

License Prerequisite

- Precryption™ requires a SecureVUE Plus license.

Supported Kernel Version

Precryption is supported for Kernel Version 5.4 and above for 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)

Kernel-Version	Operating System
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	ubuntu19.10
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 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.

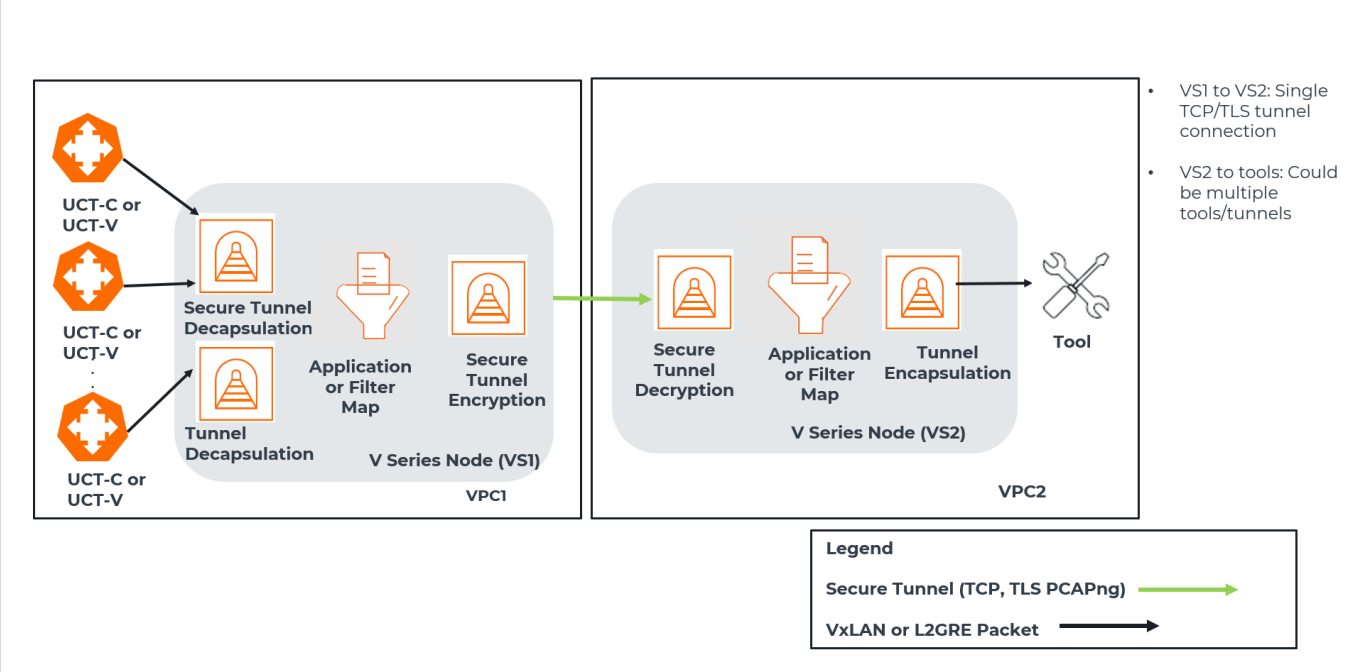
Secure Tunnels

Secure Tunnel securely transfers the cloud-captured packets on UCT-V and UCT-C to a GigaVUE V Series Node or Tool (only in the case of UCT-C). The data from UCT-V and UCT-C are encapsulated in PCAPng format, and the encrypted data is sent over a TLS connection to a GigaVUE V Series Node.

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

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

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



Supported Platforms

Secure Tunnels is supported on:

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

For information about how to configure secure tunnels, refer to the section Configure Secure Tunnel for Third Party Orchestration

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 Configure Precryption in UCT-V

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics[1] you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects. Refer to Analytics section in *GigaVUE Fabric Management Guide* for more detailed information on Analytics.

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

Rules and Notes:

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations. Refer to the Clone Dashboard section in GigaVUE-FM Installation and Upgrade Guidefor more details.
- Use the Time Filter option to select the required time interval for which you need to view the visualization.

Virtual Inventory Statistics and Cloud Applications Dashboard

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

To access the dashboards:

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

The following table lists the various virtual dashboards:

Dashboard	Displays	*Visualizations*	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: • Number of Monitoring Sessions • Number of V Series Nodes • Number of Connections • Number of GCB Nodes You can filter the visualizations based on the following control filters: • Platform • Health Status	*V Series Node Status by Platform*	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		Monitoring Session Status by Platform	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		Connection Status by Platform	Number of healthy and unhealthy connections for each of the supported cloud platforms
		GCB Node Status by Platform	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the	*V Series Node Maximum CPU Usage Trend*	Line chart that displays maximum

Dashboard	Displays	*Visualizations*	Displays
	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		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. **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

Dashboard	Displays	*Visualizations*	Displays
			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: • **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.	*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
	• **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. By default, the following statistics are displayed: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets	*App Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	*Visualizations*	Displays
	• 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.

Cloud Health Monitoring

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

For more information on how to configure cloud health monitoring, refer to the topic Monitor Cloud Health.

Customer Orchestrated Source - Use Case

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

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

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

Get Started with Third Party Orchestration

This chapter describes how to plan and start the third party orchestration deployment.

Refer to the following sections for details:

- License information
- Network Firewall Requirement
- GigaVUE-FM Version Compatibility
- Configure Role-Based Access for Third Party Orchestration
- Modes of Deployments

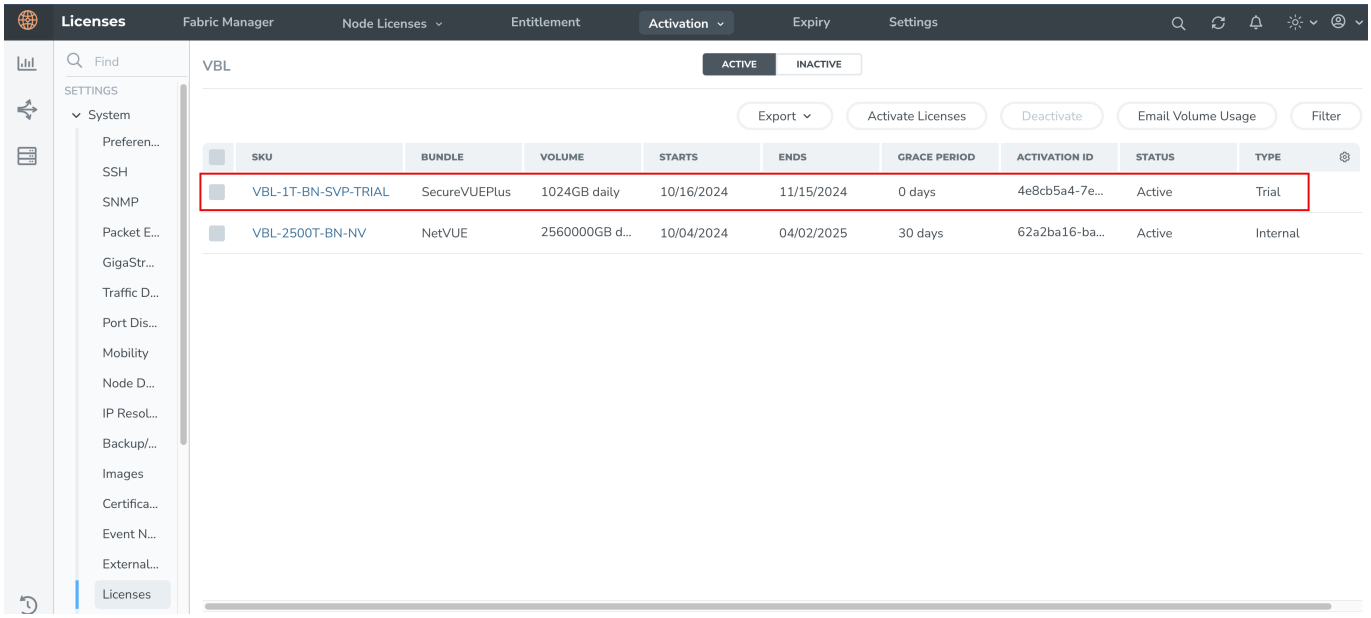
License information

GigaVUE Cloud Suite for third-party orchestration supports Volume-Based Licensing model. Refer to the following topics for more detailed information on Volume-Based Licensing and how to activate your license:

- Default Trial Licenses
- Volume-Based License
- Activate Volume-Based Licenses
- Manage Volume-Based Licenses

Default Trial Licenses

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



This license includes the following applications:

- ERSPAN
- GENEVE
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing

- Enhanced Load Balancing
- Flow map
- Header Stripping
- Header Addition
- De-duplication
- NetFlow
- Application Packet Filtering
- Application Filtering Intelligence
- Application Metadata Intelligence
- Application Metadata Exporter
- Inline SSL
- SSL Decrypt
- Precryption

NOTE: If you do not have any other Volume-Based Licenses installed, then after 30 days, on expiry of the trial license, any deployed Monitoring Sessions will be undeployed from the existing GigaVUE V Series Nodes.

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

Volume-Based License

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

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

Volume-based licenses are available as monthly subscription licenses with a service period of one month. Service period is the period of time for which the total usage or overage is tracked.

For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales.

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUEPlus

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

Bundle Replacement Policy

Refer to the following notes:

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

Add-on Packages

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

Rules for add-on packages:

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

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

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

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

How GigaVUE-FM Tracks Volume-Based License Usage

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

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only those applications that are licensed at that point (applicable only for ACTIVE licenses).
- When a license expires, you will be notified with an audit log. Refer to the *About Audit Logs* section in the respective GigaVUE Cloud Suite Deployment Guide.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license will not be undeployed.
    - For releases prior to 6.4:
        - The Monitoring Sessions using the corresponding license will be undeployed (but not deleted from the database).
        - When a license is later renewed or newly imported, any undeployed monitoring sessions are redeployed.

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

Activate Volume-Based Licenses

To activate Volume-Based Licenses:

1. On the left navigation pane, click  .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL** from the **Activation** drop-down.
3. Click **Activate Licenses**. The **Activate License** page appears.
4. Select **IP Address** or **Hostname** to include this information. If you exclude the IP Address or Hostname, you will have to identify the chassis or GigaSMART card by its ID when activating.
5. Download the fabric inventory file that contains information about GigaVUE-FM. Click **Next**. Refer to the What is a Fabric Inventory File section in *GigaVUE Licensing Guide* for more details.

6. Click **Gigamon License Portal** to navigate to the Licensing Portal. Upload the Fabric Inventory file in the portal. Once the fabric inventory file is uploaded, select the required license and click **Activate**. A license key is provided. Record the license key or keys.
7. Return to GigaVUE-FM and upload the file by clicking **Choose File** button.

Manage Volume-Based Licenses

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

Manage active Volume-Based License

To manage active Volume-Based License (VBL):

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

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

Field	Description
SKU	Unique identifier associated with the license.
Bundle	Bundle to which the license belongs to.
Volume	Total daily allowance volume.
Starts	License start date.
Ends	License end date.
Type	Type of license (Commercial, Trial, Lab, and other license types).
Activation ID	Activation ID.
Entitlement ID	Entitlement ID. Entitlement ID is the permission with which the acquired license can be activated online.
Reference ID	Reference ID.
Status	License status.

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

Manage Inactive Volume-Based License

To manage inactive Volume-Based License (VBL):

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

   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, click on the column setting configuration option and enable these fields.

   Use the following buttons to manage your VBL.

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

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

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

Network Firewall Requirement

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

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

GigaVUE-FM

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-C Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-C Controller using REST API.
Inbound	TCP	5671	GigaVUE V Series	Allows GigaVUE-FM to receive

			Node IP	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-C 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	GigaVUE-FM 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 (default)	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				
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 the GigaVUE-FM
Inbound	TCP	8300	UCT-V Subnet	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				
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				
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 the 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	Allows GigaVUE V Series Node

			Proxy	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.

GigaVUE V Series Proxy (optional)

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
Universal Cloud Tap - Container deployed inside Kubernetes worker node				
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	42042	Any IP address	Allows UCT-C to send statistical information to UCT-C Controller.
Outbound	UDP	VXLAN (default 4789)	Any IP address	Allows UCT-C to tunnel traffic to the GigaVUE V Series Node or other destination.
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 to be opened for Backward Compatibility:

These ports must be opened 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				
Direction	**Protocol**	**Port**	**Source CIDR**	**Purpose**
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests from 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.
UCT-V				
Direction	**Protocol**	**Port**	**Source CIDR**	**Purpose**
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V Controller IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat
GigaVUE V Series Node				
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)				
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.

GigaVUE-FM Version Compatibility

GigaVUE-FM version 6.10.00 supports the latest version (6.10.00) of GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, and UCT-V, as well as (n-2) versions. For better compatibility, it is always recommended to use the latest version of fabric components with GigaVUE-FM.

Configure Tokens for Third Party Orchestration

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.

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. The default value is 30 days, and the maximum value is 105 days.
  - When a related user group that exists as part of the token is deleted, the corresponding token is deleted.
  - When there is a password change for the user(local), the corresponding token is deleted.
  - When there is a change in the authentication type, all the tokens are deleted.
- During the back up and restoration of the GigaVUE-FM, previously generated tokens will not be 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 will see the error code 401 on GigaVUE-FM REST API access.

This section explains about the following:

- Create Token
- Revoke Tokens
- Export Token
- Using Token to access GigaVUE-FM REST API

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, click **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. Click **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 the GigaVUE-FM from the **User Group** drop-down list.
7. Click **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.

Select the token that you want to copy, click the **Actions** button drop-down list, and select **Copy Token.** The token is copied. You can paste in the required areas.

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

Revoke Tokens

You can only revoke tokens created by other users if you have write access in GigaVUE-FM Security Management. To revoke tokens, follow these steps:

1. Go to , select **Authentication** > **GigaVUE-FM User Management**.
2. In the **User Management** page that appears, click **Tokens**.
3. Select **Token Management** from the drop-down list. You can view the token created by other users.
4. Select the token that you want to revoke, click the **Action** button, and then click **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, click 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, click the **Export All** drop-down list box, and then select the **CSV** or **XLSX** format as per requirement.

Using Token to access GigaVUE-FM REST API

The following example shows how to access GigaVUE-FM REST APIs using tokens:

Example

```
import getpass
import requests #
https://requests.readthedocs.io/en/latest/user/install/#install
FM_SERVER = '<FM_IP>'
GET_URL = f'https://{FM_SERVER}/api/v1.3/fabricResource'
try:
      fm_token = getpass.getpass(prompt=f'Enter FM API token for FM server {FM_
SERVER}: ')
except (KeyboardInterrupt, EOFError):
      print(''); exit(2)
with requests.Session() as fm_session:
      fm_session.headers.update({'Authorization': f'Bearer {fm_token}'})
      fm_session.verify = True
      #
      response = fm_session.get(GET_URL, timeout=(5, 20))
      print(f'status_code = {response.status_code}')
      print(f'response = {str(response.text)}')
```

Modes of Deployments

There are two ways in which GigaVUE fabric components can be deployed using the third party orchestration. They are:

- Generic Mode
- Integrated Mode

Generic Mode

In generic mode, when deploying the fabric components, you can provide the monitoring domain and connection name directly in your orchestrator. A Monitoring Domain will be created under the **Third Party Orchestration** monitoring domain page in GigaVUE-FM and your GigaVUE fabric components will be deployed in that monitoring domain. Or you can also create a monitoring domain under **Third Party Orchestration** and provide the monitoring domain name and the connection name in the user data that will be used in your orchestrator.

In generic mode, the platform credentials are not shared with GigaVUE-FM.

Integrated Mode

In integrated mode, you create a monitoring domain in your respective GigaVUE Cloud Suite in GigaVUE-FM and then use your own orchestration system to just deploy nodes. The fabric components deployed using your own orchestration system will be displayed under the monitoring domain created in your respective GigaVUE Cloud Suite. In this case, ensure that the monitoring domain and the connection name given in the GigaVUE-FM matches the groupName and subGroupName in the user data provided in your orchestration system.

In generic mode, the platform credentials are shared with GigaVUE-FM. Only the GigaVUE fabric components deployment happens in the platform.

Deployment Options for GigaVUE Cloud Suite for Third Party Orchestration

This section provides a detailed information on the multiple ways in which GigaVUE Cloud Suite for Third Party Orchestration can be configured to provide visibility for physical and virtual traffic. There are five different ways in which GigaVUE Cloud Suite for Third Party Orchestration can be configured based on the traffic acquisition method and the method in which you want to deploy fabric components. For more detailed information and the work flow refer the following topics:

- Deploy GigaVUE Fabric Components using Generic Mode
  - Without Creating Monitoring Domain
  - By Creating Monitoring Domain
- Deploy GigaVUE Fabric Components using Integrated Mode

Deploy GigaVUE Fabric Components using Generic Mode

If you wish to deploy GigaVUE fabric components using generic mode, it can be done in four ways:

Without Creating Monitoring Domain

In generic mode, when deploying the fabric components, you can provide the monitoring domain and connection name directly in your orchestrator. A Monitoring Domain will be created under the **Third Party Orchestration** monitoring domain page in GigaVUE-FM and your GigaVUE fabric components will be deployed in that monitoring domain.

Traffic Acquisition Method as UCT-V

Follow instruction in the below table, if you wish to use UCT-V as your traffic acquisition method. When using UCT-V the traffic from the Virtual Machines are acquired using the UCT-V and it is sent to the GigaVUE V Series Nodes.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Install UCT-V	Install UCT-V
3	Create User and Password	Configure Role-Based Access for Third Party Orchestration
4	Configure GigaVUE Fabric Components	Deploy Fabric Components using Generic Mode
5	Create Monitoring session	Configure Monitoring Session
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 GigaVUE V Series Nodes without deploying UCT-V or UCT-V controllers.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Create User and Password	Configure Role-Based Access for Third Party Orchestration
3	Configure GigaVUE Fabric Components	Deploy Fabric Components using Generic Mode
4	Create Monitoring session	Configure Monitoring Session

Step No	Task	Refer the following topics
5	Create Ingress and Egress Tunnel Endpoints	Create Ingress and Egress Tunnels
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

By Creating Monitoring Domain

In generic mode, you can also create a monitoring domain under **Third Party Orchestration** and provide the monitoring domain name and the connection name in the user data that will be used in your orchestrator.

Traffic Acquisition Method as UCT-V

Follow instruction in the below table, if you wish to use UCT-V as your traffic acquisition method. When using UCT-V the traffic from the Virtual Machines are acquired using the UCT-V and it is sent to the GigaVUE V Series Nodes.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Install UCT-V	Install UCT-V
3	Create User and Password	Configure Role-Based Access for Third Party Orchestration
4	Create a Monitoring Domain	Create Monitoring Domain
5	Configure GigaVUE Fabric Components	Deploy Fabric Components using Generic Mode
6	Create Monitoring session	Configure Monitoring Session
7	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
8	Deploy Monitoring Session	Deploy Monitoring Session
9	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-V or UCT-V controllers.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Create User and Password	Configure Role-Based Access for Third Party Orchestration
3	Create a Monitoring Domain	Create Monitoring Domain
4	Configure GigaVUE Fabric Components	Deploy Fabric Components using Generic Mode
5	Create Monitoring session	Configure Monitoring Session
6	Create Ingress and Egress Tunnel Endpoints	Create Ingress and Egress Tunnels
7	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
8	Deploy Monitoring Session	Deploy Monitoring Session
9	View Monitoring Session Statistics	View Monitoring Session Statistics

Deploy GigaVUE Fabric Components using Integrated Mode

GigaVUE-FM allows you to use your own cloud platform as an orchestrator to deploy GigaVUE fabric components and then use GigaVUE-FM to configure the advanced features supported by these nodes. In integrated mode, you create a monitoring domain in your respective GigaVUE Cloud Suite in GigaVUE-FM and then use your own orchestration system to just deploy nodes. The GigaVUE V Series Nodes deployed using your own orchestration system will be displayed under the monitoring domain created in your respective GigaVUE Cloud Suite. In this case, ensure that the monitoring domain and the connection name given in the GigaVUE-FM matches the groupName and subGroupName in the user data provided in your orchestration system. Refer the following table for the step-by-step instructions.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Create User and Password in GigaVUE-FM.	Configure Role-Based Access for Third Party Orchestration
3	Install UCT-V	Install UCT-V
4	Create a Monitoring Domain **NOTE:** Ensure that the Use FM to Launch Fabric toggle button is disabled.	Refer to the *Create Monitoring Domain* section in the respective cloud guide.
5	Configure GigaVUE Fabric Components	Deploy Fabric Components using Integrated Mode

Step No	Task	Refer the following topics
	NOTE: Select UCT-V as the Traffic Acquisition Method. When using integrated mode you can only use UCT-V as the traffic acquisition method.	
6	Create Monitoring session	Configure Monitoring Session
7	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
8	Deploy Monitoring Session	Deploy Monitoring Session
9	View Monitoring Session Statistics	View Monitoring Session Statistics

Deploy GigaVUE Cloud Suite for Third Party Orchestration

You can use your own orchestration system to deploy the GigaVUE fabric components instead of using GigaVUE-FM to deploy your fabric components.

The third-party orchestration feature allows you to deploy GigaVUE fabric components using your own orchestration system. These fabric components register themselves with GigaVUE-FM using the information provided by the user. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

You can either manually deploy the fabric components using a configuration file or you can use your orchestration portal to launch the instances and deploy the fabric components using user data. Using the user data provided by you, the fabric components register itself with the GigaVUE-FM. Based on the group name and the sub group name details provided in the user data, GigaVUE-FM groups these fabric components under their respective monitoring domain and connection name. Health status of the registered nodes is determined by the heartbeat messages sent from the respective nodes.

This chapter describes how to connect, launch, and deploy the fabric components of GigaVUE Cloud Suite using third party orchestration. Refer to the following sections for more detailed information:

- Install GigaVUE-FM
- Install UCT-V
- Uninstall UCT-V
- Upgrade or Reinstall UCT-V
- Install Custom Certificate

- Adding Certificate Authority
- Create Monitoring Domain
- Deploy Fabric Components using Generic Mode
- Deploy Fabric Components using Integrated Mode

Install GigaVUE-FM

The GigaVUE-FM software package is available in multiple formats such as OVA, QCOW2, ISO. Use the appropriate media format to deploy GigaVUE-FM.

After you deploy GigaVUE-FM you must perform an initial configuration before you start using GigaVUE-FM. Refer to the *GigaVUE-FM Installation and Upgrade Guide* for details.

To install GigaVUE-FM in your cloud environment refer to *GigaVUE-FM Installation and Upgrade Guide* for details.

Install UCT-V

UCT-V is the primary Gigamon monitoring module that is installed in your Virtual Machines (VMs). UCT-V mirrors the selected traffic from a source interface to a destination mirror interface. The mirrored traffic is encapsulated using GRE or VXLAN tunneling and then sent to the GigaVUE Cloud Suite® V Series Node.

NOTE: The UCT-V installation is applicable only when the UCT-V is your traffic acquisition method.

A UCT-V can consists of multiple source interface and a single destination interface. The network packets collected from the source interface are sent 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.

A source interface can be configured with one or more Network Interfaces. While configuring a source interface, you can specify the direction of the traffic to be monitored in the instance. The direction of the traffic can be egress or ingress 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.

Refer to the following sections for more information:

- Supported Operating Systems for UCT-V
- Modes of Installing UCT-V

- Linux UCT-V Installation
- Windows UCT-V Installation

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

The table below lists the validated and the 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 6.10 supports UCT-V version 6.10 as well as (n-2) versions. It is always recommended to use the latest version of UCT-V with GigaVUE-FM, for better compatibility.

Modes of Installing UCT-V

You can install UCT-V in your virtual machine in two ways. Refer to the following points for more detailed information and step-by-step instructions on how to configure UCT-V:

1. **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V register themselves with GigaVUE-FM using the information provided by the user. UCT-V can be registered with GigaVUE-FM using Third Party Orchestration in two ways:
   - 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

   Refer to Modes of Deployment section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration for more detailed information on generic and integrated mode.

2. **GigaVUE-FM Orchestration**: Refer to Install UCT-V for more details.

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

Linux UCT-V Installation

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

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

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

Single Network Interface Configuration

A single network interface card (NIC) acts as the source and the destination interface. UCT-V with a single network interface configuration lets you monitor the ingress or egress traffic from the network interface. The monitored traffic is sent out using the same network interface.

For example, assume that there is only one interface, eth0, in the monitoring instance. In the UCT-V configuration, you can configure eth0 as the source and the destination interface and specify both egress and ingress traffic to be selected for monitoring purposes. The egress and ingress traffic from eth0 are mirrored and sent out using the same interface.

Using a single network interface card as the source and the destination interface can sometimes cause increased latency when sending the traffic out from the instance.

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

UCT-V lets you configure two network interface cards (NICs). One network interface card can be configured as the source interface and another as the destination interface.

For example, assume that eth0 and eth1 are in the monitoring instance. In the UCT-V configuration, eth0 can be configured as the source interface, and egress traffic can be selected for monitoring purposes. The eth1 interface can be configured as the destination interface. So, the mirrored traffic from eth0 is sent to eth1. From eth1, the traffic is sent to the GigaVUE V Series Node.

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, which 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.

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. Refer to Network Firewall Requirement for GigaVUE Cloud Suite for more details on the firewall requirements or security groups required for your environment.

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 will initialize at boot time.

Prerequisites

- UCT-V requires specific packages to function properly. By default, most modern Linux operating systems come pre-installed with all the necessary packages for the UCT-V to function without additional configuration. Ensure you have the following packages installed before installing deb or rpm packages on your Linux VMs. If you have already installed UCT-V, use the uctv-wizard pkg-install command to install the packages.
  - Python v3.x
  - Python v3.x-pip
  - Python modules
    - netifaces
    - urllib3
    - requests
  - iproute-tc for RHEL and CentOS VMs

    NOTE: When using Amazon Linux version 2, ensure iproute-tc package is installed first.

- 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. It is used once and does not need to be maintained. Before installation, create a configuration file named gigamon-cloud.conf in the /tmp directory or after installing UCT-V you can add the configuration file in the /etc directory with the following detail:

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

  For more details on how to create tokens, refer to Token-based Authentication.

You can install the UCT-Vs either from Debian or RPM packages in two ways.

- 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

1. **To install UCT-V from Ubuntu/Debian:**
    a. Download the UCT-V**6.10.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
    b. Copy this package to your instance. Install the package with root privileges, for example:

    ```
    $ ls gigamon-gigavue_uctv_6.10.00_amd64.deb
    $ sudo dpkg -i gigamon-gigavue_uctv_6.10.00_amd64.deb
    ```

2. **To install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS:**
    a. Download the UCT-V**6.10.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
    b. Copy this package to your instance. Install the package with root privileges, for example:

    ```
    $ ls gigamon-gigavue_uctv_6.10.00_x86_64.rpm
    $ sudo rpm -i gigamon-gigavue_uctv_6.10.00_x86_64.rpm
    ```

3. Once the UCT-V package is installed, use the command below to perform pre-check, installation, and configuration functionalities.

```
sudo uctv-wizard
```

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

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 there are any missing packages, it will display an appropriate message with the missing package details. If all the packages are installed, it will display 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 Install Linux UCT-Vs using Manual Configuration.	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 will install the missing packages and restart the UCT-V service. Enter **N** if you wish to install it manually. Refer to the Install Linux UCT-Vs using Manual Configuration section for more details.
configure	sudo uctv-wizard configure	First, it checks for any existing configured file in the tmp directory. If available, UCT-V will use that configuration. If unavailable, UCT-V will automatically add 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

Options	Use Command	Description
		the required firewall policy, enter your option as **y**. The console interface will add the firewall rules automatically. Enter **N** if you wish to configure manually. Refer to the Install Linux UCT-Vs using Manual Configuration section for more details.
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, there is zero interference 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, and it will perform auto-configuration and restart 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 should 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

NOTE: When using Kernel version less than 5.4 on Ubuntu 16.04 with Python version 3.5 installed, follow the instructions given below before installing UCT-V.

```
sudo apt-get update
sudo apt install python3-netifaces
curl https://bootstrap.pypa.io/pip/3.5/get-pip.py -o get-pip.py
/usr/bin/python3.5 get-pip.py
```

```
sudo /usr/bin/python3.5 -m pip uninstall requests
sudo /usr/bin/python3.5 -m pip install requests==2.22.
```

To install from a Debian package:

1. Download the UCT-V**6.10.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue_uctv_6.10.00_amd64.deb
$ sudo dpkg -i gigamon-gigavue_uctv_6.10.00_amd64.deb
```

3. Once the UCT-V package is installed, 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 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' which will be 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.

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

   ```
   $ sudo service uctv restart
   ```

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

```
$ sudo service uctv status
```

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

NOTE: Use the following commands to install the required packages:.

```
sudo yum install iproute-tc -y
sudo yum install python3 -y
sudo yum install python3-pip -y
sudo pip3 install urllib3
sudo pip3 install requests
sudo pip3 install netifaces
```

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

1. Download the UCT-V**6.10.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue_uctv_6.10.00_x86_64.rpm
$ sudo rpm -i gigamon-gigavue_uctv_6.10.00_x86_64.rpm
```

3. Once the UCT-V package is installed, 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' which will be 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.

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

   ```
   $ sudo service uctv restart
   ```

The UCT-V status will be displayed as running. Check the status with the following command:

```
$ sudo service uctv status
```

Post Deployment Check:

After installing UCT-V, you can verify the version of UCT-V by running the following command:

1. Enter the command:

   ```
   sudo uctvl uctv-show
   ```

2. Manually execute the following command:

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

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 gives you more granular control over what traffic is monitored and mirrored.

Points to Note:

- VXLAN is the only tunnel type supported for Windows UCT-V.
- Loopback Interface is not supported for 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. It is used once and does not need to be maintained. Before installation, create a configuration file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** location or after installing UCT-V you can the configuration file in the **C:\ProgramData\Uctv\gigamon-cloud.conf** location with the following detail:

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

  For more details on how to create tokens, refer to Token-based Authentication.

Windows 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. Refer to Network Firewall Requirement for GigaVUE Cloud Suite for more details on the firewall requirements or security groups required for your environment.

The following ports for Network Firewall rules can be added from Firewall Settings.

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
Outbound	8892	TCP	UCT-V Subnet IP	Allows UCT-V to communicate with UCT-V Controller for registration and heartbeat
Outbound	4789	UDP	UCT-V Subnet IP	Allows UCT-V to tunnel VXLAN traffic to GigaVUE V Series Nodes
Outbound	4789	UDP	UCT-V Subnet IP	Allows UCT-V to tunnel L2GRE traffic to GigaVUE V Series Nodes

Install Windows UCT-Vs

You can install the UCT-Vs using MSI package in two ways.

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

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

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V **`6.10.00`** MSI package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator**, and the UCT-V service starts automatically.

3. Once the UCT-V package is installed, use the command below to perform pre-check, adapter setup, adapter restore, and configuration functionalities.

```
sudo uctv-wizard
```

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 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:** It is recommended 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	sudo 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. Refer to the Install Windows UCT-Vs using Manual Configuration section for more details.
adapter-restore	sudo 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

Options	Use Command	Description
		compatible network adapters, enter the option as **y**. • Enter **N** if you wish to restore it manually. Refer to the Install Windows UCT-Vs using Manual Configuration section for more details.
configure	sudo uctv-wizard configure	First, it checks for any existing configured file in the tmp directory. If available, UCT-V will use that configuration. If unavailable, UCT-V will automatically add 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 will add the firewall rules automatically. • Enter **N** if you wish to configure manually. Refer to the Install Windows UCT-Vs using Manual Configuration section for more details.
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 /**C:\ProgramData\uctv\uctv-installation.txt**

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

- 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, there is zero interference 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, and it will perform auto-configuration and restart the service.

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V**6.10.00** MSI package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator** and the UCT-V service starts automatically.

3. Once the UCT-V package is installed, 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 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.

   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 needs to be 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 will be 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
   2001:db8:abcd:ef01::/64 mirror-src-egress
   2001:db8:abcd:ef01::/64 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:ef02::/64 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:
   - Run 'sc stop uctv' and 'sc start uctv' from the command prompt.
   - Restart the UCT-V from the Windows Task Manager.

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

Uninstall UCT-V

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

- For Linux, to uninstall the UCT-V in Ubuntu/Debian, RPM, Red Hat Enterprise Linux, and CentOS packages, use the following command:

  ```
  sudo uctv-wizard uninstall
  ```

- For Windows, to 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 in two ways.

- Upgrade UCT-V manually on Virtual Machine
- Upgrade UCT-V through GigaVUE-FM

Refer to the following sections for more detailed information and step-by-step instructions on how to upgrade UCT-V:

Upgrade UCT-V manually on Virtual Machine

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.

Upgrade UCT-V through GigaVUE-FM

Upgrading UCT-V manually involves a series of steps to uninstall, install, and restart the service again. This method can be complicated when 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 more details and step-by-step process:

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

Rules and Notes:

- Currently, upgrades are only allowed to versions 6.9.00 or later. Ensure that the UCT-V Controller version is compatible with the version to which you are upgrading.
- 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.
- A UCT-V can only be associated with 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 will be rejected for the upgrade job.
- Upgrade through GigaVUE-FM is not applicable for OVS agents. For OVS tapping, you should upgrade the UCT-Vs manually.

Upload the UCT-V Images

Follow the below-listed 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. Click 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. Click **Choose File**, upload the UCT-V files from your local, and click **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 will not accept the image files with modified names.
   - When the upload is in process, GigaVUE-FM will not allow to upload a file with similar type and version.

5. Once completed, the uploaded UCT-V images will be listed in the **Images** page.

In the **Images** page, click **Filter** to filter the images based on Image Name, Version, and Image Type. You can delete one or multiple images. Select the required images and click **Delete** or **Delete All** from the Actions drop-down menu. 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, click **Dashboard** to view the UCT-V upgrade landing page.
2. 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.
3. Select the required UCT-Vs and click **Upgrade** from the **Actions** drop-down menu. **UCT-V Upgrade task** page appears.
4. Enter the task name.
5. In the **Image Version** drop-down menu, select the required version you want to upgrade to from the list of available image versions.
6. You can choose to upgrade immediately or schedule a time for the upgrade to happen. 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.

   NOTE: The upgrade should not be scheduled for a time in the past.

7. Click **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 will display a pop-up message with the list of UCT-Vs that are not compatible for upgrade. Click **Proceed** to ignore the unsupported UCT-Vs and upgrade the compatible ones, or click "**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 will change 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 will be marked with if it is successful and in case of failure. If the upgrade is successful, GigaVUE-FM will update 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.
> - In case of failure, you can upgrade the failed instance manually.

Integrate Private CA

If you want to integrate your own PKI infrastructure with GigaVUE-FM, you must generate a Certificate Signing Request (CSR) and get the CSR signed by the Certificate Authority (CA) and upload it back in GigaVUE-FM.

Rules and Notes

- The root CA must always be placed in a separate file.
- When using multiple intermediate CAs, ensure that they are placed in a single file in the correct order. The last intermediate CA in the chain should be placed at the top, followed by the preceding CAs in descending order.

Generate CSR

To create 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. In the **Country** field, enter the name of your country.
4. In the **Organization** field, enter your organization name.
5. In the **Organization Unit** field, enter the department or unit name.
6. In the **Common Name** field, enter the common name associated with the certificate.
7. From the **Algorithm** drop-down list, select the desired encryption algorithm used to encrypt your private key.
8. Click the **Generate CSR** button to create and download the 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** popup appears.
4. Click **Choose File** next to **Intermediate CA** to upload the signed intermediate CA certificate.
5. Click **Choose File** next to **Root CA** to upload the corresponding root or intermediate CA that signed the given intermediate CA.

You can view the uploaded CA certificate in the **CA Certificate** page.

Adding Certificate Authority

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

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

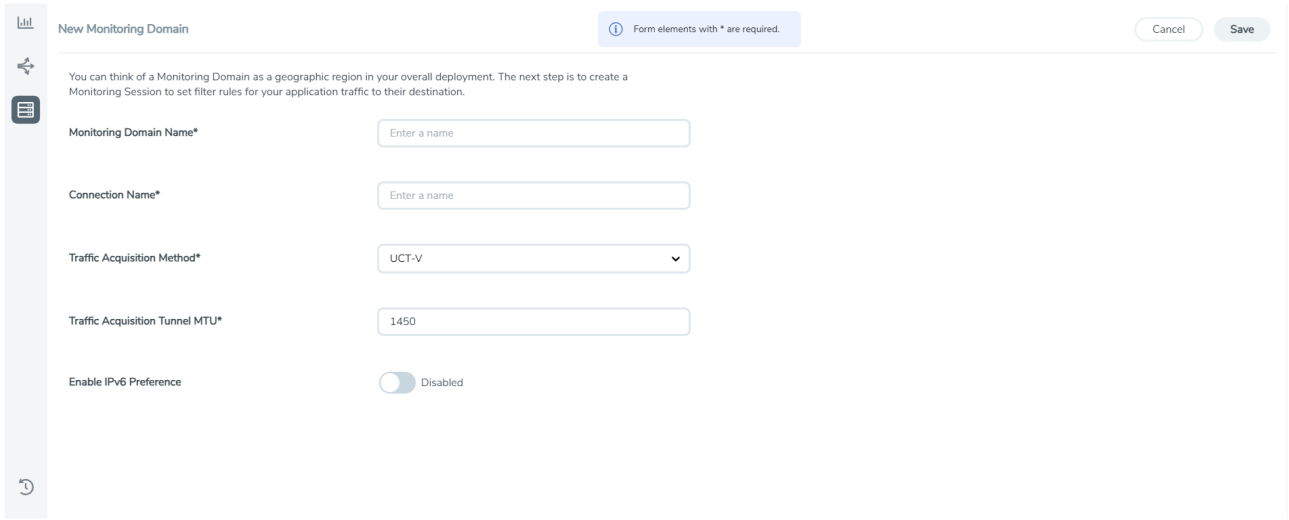
To upload the CA using GigaVUE-FM follow the steps given below:

1. Go to **Inventory > Resources > Security > CA List**.
2. Click **Add**, to add a new Custom Authority. The **Add Certificate Authority** page appears.
3. In the **Alias** field, enter the alias name of the Certificate Authority.
4. Use one of the following options to enter the Certificate 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**: Click **Choose File** to browse and select a certificate from the local directory.
5. Click **Save**.

Create Monitoring Domain

To create a monitoring domain in Third Party Orchestration:

1. Go to **Inventory > VIRTUAL > Third Party Orchestration**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. In the Monitoring Domain page, click **New**. The **Monitoring Domain Configuration** page appears.



3. Select or enter appropriate information as described in the following table:

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain. A monitoring domain consists of set of connections.
Connection Alias	An alias used to identify the connection.
Traffic Acquisition Method	Select a tapping method. The available options are: • **UCT-V**: UCT-Vs are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series nodes. If you select UCT-V as the tapping method, you must configure the UCT-V Controller to communicate to the UCT-Vs from GigaVUE-FM. The default MTU value is 1450. • **Customer Orchestrated Source**: If you select the Customer Orchestrated Source option, the mirrored, tunneled or the raw traffic from your workloads is directed directly to the GigaVUE V Series Nodes, and you need not configure the UCT-Vs and UCT-V Controllers.
Uniform Traffic Policy (When Traffic Acquisition Method is Customer Orchestrated Source)	Enable this option if you wish to use the same monitoring session configuration for the GigaVUE V Series Node deployed under this monitoring domain. Enable this check box when using packet mirroring configuration for GCP. **NOTE:** Once the monitoring session is deployed for the monitoring domain you cannot enable or disable this option.
Traffic Acquisition Tunnel MTU (When Traffic Acquisition Method is UCT-V)	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 V Series Node. The MTU values for the respective platforms when using IPv4 tunnels: AWS - 8950 Azure - 1450 OpenStack - 1450 Nutanix - 1250 GCP - 1410 When using IPv4 tunnels, the MTU must be 50 bytes less than the native MTU of the respective platform. The MTU values for the respective platforms when using IPv6 tunnels: AWS - 8930 Azure - 1430 OpenStack - 1430 Nutanix - 1230 GCP - 1390 When using IPv6 tunnels, the MTU must be 70 bytes less than the native MTU of the respective platform.
Enable IPv6 Preference	Enable this option to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

4. Click **Save**.

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.

You perform the following actions in the Monitoring domain page:

Actions	Description
Edit Monitoring Domain	Use to edit a monitoring domain.
Delete Monitoring Domain	Use to delete a Monitoring Domain.
Edit SSL Configuration	Use to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Generate Sysdump	You can select one or multiple GigaVUE V Series Nodes (Upto maximum 10) to generate the sysdump files. The generation of sysdump takes few minutes in GigaVUE V Series Node, you can proceed with other tasks and upon completion the status will be shown in GUI. These sysdump files can be used to troubleshoot the system. Refer to Debuggability and Troubleshooting for more information.
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. Auto-renewal is performed based on the duration specified in the **Certificate Settings** page. Refer to Configure Certificate Settings for more details.

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.

Edit SSL Configuration

You can add certificate authority and SSL keys to your fabric components after deploying it. To add certificate authority and SSL keys when using secure tunnels:

1. Go to **Inventory > VIRTUAL > Third Party Orchestration**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select the monitoring domain for which you want to add the SSL key.
3. Click the **Actions** drop down list and select **Edit SSL Configuration**. An **Edit SSL Configuration** window appears.
4. Select the CA in the **UCT-V Agent Tunnel CA** drop down list.
5. Select the SSL key in the **V Series Node SSL key** drop down list.
6. Click **Save**.

Deploy Fabric Components using Generic Mode

In generic mode, when deploying GigaVUE V Series Nodes you can provide the monitoring domain and connection name in your orchestration system. A Monitoring Domain will be automatically created under the **Third Party Orchestration** monitoring domain page in GigaVUE-FM and your GigaVUE fabric components will be deployed in that monitoring domain. In this case, the monitoring domain and connection will be created in GigaVUE-FM after the fabric component deployment in your orchestrator.

Refer to the following section for more detailed information on how to deploy your fabric components in the respective cloud platforms:

- Configure GigaVUE Fabric Components using AWS
- Configure GigaVUE Fabric Components using Azure
- Configure GigaVUE Fabric Components using GCP
- Configure GigaVUE Fabric Components using Nutanix
- Configure GigaVUE Fabric Components using OpenStack
- Configure GigaVUE Fabric Components using VMware ESXi
- Configure GigaVUE Fabric Components using Third Party Orchestration on NSX-T Federation Environment

Configure GigaVUE Fabric Components using AWS

This section provides step-by-step information on how to register GigaVUE fabric components using AWS EC2 or a configuration file.

Recommended Instance Type

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

Fabric Component	Machine type
GigaVUE V Series Node	c5n.xlarge
UCT-V Controller	t2.medium

Keep in mind the following when deploying the fabric components using generic mode:

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 8950 when using IPv4 tunnels or 8930 when using IPv6 tunnels. 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** value and click Save.
- Before deploying the Monitoring Session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- When deploying the fabric components using generic mode, the connection name must be used as the subGroupName in the registration data.
- You can also create a Monitoring Domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to Create Monitoring Domain for more detailed information on how to create monitoring domain under third party orchestration.
- Only **UCT-V** or **Customer Orchestrated Source** can be used as the traffic acquisition method when using generic mode.
- When you deploy the fabric components using third 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 AWS. Refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation for more detailed information on how to add network interfaces when launching an instance.
- Create tokens in the **User Management** page in GigaVUE-FM. Refer to Configure Tokens for Third Party Orchestration 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 AWS EC2, you can configure the following GigaVUE fabric components:

- Configure UCT-V Controller in AWS
- Configure UCT-V in AWS
- Configure GigaVUE V Series Nodes and V Series Proxy in AWS

Configure UCT-V Controller in AWS

You can configure more than one UCT-V Controller in a monitoring domain.

To register UCT-V Controller in AWS EC2, use any one of the following methods:

- Register UCT-V Controller during Instance Launch
- Register UCT-V Controller after Instance Launch

Register UCT-V Controller during Instance Launch

In your AWS EC2 portal, to launch the UCT-V Controller AMI instance and register UCT-V Controller using user data, follow the steps given below:

1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The UCT-V Controller uses this user data 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
```

3. You can navigate to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

The UCT-V Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller after Instance Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file, follow the steps given below:

1. Log in to the UCT-V Controller.
2. 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
```

3. Restart theUCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP. If you wish to assign a static IP address, follow the steps below:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file. (Other than the default 50-cloud-init.yaml file)
3. Update the file as shown in the following sample:

```
network:
        version: 2
        renderer: networkd
        ethernets:
                ens3:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens4:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens5:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
```

4. Save the file.
5. Restart theUCT-V Controller service.

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

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

Configure UCT-V in AWS

NOTE: Deployment of GigaVUE fabric components 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 on Linux and Windows UCT-V.

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

To register UCT-V in AWS, use any one of the following methods.

- Register UCT-V during Instance Launch
- Register UCT-V after Instance Launch

Register UCT-V during Instance Launch

NOTE: Registering UCT-V during Virtual Machine Launch is not applicable for Windows Agents. You can register your Windows Agents after launching the Virtual machine, using a configuration file.

In your AWS EC2, to launch the UCT-V AMI instance and register the UCT-V using user data, follow the steps given below:

1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The UCT-V uses this user data 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 UCT-V Controller 1>, <IP address of the UCT-V
Controller 2>
         sourceIP: <IP address of UCT-V> (Optional Field)
```

3. You can navigate to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

Register UCT-V after Instance Launch

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.

To register UCT-V after launching a Virtual Machine using a configuration file, follow the steps given below:

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)
   ```

   NOTE: 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.

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.

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if you do not wish to reveal the IP addresses of the GigaVUE V Series Nodes, then you can register your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

To register GigaVUE V Series Node and GigaVUE V Series Proxy in AWS EC2, use any one of the following methods.

- Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch
- Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data 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
```

   NOTE: You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series Proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the **`remotePort`** value as 443 and the **`remoteIP`** as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the **`remotePort`** value as 8891 and **`remoteIP`** as <IP address of the Proxy>.

3. You can navigate to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

1. Log in to the GigaVUE V Series Node or Proxy.
2. 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> or <IP address of the proxy>
    remotePort: 443
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use GigaVUE V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the `remotePort` value as 443 and the `remoteIP` as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

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

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

> **NOTE:** When the GigaVUE V Series Node is stopped or terminated from the AWS, it does not send any unregistration request and GigaVUE-FM will unregister the GigaVUE V Series Node soon after.

Configure GigaVUE Fabric Components using Azure

This section provides step-by-step information on how to register GigaVUE fabric components using Azure Portal or a configuration file.

Recommended Instance Type

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

NOTE: Additional instance types are also supported. Refer to Support, Sales, or Professional Services for deployment optimization.

Product	Instance Type	vCPU	RAM
GigaVUE V Series Node	Standard_D4s_v4	4 vCPU	16GB
	Standard_D8S_V4	8 vCPU	32GB
GigaVUE V Series Proxy	Standard_B1s	1 vCPU	1GB
UCT-V Controller	Standard_B4ms	4 vCPU	16GB

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.

Keep in mind the following when deploying the fabric components using generic mode:

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1450 when using IPv4 tunnels or 1430 when using IPv6 tunnels. 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** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to Create Monitoring Domain for more detailed information on how to create monitoring domain under third party orchestration.
- When creating virtual machine for deploying the fabric components in Azure, **SSH public key** must only be used as the **Authentication type** in Azure.
- Create tokens in the **User Management** page in GigaVUE-FM. Refer to Configure Tokens for Third Party Orchestration 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.

Prerequisites

GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC with Accelerated Networking enabled.

When creating a virtual machine for GigaVUE V Series Node using CLI, Management NIC and Data NIC can be attached at the time of the virtual machine creation. However, if you are using Azure GUI to create the virtual machine for GigaVUE V Series Node, then the data NIC can only be attached after creating the virtual machine. Refer to the following topics for more detailed information on how to create GigaVUE V Series Node with Management and Data NIC using CLI or Azure GUI:

- Create GigaVUE V Series Node with Management and Data NIC Attached using CLI
- Create GigaVUE V Series Node with Management and Data NIC Attached using Azure GUI

NOTE:

- Accelerated Networking must be enabled in the Data NIC only when deploying GigaVUE V Series Nodes using Third Party Orchestration.
- Accelerated Networking is not required for Management NIC.

Create GigaVUE V Series Node with Management and Data NIC Attached using CLI

Create management NIC:

```
az network nic create -g <resource group> --vnet-name <VNet Name> --subnet
<Subnet name> -n <Mangement NIC Name>
```

Create data NIC with Accelerated Networking enabled:

```
az network nic create -g <resource group> --vnet-name <VNet> --subnet <Subnet> -
n <Data NIC> --accelerated-networking true
```

Create GigaVUE V Series Node virtual machine using the above NICS:

```
az vm create --resource-group <Resource group> --size <Standard_D4s_v4/Standard_
D8S_V4> --name <GigaVUE V Series Node> --admin-username gigamon --generate-ssh-
keys --image gigamon-inc:gigamon-gigavue-cloud-suite:vseries-node:6.10.00 --
plan-name vseries-node --plan-product gigamon-gigavue-cloud-suite --plan-
publisher gigamon-inc --nics <Management NIC and Data NIC>
```

NOTE: You can use the following command to get all the images published by Gigamon.

```
az vm image list --all --publisher gigamon-inc
```

Create GigaVUE V Series Node with Management and Data NIC Attached using Azure GUI

Enable Management NIC when creating the GigaVUE V Series Node virtual machine. Refer to Create virtual machine topic in Azure Documentation for more detailed information on how to create a virtual machine. Follow the steps given below to attach the data NIC:

1. Select the GigaVUE V Series Node virtual machine from the Resources Page.
2. Stop the Virtual Machine using the **Stop** button.
3. Navigate to **Setting > Networking** from the left navigation pane. The **Networking** page appears.
4. In the **Networking** page, click **Attach network interface**. Select an existing network interface for Data NIC and click **OK**.
5. To enable accelerated networking, refer to Manage Accelerated Networking through the portal.
6. Start the Virtual Machine.

In your Azure Portal, you can configure the following GigaVUE fabric components:

- Configure UCT-V Controller in Azure
- Configure UCT-V in Azure
- Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure

Configure UCT-V Controller in Azure

You can configure more than one UCT-V Controller in a monitoring domain.

To register UCT-V Controller in Azure Portal, use any one of the following methods:

- Register UCT-V Controller during Virtual Machine Launch
- Register UCT-V Controller after Virtual Machine Launch

Register UCT-V Controller during Virtual Machine Launch

In your Azure portal, to launch the UCT-V Controller init virtual machine and register UCT-V Controller using custom data, follow the steps given below:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to Create virtual machine topic in Azure Documentation.

2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The UCT-V Controller uses this custom data 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 your Azure portal appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller after Virtual Machine Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file, follow the steps given below:

1. Log in to the UCT-V Controller.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following custom 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
```

3. Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP. If you wish to assign a static IP address, follow the steps below:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file. (Other than the default 50-cloud-init.yaml file)
3. Update the file as shown in the following sample:

```
network:
        version: 2
        renderer: networkd
        ethernets:
                ens3:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens4:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens5:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
```

4. Save the file.
5. Restart theUCT-V Controller service.

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

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

Configure UCT-V in Azure

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

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

To register UCT-V in Azure Portal, use any one of the following methods.

- Register UCT-V during Virtual Machine Launch
- Register UCT-V after Virtual Machine Launch

Register UCT-V during Virtual Machine Launch

NOTE: Registering UCT-V during Virtual Machine Launch is not applicable for Windows Agents. You can register your Windows Agents after launching the Virtual machine, using a configuration file.

In your Azure portal, to launch the UCT-V init virtual machine and register the UCT-V using custom data, follow the steps given below:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to Create virtual machine topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The UCT-V uses this custom data 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 UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
         sourceIP: <IP address of UCT-V> (Optional Field)
```

NOTE: 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>
```

Register UCT-V after Virtual Machine Launch

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.

To register UCT-V after launching a Virtual Machine using a configuration file, follow the steps given below:

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. Edit the local configuration file and enter the following custom 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)
```

   NOTE: 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.

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.

Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if the user does not wish to reveal the IP addresses of the nodes, then you can register your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

To register GigaVUE V Series Node and GigaVUE V Series Proxy in Azure Portal, use any one of the following methods.

- Register GigaVUE V Series Node and GigaVUE V Series Proxy during Virtual Machine Launch
- Register GigaVUE V Series Proxy after Virtual Machine Launch

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Virtual Machine Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy using the custom data in Azure Portal, follow the steps given below:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to Create virtual machine topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The GigaVUE V Series Node and GigaVUE V Series Proxy uses this custom data 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
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the `remotePort` value as 443 and the `remoteIP` as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

Register GigaVUE V Series Proxy after Virtual Machine Launch

To register GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

1. Log in to the GigaVUE V Series Proxy.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following custom data.

```
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
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the **`remotePort`** value as 443 and the **`remoteIP`** as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the **`remotePort`** value as 8891 and **`remoteIP`** as <IP address of the Proxy>.

3. Restart the GigaVUE V Series Proxy service.
   - GigaVUE V Series Node:
     `$ sudo service vseries-node restart`
   - GigaVUE V Series Proxy:
     `$ sudo service vps restart`

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

> **NOTE:** When the GigaVUE V Series Node is stopped or terminated from the Azure, it does not send any unregistration request and GigaVUE-FM will unregister the V Series Node soon after.

Keep in mind 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 and 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. The username would be **orchestration**, and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure there is no existing user in GigaVUE-FM, with the username **orchestration**.

Once the upgrade is complete, it is recommended that the password be changed on the Users page. Refer to Configure Role-Based Access for Third Party Orchestration for detailed steps on how to change password in the user page.

Configure GigaVUE Fabric Components using GCP

This section provides step-by-step information on how to register GigaVUE fabric components using Google Cloud Platform (GCP) or a configuration file.

Minimum Requirements

The following table lists the minimum requirements for deploying the fabric components:

Fabric Component	Machine type
GigaVUE V Series Node	• c2-standard-4 for 2 interfaces • c2-standard-8 for 3 interfaces
GigaVUE V Series Proxy	e2-micro
UCT-V Controller	e2-micro

Keep in mind the following when deploying the fabric components using GCP:

- With a default MTU of 1460 in GCP, ensure that the Traffic Acquisition Tunnel MTU is set to the value of 1410 when using IPv4 tunnels or 1390 when using IPv6 tunnels. 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** value and click **Save**. Refer to Traffic Acquisition Tunnel MTUfor more detailed information on Traffic Acquisition Tunnel MTU.
- For successful registration of fabric components, firewall rules must be configured to open ports. Refer to Use VPC firewall rules topic in GCP documentation for more detailed information on how to configure firewall rules. Refer to Network Firewall Requirement for more detailed information on ports that need to be opened.
- When you deploy the fabric components using third party orchestration, you cannot delete the Monitoring Domain or change the MTU without unregistering the registered fabric components.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to Create Monitoring Domain for more detailed information on how to create monitoring domain under third party orchestration.
- When launching an instance, if you wish to access it using a private key, you will have to add the key to the SSH key. The default password is gigamon.
- Create tokens in the **User Management** page in GigaVUE-FM. Refer to Configure Tokens for Third Party Orchestration 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 GCP, you can configure the following GigaVUE fabric components:

- Configure UCT-V Controller in GCP
- Configure UCT-V in GCP
- Configure GigaVUE V Series Nodes and V Series Proxy in GCP

Configure UCT-V Controller in GCP

You can configure more than one UCT-V Controller in a monitoring domain.

To register UCT-V Controller in GCP, use any one of the following methods:

- Register UCT-V Controller during Instance Launch
- Register UCT-V Controller after Instance Launch

Register UCT-V Controller during Instance Launch

In your GCP, to launch the UCT-V Controller and to register UCT-V Controller using custom metadata, follow the steps given below:

1. On the VM instances page of Google Cloud Platform, click **Create instances** . For detailed information, refer to Create and Start instance topic in GCP Documentation.
2. Under the **Metadata** tab, enter the **key** as **user-data** and in the **value** field enter the below mentioned text in the following format and deploy the instance. The UCT-V Controller uses this Custom Metadata 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>
        remotePort: 443
```

Register UCT-V Controller after Instance Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file, follow the steps given below:

1. Log in to the UCT-V Controller.
2. 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>
    remotePort: 443
```

3. Restart the UCT-V Controller service.

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

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

The UCT-V Controller deployed in GCP appears on the Third Party Orchestration Monitoring Domain page of GigaVUE-FM.

Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
MD1					
	[redacted]-vpc				Connected
		G-vTapController	[redacted]	1.7-304	Ok
		Gigamon-VSeriesProxy-1	[redacted]	2.1.0	Ok
		Gigamon-VSeriesNode-1	[redacted]	2.2.0	Ok

Configure UCT-V in GCP

NOTE: Deployment of GigaVUE fabric components through a third-party orchestrator is supported on Linux and Windows platforms.

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.

When using a windows UCT-V follow the steps given below installing the Windows UCT-V:

1. Deploy Windows server in GCP. Refer to Create a Windows Server VM instance in Compute Engine topic in Google documentation for step by step instructions.
2. After creating the windows server, follow the instruction in the *Connect to the VM instance by using RDP* section of Set up Chrome Remote Desktop for Windows on Compute Engine topic in the GCP documentation.
3. Download UCT-V build in your desktop and copy it to RDP session.
4. Turn off the Windows Firewall Defender. Then, install the Windows Agent refer to Windows UCT-V Installation for step-by-step instructions on how to install Windows Agent.

To register UCT-V in GCP, use any one of the following methods.

- Register UCT-V during Instance Launch
- Register UCT-V after Instance Launch

Register UCT-V during Instance Launch

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

NOTE: Registering UCT-V during Virtual Machine Launch is not applicable for Windows Agents. You can register your Windows Agents after launching the Virtual machine, using a configuration file.

In your GCP, to launch the instance and register the UCT-V using Custom Metadata, follow the steps given below:

1. On the VM instances page of Google Cloud Platform, click **Create instances** . For detailed information, refer to Create and Start instance topic in GCP Documentation.
2. Under the **Metadata** tab, enter the **key** as **user-data** and in the **value** field enter the below mentioned text in the following format and deploy the instance. The UCT-V uses this Custom Metadata 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 UCT-V Controller 1>, <IP address of the UCT-V
Controller 2>
```

Register UCT-V after Instance Launch

To register UCT-V after launching a Virtual Machine using a configuration file, follow the steps given below:

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to Linux_UCT-V_Installation.htm and Thirdparty_Windows_UCT-V_Installation.htm.
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>
   ```

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

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.

Configure GigaVUE V Series Nodes and V Series Proxy in GCP

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if the user does not wish to reveal the IP addresses of the nodes, then you can register your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

To register GigaVUE V Series Node and GigaVUE V Series Proxy in GCP, use any one of the following methods.

- Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch
- Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

1. On the VM instances page of Google Cloud Platform, click **Create an instance** . For detailed information on how to create a Virtual machine in GCP, refer to Create VMs with multiple network interfaces topic in GCP Documentation.
2. Under the **Metadata** tab, enter the **key** as **user-data** and in the **value** field enter the below mentioned text in the following format and deploy the instance. The UCT-V uses this Custom Metadata 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
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the `remotePort` value as 443 and the `remoteIP` as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using GigaVUE V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

1. Log in to the GigaVUE V Series Node or Proxy.
2. 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> or <IP address of the Proxy>
    remotePort: 443
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the **`remotePort`** value as 443 and the **`remoteIP`** as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using GigaVUE V Series proxy then, enter the **`remotePort`** value as 8891 and **`remoteIP`** as <IP address of the Proxy>.

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

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

> **NOTE:** When the GigaVUE V Series Node is stopped or terminated from the GCP, it does not send any unregistration request and GigaVUE-FM will unregister the V Series Node soon after.

Configure Packet Mirroring for GCP

Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers. The capture can be configured for both egress and ingress traffic, only ingress traffic, or only egress traffic.

NOTE: When deploying GigaVUE V Series Nodes for configuring Application Intelligence Session, Packet Mirroring should not be used. Since Application Intelligence uses stateful traffic, you may experience packet drop due to GCP platform limitation.

Refer to the following topics for detailed information.

- Configure Packet Mirroring in GCP
- Configure Monitoring Session with Packet Mirroring

Rules and Notes:

- Load Balancer forwards raw traffic. Therefore when configuring the monitoring session the Raw End Point must be used as the first component which receives traffic.
- Three NICs must be configured for GigaVUE V Series Node because REP and TEP cannot share the same interface.

A typical GCP deployment to support the internal load balancer and packet mirroring requires the following components:

- GigaVUE-FM
- GigaVUE V Series Node
- GCP Internal Load Balancer (uniformly distributes traffic from GCP target VMs to GigaVUE V Series Nodes)

Configure Packet Mirroring in GCP

This section provides step-by-step instructions on how to configure packet mirroring in GCP.

1. Create an instance template in GCP to deploy the GigaVUE V Series Node in GCP using Third Party Orchestration, refer to Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch for more detailed information on how to deploy GigaVUE V Series Node in GCP.

   - When using packet mirroring, a minimum of 3 NICs must be configured and the Machine Type must be c2-standard-8 (8 vCPU, 32GB memory).
   - Enable **IP Forwarding** when creating the instance template in GCP.

2. Create Instance Group in GCP with autoscaling in Managed Instance Group. Refer Create a MIG with autoscaling enabled topic in Google Cloud Platform Documentation for more details.
3. Configure TCP or UDP internal Load balancer with packet forwarding enabled and ensure that the GigaVUE V Series Nodes data NICs are used to receive traffic. Refer to Create a load balancer for Packet Mirroring section in Google Cloud Platform documentation for step-by-step instructions on how to create a TCP or UDP internal

Load balancer.

4. Configure packet mirroring in GCP, refer to Use Packet Mirroring topic in Google Cloud Documentation for step-by-step instructions.

After configuring packet mirroring in GCP, edit the Monitoring Domain in GigaVUE-FM and configure the Monitoring Session.

Configure Monitoring Session with Packet Mirroring

To configure monitoring session with packet mirroring enabled in GCP, follow the steps given below:

Edit the monitoring domain and update the following details:

1. Go to **Inventory > VIRTUAL > Third Party Orchestration**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select the Monitoring Domain with the GigaVUE V Series Node deployed with packet mirroring.
3. Click **Actions > Edit**.
4. In the **Monitoring Domain Configuration** page, select **Customer Orchestrated Source** as the Traffic Acquisition method.
5. Enable the **Uniform Traffic Policy** check box. When enabling this option, same monitoring session configuration will be applied to all GigaVUE V Series Nodes.
6. Click **Save** to save the configuration.

Create a monitoring session with the following instructions:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select **Third Party Orchestration**. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page. Refer to Create a Monitoring Session (Third Party Orchestration) for more detailed information on how to create a monitoring session.
3. In the **Edit Monitoring Session** page. Add Raw End Point as the first component and Tunnel End Point as the final component. Refer to Create Raw Endpoint (Third Party Orchestration) and Create Ingress and Egress Tunnel (Third Party Orchestration) for more detailed information on how to create tunnel endpoints and raw endpoints.
4. Add your application to the monitoring session. Connect your components.
5. To deploy the monitoring session after adding the Raw End Point click the **Deploy** button in the edit monitoring session page.
6. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the interface for REP and TEP from the drop-down menu.

Configure GigaVUE Fabric Components using Nutanix

This section provides step-by-step information on how to register GigaVUE fabric components using a configuration file.

Recommended Instance Type

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

Compute Instances	vCPU	Memory	Disk Space
GigaVUE V Series Node	4 vCPU	8GB	10GB
GigaVUE V Series Proxy	1 vCPU	4GB	8GB
UCT-V	1 vCPU	4GB	8GB
UCT-V Controller	1 vCPU	2GB	4GB

Keep in mind the following when deploying the fabric components using generic mode:

- Ensure that the Traffic Acquisition Tunnel MTU is set to thedefault value of 1250 when using IPv4 tunnels or 1230 when using IPv6 tunnels. 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** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- Create tokens in the **User Management** page in GigaVUE-FM. Refer to Configure Tokens for Third Party Orchestration for more detailed information.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to Create Monitoring Domain for more detailed information on how to create monitoring domain under third party orchestration.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- 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 Nutanix Prism Central, you can configure the following GigaVUE fabric components:

- Configure UCT-V Controller in Nutanix
- Configure UCT-V in Nutanix
- Configure GigaVUE V Series Nodes and V Series Proxy in Nutanix

Configure UCT-V Controller in Nutanix

You can configure more than one UCT-V Controller in a monitoring domain.

To register the UCT-V Controller in Nutanix, you can use any one of the following methods:

- Register UCT-V Controller during Instance Launch
- Register UCT-V Controller after Instance Launch

Register UCT-V Controller during Instance Launch

In the Nutanix Prism Central, to launch the UCT-V Controller instance and register the UCT-V Controller using user data, perform the following steps:

1. On the Prism Central, go to the **List** tab and click **Create VM**. The Create VM dialogue box appears. For more information, refer to Creating a VM through Prism Central (AHV) topic in the Nutanix Documentation.
2. On the **Step 3:Management** tab, in the Guest Customization field, select **Cloud-init (Linux)**. Enter the registration data in the text box and deploy the instance. The UCT-V Controller uses the user data to generate the config file (**/etc/gigamon-cloud.conf**) that is 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 Nutanix appears on the Monitoring Domain page of GigaVUE-FM.

Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
MD1					
	[redacted]vpc				Connected
		G-vTapController	[redacted]	1.7-304	Ok
		Gigamon-VSeriesProxy-1	[redacted]	2.1.0	Ok
		Gigamon-VSeriesNode-1	[redacted]	2.2.0	Ok

Register UCT-V Controller after Instance Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file, perform the following steps:

1. Log in to the UCT-V Controller.
2. 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
```

3. Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP. If you wish to assign a static IP address, follow the steps below:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file. (Other than the default 50-cloud-init.yaml file)
3. Update the file as shown in the following sample:

```
network:
        version: 2
        renderer: networkd
        ethernets:
                ens3:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens4:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens5:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
```

4. Save the file.
5. Restart theUCT-V Controller service.

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

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

NOTE: When you deploy GigaVUE V Series Nodes or UCT-V Controllers using 3rd party orchestration, you cannot delete the monitoring domain without unregistering the GigaVUE V Series Nodes or UCT-V Controllers.

Configure UCT-V in Nutanix

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

UCT-V should be registered using the registered UCT-V Controller. It uses PORT 8891.

To register UCT-V in Nutanix, you can use any one of the following methods.

- Register UCT-V during Instance Launch
- Register UCT-V after Instance Launch

Register UCT-V during Instance Launch

NOTE: Registering UCT-V during Virtual Machine Launch is not applicable for Windows Agents. You can register the Windows Agent after launching the Virtual machine using a configuration file. The configuration file is located in **C:\ProgramData\uctv\gigamon-cloud.conf**

In Nutanix Prism Central, to launch the UCT-V instance and register the UCT-V using user data, perform the following steps:

1. On the Prism Central, go to the **List** tab and click **Create VM**. The Create VM dialogue box appears. For detailed information, refer to Creating a VM through Prism Central (AHV) topic in Nutanix Documentation.

2. On the **Step 3:Management** tab, in the Guest Customization field, select **Cloud-init (Linux)**. Enter the registration data in the text box and deploy the instance. The UCT-V uses this user data 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 UCT-V Controller 1>, <IP address of the UCT-V
Controller 2>
         sourceIP: <IP address of UCT-V> (Optional Field)
```

NOTE: 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>
```

Register UCT-V after Instance Launch

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.

To register UCT-V after launching a Virtual Machine using a configuration file, perform the following steps:

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to Linux UCT-V Installation and Thirdparty_Windows_UCT-V_Installation.htm.
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)
```

   NOTE: 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.

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.

Configure GigaVUE V Series Nodes and V Series Proxy in Nutanix

NOTE: It is not mandatory to register GigaVUE V Series Nodes using the V Series proxy. However, if there are large number of nodes connected to GigaVUE-FM or if you want to hide the IP addresses of the nodes, then you can register the nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

NOTE: Before deploying GigaVUE V Series Node, enable the Multi Queue. For more information on enabling the multi-queue, refer to the Nutanix KB article How to change number of vNIC queues and enable RSS virtio-net Multi-Queue for AHV VMs. You can enable the Multi Queue using the Nutanix REST APIs. For more infomation on Nutanix APIs, refer to Nutanix support site.

To register GigaVUE V Series Node and GigaVUE V Series Proxy in Nutanix, you can use any one of the following methods.

- Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch
- Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

1. On the Prism Central, go to the **List** tab and click **Create VM**. The Create VM dialogue box appears. For detailed information, refer to Creating a VM through Prism Central (AHV) topic in Nutanix Documentation.
2. On the **Step 3:Management** tab, in the Guest Customization field, select **Cloud-init (Linux)**. enter the registration data in the text box and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data 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
```

NOTE: You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use GigaVUE V Series Proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the **`remotePort`** value as 443 and the **`remoteIP`** as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the **`remotePort`** value as 8891 and **`remoteIP`** as <IP address of the Proxy>.

Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, perform the following steps:

1. Log in to the GigaVUE V Series Node or Proxy.
2. Edit the 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> or <IP address of the Proxy>
    remotePort: 443
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the **`remotePort`** value as 443 and the **`remoteIP`** as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the **`remotePort`** value as 8891 and **`remoteIP`** as <IP address of the Proxy>.

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

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

Limitations

IPv6 is not supported by Nutanix for the current release of GigaVUE Cloud Suite.

Configure GigaVUE Fabric Components using OpenStack

This section provides step-by-step information on how to register GigaVUE fabric components using OpenStack or a configuration file.

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 generic mode:

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1450 when using IPv4 tunnels or 1430 when using IPv6 tunnels. 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** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to Create Monitoring Domain for more detailed information on how to create monitoring domain under third party orchestration.
- 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 Third Party Orchestration 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 UCT-V Controller in OpenStack
- Configure UCT-V in OpenStack
- Configure GigaVUE V Series Nodes and V Series Proxy in OpenStack

Configure UCT-V Controller in OpenStack

You can configure more than one UCT-V Controller in a monitoring domain.

To register UCT-V Controller in OpenStack, use any one of the following methods:

- Register UCT-V Controller during Instance Launch
- Register UCT-V Controller after Instance Launch

Register UCT-V Controller during Instance Launch

In your OpenStack dashboard, to launch the UCT-V Controller and register UCT-V Controller using Customization Script, follow the steps given below:

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 UCT-V Controller uses this registration data 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>
        remotePort: 443
```

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

Register UCT-V Controller after Instance Launch

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.

To register UCT-V after launching a Instance using a configuration file, follow the steps given below:

1. Log in to the UCT-V Controller.
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
```

3. Restart the UCT-V Controller service.
```
$ sudo service uctv-cntlr restart
```

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP. If you wish to assign a static IP address, follow the steps below:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file. (Other than the default 50-cloud-init.yaml file)
3. Update the file as shown in the following sample:

```
network:
        version: 2
        renderer: networkd
        ethernets:
                ens3:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens4:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens5:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
```

4. Save the file.
5. Restart theUCT-V Controller service.
```
$ sudo service uctv-cntlr restart
```

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

NOTE: When you deploy GigaVUE V Series Nodes or UCT-V Controllers using Third Party orchestration, you cannot delete the monitoring domain without unregistering the V Series Nodes or UCT-V Controllers.

Configure UCT-V in OpenStack

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.

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. Edit the local configuration file and enter the following Customization Script.

   - **/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>
   ```

   NOTE: 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-agent restart
   - Windows platform: Restart from the Task Manager.

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.

Configure GigaVUE V Series Nodes and V Series Proxy in OpenStack

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if the user does not wish to reveal the IP addresses of the nodes, then you can register your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

To register GigaVUE V Series Node and GigaVUE V Series Proxy in OpenStack, use any one of the following methods:

- Register V Series Nodes or V Series Proxy during Instance Launch
- Register V Series Node or V Series Proxy after Instance Launch

Register V Series Nodes or V Series Proxy during Instance Launch

To register V Series nodes or proxy using the Customization Script 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
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the `remotePort` value as 443 and the `remoteIP` as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

Register V Series Node or V Series Proxy after Instance Launch

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

1. Log in to the GigaVUE V Series Node or Proxy.
2. Edit the 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> or <IP address of the Proxy>
    remotePort: 443
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the **`remotePort`** value as 443 and the **`remoteIP`** as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the **`remotePort`** value as 8891 and **`remoteIP`** as <IP address of the Proxy>.

3. Restart the GigaVUE V Series Node or Proxy service.
   - GigaVUE V Series Node:
     `$ sudo service vseries-node restart`
   - GigaVUE 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 fabric component 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.

   > **NOTE:** When the GigaVUE V Series Node is stopped or terminated from the OpenStack, it does not send any unregistration request and GigaVUE-FM will unregister the V Series Node soon after.

Configure GigaVUE Fabric Components using VMware ESXi

This section provides step-by-step instructions on how to deploy the fabric components for VMware ESXi.

Register GigaVUE V Series Node

> **NOTE:**

- When registering GigaVUE V Series Nodes in GigaVUE-FM, the connection name under each Monitoring Domain must be unique.
- 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.
- Create tokens in the **User Management** page in GigaVUE-FM. Refer to Configure Tokens for Third Party Orchestration for more detailed information.

1. Login to VMware ESXi host using your web browser.
2. On the left navigation pane, select Virtual Machines and click **Create/Register VM**. The New Virtual Machine dialog box appears.
3. On the **Select Creation Type** page, select **Deploy a virtual machine from an OVF or OVA file**.

4. The OVA file is essentially a package of OVF files. For Third Party Orchestration deployment, you will need to extract the specific OVF file that has the desired characteristics, along with the VMDK and manifest files, from the OVA package. Unzip the **OVA** file that is obtained. After extracting the **OVA** file, you can select the required **OVF**, **VMDK**, and the **.mf** files from the multiple files that are available. Refer to the table below for details on the **OVF** files.

File Name	Form Factor	Comments	Supported Ports
vseries-node-file1.ovf	Small (2 vCPU, 4GB Memory, and 8GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware vCenter.	Mgmt Port, Tool Port, and 8 Network Ports
vseries-node-file2.ovf	Medium (4 vCPU, 8GB Memory, and 8GB Disk space)		
vseries-node-file3.ovf	Large (8 vCPU, 16GB Memory, and 8GB Disk space)		
vseries-node-file4.ovf	Small (2 vCPU, 4GB Memory, and 8GB Disk space)	Use these when deploying GigaVUE V Series Node via VMware NSX-T Manager.	Mgmt Port, Data Port, and Tool Port
vseries-node-file5.ovf	Medium (4 vCPU, 8GB Memory, and 8GB Disk space)		
vseries-node-file6.ovf	Large (8 vCPU, 16GB Memory, and 8GB Disk space)		
vseries-node-file7.ovf	Small (2 vCPU, 4GB Memory, and 8GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware ESXi without vCenter.	Mgmt Port, Tool Port, and 8 Network Ports
vseries-node-file8.ovf	Medium (4 vCPU, 8GB Memory, and 8GB Disk space)		
vseries-node-file9.ovf	Large (8 vCPU,		

File Name	Form Factor	Comments	Supported Ports
	16GB Memory, and 8GB Disk space)		
vseries-node-file12.ovf	Small (2 vCPU, 4GB Memory, and 80GB Disk space)	Not Applicable - Reserved.	
	Medium (4 vCPU, 8GB Memory, and 80GB Disk space)	Not Applicable - Reserved.	
	Larger (8 vCPU, 16GB Memory, and 80GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware vCenter and if you wish to configure AMX application.	Mgmt Port , Data Port, and Tool Port
vseries-node-file15.ovf	Small (2 vCPU, 4GB Memory, and 80GB Disk space)	Not Applicable - Reserved.	
	Medium (4 vCPU, 8GB Memory, and 80GB Disk space)	Not Applicable - Reserved.	
	Larger (8 vCPU, 16GB Memory, and 80GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware ESXi without vCenter and if you wish to configure AMX application	Mgmt Port , Data Port, and Tool Port
vseries-node-file16.ovf		minipc - Virtual Small Form Factor	Mgmt Port, Tool Port, and 2 Network Ports

5. The **Select OVF and VMDK files** page appears. Provide a name for the Virtual machine. Upload OVF, VMDK, and the .mf files. Click Next.

   NOTE: Ensure to edit and modify the **.mf** file to contain only the required **OVF** file type and the **VDMK** file.

6. Then, the **Select Storage** page appears, select the storage type and data store. Click Next.

7. Under the **Deployment Options**, provide the necessary details given below.
   a. Select the network port group associated with the host, network ports and tunneling port details from the **Network Mappings** drop-down.
   b. Select Thick/Thin from the **Disk provisioning** field.
   c. Select **Management Port DHCP** from the **Deployment type** drop-down.
   d. (optional) Enable the **Power on automatically** check-box to power on the Virtual Machine automatically.

   NOTE: Ensure to disable this option, if you are deploying GigaVUE V Series Nodes to export enriched metadata for Mobile Networks using the AMX application. Before powering on the Virtual Machine, ensure that the VM specifications are modified. Refer to the section below for more details on how to modify the VM specifications.

8. Under the additional settings page, provide the user data as shown below:

```
Hostname: <Host Name>
Administration Password: <Your Password>
GroupName: <Monitoring domain name>
SubGroupName: < Connection name>
token: <Token>
remoteIP: <IP address of the GigaVUE-FM>
remotePort: 443
Custom node properties: app_mode=linux_apps; (Update this option only if
you wish to export enriched metadata using the AMX application)
```

9. Review the setting selection in the **Ready to Complete page**, then click Finish.

The GigaVUE V Series Node is configured successfully.

Post Configuration Steps for Exporting Metadata for Mobile Networks using AMX

Follow the steps given below if you are deploying the GigaVUE V Series Node to configure AMX application to export enriched metadata for mobile networks.

1. Click edit on the VM page in the VMware ESXi, the **Edit Settings** page appears.
2. In the Virtual Hardware tab, edit the following fields:
   a. CPU: 40
   b. Memory: 128GB
   c. Hard disk 1: 200GB
   d. (optional) If you wish to get higher throughput, change the **Adapter type** for the Network Adapter to **SR-IOV passthrough**.

   When exporting GigaVUE enriched Metadata for Mobile Networks using AMX application, the GigaVUE V Series Node used to deploy AMX application can also be configured in GFM-HW2-FM001-HW. Refer to GigaVUE-FM Hardware Appliances Guide for more detailed instructions on how to set up GFM-HW2-FM001-HW.

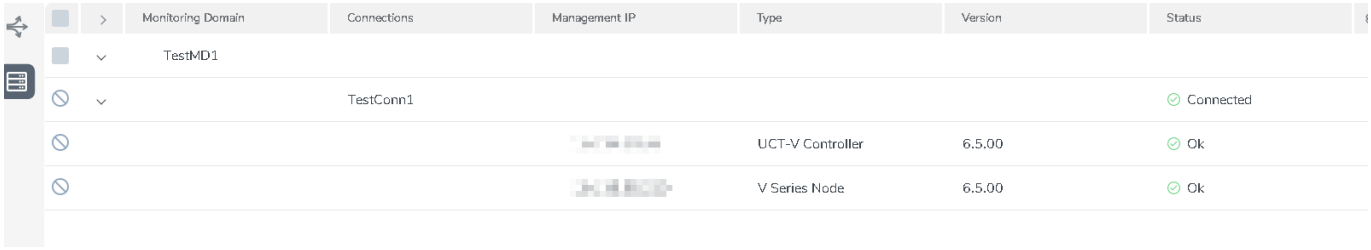
   Refer to Application Metadata Exporter for information about how to configure the AMX application.

For a high transactional ingress environment, follow the steps given below to edit the ring buffer settings:

NOTE: These steps must be performed consistently every time after rebooting the GigaVUE V Series Nodes.

1. Log in to the GigaVUE V Series Node.
2. Use the following command to view the maximum pre-set hardware settings value and your current hardware settings.
   ```
   sudo ethtool -g <interface name>
   ```
3. Ensure that the ingress interface ring buffers are set to the maximum supported values.

The GigaVUE V Series Node deployed in VMware ESXi host appears in Third-party Orchestration Monitoring Domain page of GigaVUE-FM.



Procedure to deploy V Series Node in VMware ESXi with SR-IOV Adapter

Follow the steps given below when you deploy V Series Node in VMware ESXi host with SR-IOV Adapter:

1. Click edit on the VM page in the VMware ESXi host environment, and the **Edit Settings** page appears.
2. In the Virtual Hardware tab, edit the following fields:
   a. CPU: 8
   b. Memory: 16GB
   c. Hard disk 1: 80GB
   d. Network adapter 1: VM Network (Connected)
   e. Network adapter 2: Port Group (Connected)
   f. Network adapter 3: Port Group (Connected)
   g. Video card: 4MB

   NOTE: Ensure that "Reserve all guest memory" is selected for VM Memory.

   Deploy V Series Node with OVF15 template (Large Form Factor), which has Management, Tool, and Data Ports. The Port-Group mappings and Netplan configs are as follows:

   Port-Group Mapping:

   - ens160 is mapped with VMNetwork
   - ens192 and ens224 are correctly mapped with the Port Groups created by the user

   Sample Netplan Configs:

   - ens192 with 192.168.10.X
   - ens224 with 192.168.20.X
3. Power off VM and remove Network Adapter 2 and Network Adapter 3. Now, without saving, add two new Network Adapters and change the **Adapter Type** to **SR-IOV passthrough**.
   Once added, the Port-Group mappings created by the user for ens192 and ens224 get swapped.
4. In **Edit Settings**, swap the adapters to correct the configuration mismatch with Netplan configs. Save the configuration and deploy the VM.
   Now, ens192 and ens224 will get mapped with the correct Port Group Mappings.
5. Use the following command to manually configure /etc/gigamon-cloud.conf with registration configurations to register V Series Node with GigaVUE-FM.

```
gigamon@vsn-5gc-new:~$ cat /etc/gigamon-cloud.conf
```

6. Under the additional settings page, provide the user data as shown below:
   - GroupName: <Monitoring domain name>
   - SubGroupName: < Connection name>
   - User: <Username>
   - Password: <Password>
   - remoteIP: <IP address of the GigaVUE-FM>
   - remotePort: 443

Configure GigaVUE Fabric Components using VMware vCenter

This section provides step-by-step instructions on how to deploy the fabric components using VMware vCenter.

GigaVUE Cloud Suite for VMware ESXi uses port mirroring for traffic acquisition method. However you can also use UCT-V for traffic acquisition. The traffic from the workload virtual machines can be acquired using UCT-V. The traffic acquired from the workload VMs is sent to the GigaVUE V Series Nodes for processing.

NOTE: 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.

Prerequisite

Create tokens in the **User Management** page in GigaVUE-FM. Refer to Configure Tokens for Third Party Orchestration for more detailed information.

Recommended Instance Type

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

Compute Instances	vCPU	Memory	Disk Space
GigaVUE V Series Node	4vCPU	8GB	8GB
UCT-V Controller	2vCPU	4GB	8GB

Refer to the following topics for more details on how to register the fabric components with GigaVUE-FM after deploying the fabric components using VMware vCenter on the host server:

- Register UCT-V Controller
- Register UCT-V
- Register GigaVUE V Series Node

Register UCT-V Controller

Deploy UCT-V Controller through VMware vCenter on the host server.

To register UCT-V Controller after launching a Virtual Machine using a configuration file, follow the steps given below:

1. Log in to the UCT-V Controller.
2. 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>
    remotePort: 443
```

3. When using Static IP configuration or multiple interfaces with Static IP configuration, create a new .yaml file in **/etc/netplan/** directory. Update the file and save it.
4. Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP. If you wish to assign a static IP address, follow the steps below:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file. (Other than the default 50-cloud-init.yaml file)
3. Update the file as shown in the following sample:

```
network:
        version: 2
        renderer: networkd
        ethernets:
                ens3:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens4:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens5:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
```

4. Save the file.
5. Restart theUCT-V Controller service.
```
$ sudo service uctv-cntlr restart
```

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

Register UCT-V

To register UCT-V after launching a Virtual Machine using a configuration file, follow the steps given below:

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>
```

4. Restart the UCT-V service.

NOTE: Before restarting the UCT-V service, update the **/etc/uctv/uctv.conf** file with network interface information to tap traffic and outgoing interface of tapped traffic.

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

Register GigaVUE V Series Node

NOTE: When registering GigaVUE V Series Nodes in GigaVUE-FM, the connection name under each monitoring domain must be unique.

1. Log in to the VMware vCenter web interface.
2. Right-click the ESXi Host, Cluster, or data center on which you want to deploy the GigaVUE V Series Node and then select Deploy OVF Template.

3. Provide a name for the Virtual machine. Upload OVF file and VMDK files based on the below table.

File Name	Form Factor	Comments	Supported Ports
vseries-node-file1.ovf	Small (2vCPU, 4GB Memory, and 8GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware vCenter.	Mgmt Port, Tool Port, and 8 Network Ports
vseries-node-file2.ovf	Medium (4vCPU, 8GB Memory, and 8GB Disk space)		
vseries-node-file3.ovf	Large (8vCPU, 16GB Memory, and 8GB Disk space)		
vseries-node-file4.ovf	Small (2vCPU, 4GB Memory, and 8GB Disk space)	Use these when deploying GigaVUE V Series Node via VMware NSX-T Manager.	Mgmt Port , Data Port, and Tool Port
vseries-node-file5.ovf	Medium (4vCPU, 8GB Memory, and 8GB Disk space)		
vseries-node-file6.ovf	Large (8vCPU, 16GB Memory, and 8GB Disk space)		
vseries-node-file7.ovf	Small (2vCPU, 4GB Memory, and 8GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware ESXi without vCenter.	Mgmt Port, Tool Port, and 8 Network Ports
vseries-node-file8.ovf	Medium (4vCPU, 8GB Memory, and 8GB Disk space)		
vseries-node-file9.ovf	Large (8vCPU, 16GB Memory, and 8GB Disk space)		
vseries-node-	Larger (8vCPU,	Use these files when deploying	Mgmt Port , Data Port, and

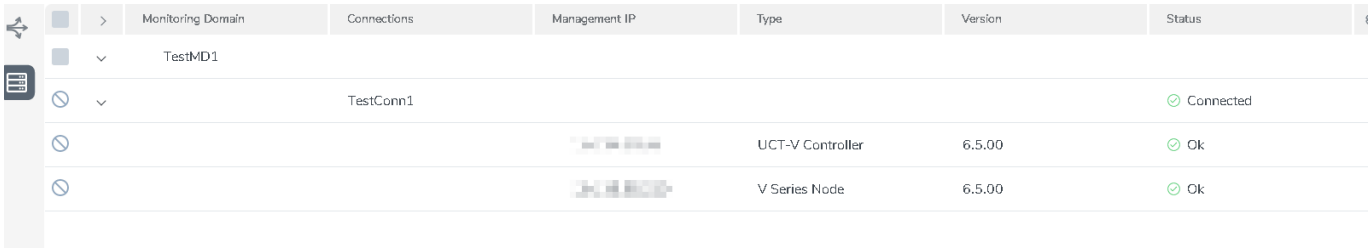
File Name	Form Factor	Comments	Supported Ports
file12.ovf	16GB Memory, and 80GB Disk space)	GigaVUE V Series Node via VMware vCenter and if you wish to configure AMX application.	Tool Port
vseries-node-file15.ovf	Larger (8vCPU, 16GB Memory, and 80GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware ESXi without vCenter and if you wish to configure AMX application	Mgmt Port , Data Port, and Tool Port
vseries-node-file16.ovf		minipc - Virtual Small Form Factor	Mgmt Port, Tool Port, and 2 Network Ports

4. Click Next and complete the Virtual machine launch. Refer VMware Documentation for more detailed information.
5. Log in to the GigaVUE V Series Node.
6. 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>
    remotePort: 443
```

7. Restart the GigaVUE V Series Node service.
   - GigaVUE V Series node:
     ```
     $ sudo service vseries-node restart
     ```
8. Review the setting selection in the **Ready to Complete page**, then click **Finish**.

The GigaVUE V Series Node deployed in VMware vCenter host appears in Third-party Orchestration Monitoring Domain page of GigaVUE-FM.



Configure GigaVUE Fabric Components using Third Party Orchestration on NSX-T Federation Environment

This section provides step-by-step instructions on how to deploy the fabric components for VMware NSX-T federated environment.

GigaVUE Cloud Suite for VMware uses service insertion as the traffic acquisition method. However, service insertion is not supported for VMware NSX-T federated environment. The traffic from the workload virtual machines can be acquired using UCT-V. The traffic acquired from the workload VMs is sent to the GigaVUE V Series Nodes for processing.

GigaVUE-FM and the fabric components are deployed on the VMware NSX-T local segments or between the stretch segments across multiple sites. The fabric components are deployed using third party orchestration.

NOTE: 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.

Prerequisites:

- Create tokens in the **User Management** page in GigaVUE-FM. Refer to Configure Tokens for Third Party Orchestration for more detailed information

- Upload OVF file and VMDK files on vCenter based on the below table:

File Name	Form Factor	Comments	Supported Ports
vseries-node-file1.ovf	Small (2vCPU, 4GB Memory, and 8GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware vCenter.	Mgmt Port, Tool Port, and 8 Network Ports
vseries-node-file2.ovf	Medium (4vCPU, 8GB Memory, and 8GB Disk space)		
vseries-node-file3.ovf	Large (8vCPU, 16GB Memory, and 8GB Disk space)		
vseries-node-file4.ovf	Small (2vCPU, 4GB Memory, and 8GB Disk space)	Use these when deploying GigaVUE V Series Node via VMware NSX-T Manager.	Mgmt Port , Data Port, and Tool Port
vseries-node-file5.ovf	Medium (4vCPU, 8GB Memory, and 8GB Disk space)		
vseries-node-file6.ovf	Large (8vCPU, 16GB Memory, and 8GB Disk space)		
vseries-node-file7.ovf	Small (2vCPU, 4GB Memory, and 8GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware ESXi without vCenter.	Mgmt Port, Tool Port, and 8 Network Ports
vseries-node-file8.ovf	Medium (4vCPU, 8GB Memory, and 8GB Disk space)		
vseries-node-file9.ovf	Large (8vCPU, 16GB Memory, and 8GB Disk space)		

File Name	Form Factor	Comments	Supported Ports
vseries-node-file12.ovf	Larger (8vCPU, 16GB Memory, and 80GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware vCenter and if you wish to configure AMX application.	Mgmt Port , Data Port, and Tool Port
vseries-node-file15.ovf	Larger (8vCPU, 16GB Memory, and 80GB Disk space)	Use these files when deploying GigaVUE V Series Node via VMware ESXi without vCenter and if you wish to configure AMX application	Mgmt Port , Data Port, and Tool Port
vseries-node-file16.ovf		minipc - Virtual Small Form Factor	Mgmt Port, Tool Port, and 2 Network Ports

Refer to the following topics for more details on how to register the fabric components with GigaVUE-FM after deploying the fabric components using VMware vCenter on the host server:

- Register UCT-V Controller
- Register UCT-V
- Register GigaVUE V Series Node

Register UCT-V Controller

Deploy UCT-V Controller through VMware vCenter on the host server.

To register UCT-V Controller after launching a Virtual Machine using a configuration file, follow the steps given below:

1. Log in to the UCT-V Controller.
2. 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
```

3. Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP. If you wish to assign a static IP address, follow the steps below:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file. (Other than the default 50-cloud-init.yaml file)
3. Update the file as shown in the following sample:

```
network:
        version: 2
        renderer: networkd
        ethernets:
                ens3:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens4:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens5:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
```

4. Save the file.
5. Restart the UCT-V Controller service.

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

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

Register UCT-V

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.

To register UCT-V after launching a Virtual Machine using a configuration file, follow the steps given below:

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)
```

   NOTE: 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.

   NOTE: Before restarting the UCT-V service, update the **/etc/uctv/uctv.conf** file with network interface information to tap traffic and outgoing interface of tapped traffic.

   - Linux platform:

     $ sudo service uctv restart

   - Windows platform: Restart from the Task Manager.

Register GigaVUE V Series Node

Refer to Configure GigaVUE Fabric Components using VMware ESXi topic for step-by-step instructions on how to deploy GigaVUE V Series Node on VMware ESXi host.

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

Deploy Fabric Components using Integrated Mode

In integrated mode, you create a monitoring domain in your respective GigaVUE Cloud Suite in GigaVUE-FM and then use your own orchestration system to just deploy nodes. The GigaVUE V Series Nodes deployed using your own orchestration system will be displayed under the monitoring domain created in your respective GigaVUE Cloud Suite. In this case, ensure that the monitoring domain and the connection name given in the GigaVUE-FM matches the groupName and subGroupName in the user data provided in your orchestration system.

You can also create a monitoring domain and connection under Third party Orchestration and use the monitoring domain name and connection name as the groupName and sunGroupName in the registration data used in your respective cloud platform.

Refer to the following topics on more detailed information on how to deploy your fabric components in the respective cloud platforms:

- Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode
- Configure GigaVUE Fabric Components in Azure
- Configure GigaVUE Fabric Components in OpenStack

Configure Secure Communication between Fabric Components in FMHA

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

Follow these steps to configure secure communication in FMHA mode:

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. Change 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 Community Portal.
6. Access 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 for Third Party Orchestration

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 Network Firewall Requirement 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.
- After configuring secure tunnels, if a Monitoring Domain has only one GigaVUE V Series Node and that GigaVUE V Series Node reboots or restarts, then the SSL Keys must be manually added to the Monitoring Domain again. Refer to Edit SSL Configuration for more detailed information on how to add SSL keys to a Monitoring Domain.

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 private keys and SSL certificates in GigaVUE V Series Node. Refer to the following steps for configuration:

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td>1.</td><td>Upload a Custom Authority Certificate (CA)</td><td>You must upload a Custom Certificate to UCT-V Controller for establishing 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. Click New, to add a new Custom Authority. The Add Custom 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.

For more information, refer to the section Adding Certificate Authority</td></tr>
<tr><td>2.</td><td>Upload a SSL Key</td><td>You must add a SSL key to GigaVUE V Series Node. To add SSL Key, follow the steps in the section SSL Decrypt.</td></tr>
<tr><td>3</td><td>Enable the secure tunnel</td><td>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 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 SSL Key and CA certificate, after deploying the fabric components.</td><td>You must select the added SSL Key and CA Authority in GigaVUE V Series Node after creating a Monitoring Domain configuring the fabric components in GigaVUE-FM. Refer to Edit SSL Configuration for more detailed information on how to select the added SSL Key and CA Authority in GigaVUE V Series Node.</td></tr>
</table>

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>Refer to</th></tr>
<tr><td>1.</td><td>Upload a Certificate Authority (CA) Certificate</td><td>You must upload a Custom Certificate to UCT-V Controller 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 section Adding Certificate Authority</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 Upload SSL Keys.</td></tr>
<tr><td>3</td><td>Create a secure tunnel between UCT-V and the first GigaVUE V Series Node</td><td>You should enable the secure tunnel feature to establish a connection between the UCT-V and the 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 SSL Key and CA certificate, after deploying the fabric components.</td><td>You must select the added SSL Key and CA Authority in GigaVUE V Series Node after creating a Monitoring Domain configuring the fabric components in GigaVUE-FM. Refer to Edit SSL Configuration for more detailed information on how to select the added SSL Key and CA Authority in GigaVUE V Series Node.</td></tr>
<tr><td>5</td><td>Create an Egress tunnel from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session.</td><td>You must create a 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 Ingress and Egress Tunnels for more detailed information on how to create</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td></td><td>tunnels.
To create the egress tunnel, follow these steps:
1. After creating a new Monitoring Session, or click Actions > Edit on an existing Monitoring Session, the GigaVUE-FM canvas appears.
2. In the canvas, select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table:
<table><tr><th>Field</th><th>Action</th></tr><tr><td>Alias</td><td>The name of the tunnel endpoint.</td></tr><tr><td>Description</td><td>The description of the tunnel endpoint.</td></tr></table></td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td>Type</td><td>Select TLS-PCAPNG for creating egress secure tunnel</td></tr>
<tr><td>Traffic Direction</td><td>Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:
MTU- The default value is 1500.
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.
DSCP - Enter the Differentiated Services Code Point (DSCP) value.
Flow Label - Enter the Flow Label value.
Source L4 Port- Enter the Souce L4 Port value
Destination L4 Port - Enter the Destination L4 Port value.
Flow Label
Cipher- Only SHA 256 is supported.
TLS Version - Select TLS Version1.3.
Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments.
SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.
Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments.</td></tr>
<tr><td>Remote Tunnel IP</td><td>Enter the interface IP address of the the second GigaVUE V Series Node (Destination IP).</td></tr>
</table>
4. Click Save.
</td></tr>
<tr><td>6</td><td>Select the added SSL Key after deploying the fabric components in the second GigaVUE V Series Node</td><td>You must select the added SSL Key in the second GigaVUE V Series Node. Select the the second GigaVUE V Series Node and follow the steps given in Edit SSL Configuration.</td></tr>
<tr><td>7</td><td>Create an ingress tunnel in the second GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring</td><td>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. Refer to Create a Monitoring Session to know about Monitoring Session.</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td>Session for the second GigaVUE V Series Node.</td><td>To create the ingress tunnel, follow these steps:
1. After creating a new Monitoring Session, or click Actions > Edit on an existing Monitoring Session, the GigaVUE-FM canvas appears.
2. In the canvas, select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table:
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td>Alias</td><td>The name of the tunnel endpoint.</td></tr>
<tr><td>Description</td><td>The description of the tunnel endpoint.</td></tr>
<tr><td>Type</td><td>Select TLS-PCAPNG for creating egress secure tunnel</td></tr>
<tr><td>Traffic Direction</td><td>Choose In (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6.</td></tr>
<tr><td>IP Version</td><td>The version of the Internet Protocol. IPv4 and IPv6 are supported.</td></tr>
<tr><td>Remote Tunnel IP</td><td>Enter the interface IP address of the first GigaVUE V Series Node (Destination IP).</td></tr>
</table>
4. Click Save.</td></tr>
</table>

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 click **Monitoring Domain**.
2. In the Monitoring Domain page, **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 **Configure Secure Tunnel** section.

Create Prefiltering Policy Template

GigaVUE-FM allows you to create a prefiltering policy template with a single rule or multiple rules. You can configure a rule with a single filter or multiple filters. Each monitoring session can have a maximum of 16 rules.

To create a prefiltering policy template, do the following steps:

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

2. Click **New**.

3. Enter the name of the template in the **Template Name** field.

4. Enter the name of a rule in the **Rule Name** field.

5. Click any one of the following options:

- Pass — Passes the traffic.
- Drop — Drops the traffic.

NOTE: In the absence of a prefilter rule, traffic is implicitly allowed. However, once rules are defined, they include an implicit drop rule. Should the traffic not conform to any of the specified rules, it will be dropped.

6. Click any one of the following options as per the requirement:

- 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.

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

7. Select the value of the priority based on which the rules must be prioritized for filtering. Select the value as 1 to pass or drop a rule in top priority. Similarly, you can select the value as 2, 3, 4 to 8, where 8 can be used for setting a rule with the least priority. Drop rules are added based on the priority and, then pass rules are added.

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

- L3
- L4

9. Select the **Filter Name** from the following options:
   - ip4Src
   - ip4Dst
   - ip6Src
   - ip6Dst
   - Proto - It is common for both ipv4 and ipv6.
10. Select the **Filter Relation** from any one of the following options:
   - Not Equal to
   - Equal to
11. Enter the source or destination port value in the **Value** field.
12. Click **Save**.

NOTE: Click **+** to add more rules or filters. Click **-** 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:

- If you wish to use Selective Precryption, your GigaVUE-FM and the fabric components version must be 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 will pass all the traffic.
- Once the templates are associated with a Monitoring Session, any changes made in the template will not be reflected in the Monitoring Session.

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

- Create Precryption Template for Filtering based on Applications
- Create Precryption Template for Filtering based on L3-L4 details

Create Precryption Template for Filtering based on Applications

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

1. Go to **Traffic > Resources > Precryption**. The **Precryption Policies** page appears.
2. Click the **APPLICATION** tab.
3. Click **Add**. The New Precryption Template page appears.
4. Select **csv** as the **Type**, if you wish to add applications using a .csv file.
   a. You can download the sample .csv file and edit it.
   b. Save your .csv file.
   c. Click **Choose File** and upload the file.
5. Select **Manual** as the **Type**, if you wish to add the applications manually. Enter the **Application Name** and click + icon to add more applications.
6. Click **Save**.

The added applications are displayed 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

1. Go to **Traffic > Resources > Precryption**. The **Precryption Policies** page appears.
2. Click the **L3-L4** tab.
3. Enter or select the following details as mentioned in the below table:

Fields	Description
Template	Enter a name for the template.
Rule Name	Enter a name for the rule.
Action	Choose any 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.

Fields	Description
	However, once rules are defined, they include an implicit pass all rule. Should the traffic not conform to any of the specified rules, it will be passed.
Direction	Choose any 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.
Priority	Select the value of the priority based on which the rules must be prioritized for filtering. Select the value as 1 to pass or drop a rule in top priority. Similarly, you can select the value as 2, 3, 4 upto 8, where 8 can be used for setting a rule with the least priority. Drop rules are added based on the priority and, then pass rules are added.
Filters	
Filter Type	Select the **Filter Type** from the following options: • L3 • L4 **NOTE:** L4 Filter Type can only be used with L3.
L3:	
Filter Name	Select the **Filter Name** from the following options: • IPv4 Source • IPv4 Destination • IPv6 Source • IPv6 Destination • Protocol - It is common for both IPv4 and IPv6.
Filter Relation	Select the **Filter Relation** from any one of the following options: • Not Equal to • Equal to
Value	Enter or Select the Value based on the selected **Filter Name**. **NOTE:** When using **Protocol** as the **Filter Name**, select **TCP** from the drop-down menu.
L4:	

Fields	Description
Filter Name	Select the **Filter Name** from the following options: • Source Port • Destination Port
Filter Relation	Select the **Filter Relation** from any one of the following options: • Not Equal to • Equal to
Value	Enter the source or destination port value.

4. Click **Save**.

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

The template is successfully created. To enable Precryption, refer to Monitoring Session Options (Third Party Orchestration) 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

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

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

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

- Create a Monitoring Session (Third Party Orchestration)
- Create Ingress and Egress Tunnel (Third Party Orchestration)
- Create Raw Endpoint (Third Party Orchestration)
- Create Map
- Add Applications to Monitoring Session
- Interface Mapping
- Deploy Monitoring Session

- View Monitoring Session Statistics
- Visualize the Network Topology (Third Party Orchestration)

Create a Monitoring Session (Third Party Orchestration)

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

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

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

You can create multiple Monitoring Sessions per Monitoring Domain.

To create a new Monitoring Session:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Click **New Monitoring Session** to open the New Monitoring Session configuration page.
3. In the **Alias** field, enter a name for the Monitoring Session.
4. From the **Monitoring Domain** drop-down list, select the desired Monitoring Domain or click **Create New** to create a new Monitoring Domain. Refer to Create a Monitoring Domain section in the respective cloud guides..
5. From the **Connections** drop-down list, select the required connections that are to be included as part of the Monitoring Domain.
6. 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.

   NOTE: Distributed Deduplication is only supported on GigaVUE V Series Node version 6.5.00 and later.
7. Click **Save**. The Monitoring Session Overview page appears.

Monitoring Session Page (Third Party Orchestration)

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

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

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

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

You can use the  icon on the left side of the Monitoring Session page to view the Monitoring Sessions list. Click  to filter the Monitoring Sessions list. In the side bar, you can:

- 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).

Monitoring Session Options (Third Party Orchestration)

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

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

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

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

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

Apply Threshold Template

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. Refer to Traffic Health Monitoring section for more details on Threshold Template. Click **Save** to save the newly created template.
3. Click **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. Click **Clear Thresholds** to clear the applied thresholds across the selected Monitoring Session.

Enable User Defined Applications

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

1. In the Monitoring Session **TRAFFIC PROCESSING** page, click **User Defined Applications** under **Options** menu.
2. Enable the **User-defined Applications** toggle button.
3. You can 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, Traffic Distribution option is renamed to Distributed De-duplication.

Create Ingress and Egress Tunnel (Third Party Orchestration)

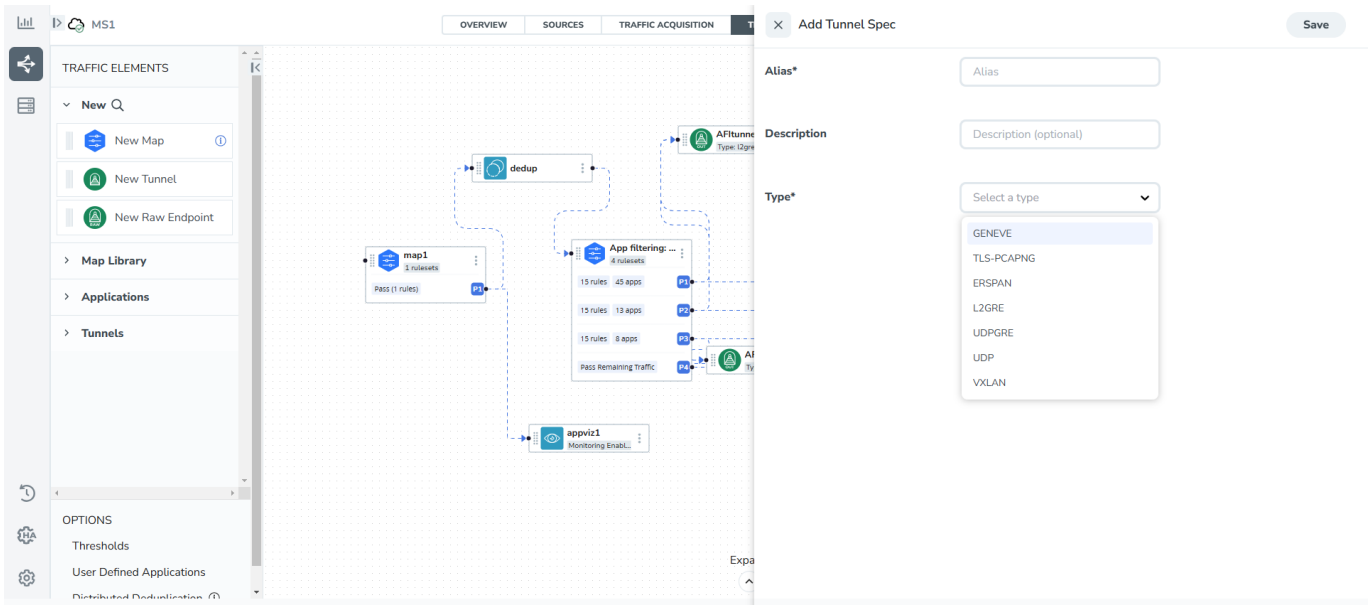
Traffic from the GigaVUE V Series Node is distributed to tunnel endpoints in a monitoring session. A tunnel endpoint can be created using a standard L2GRE, VXLAN, UDPGRE, or ERSPAN tunnel.

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

To create a new tunnel endpoint:

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

2. In the canvas, click the icon on the left side of the page to view the traffic processing elements. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
3. Enter the **Alias**, **Description**, and **Type** details. Refer to Details - Add Tunnel Specifications table.



4. Click **Save**.

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

To apply a threshold template to Tunnel End Points, click the menu button of the required tunnel end point on the canvas and click **Details**. In the quick view, go to **Threshold** tab. For more details on how to create or apply a threshold template, refer to Monitor Cloud Health topic in the respective Cloud guides.

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

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

Field	Description	
	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 **NOTE:** 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.
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.

Field	Description	
	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.
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **NOTE:** In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . Refer to the Secure Tunnels.		
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

Field	Description	
		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.
ERSPAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	**IP Version**	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **NOTE:** In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . Refer to 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 will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

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 network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.
UDP:		

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

Create Raw Endpoint (Third Party Orchestration)

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

To add Raw Endpoint to the monitoring session:

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. Click **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. Click **Deploy**.
5. Click **Export** to download all or selected V Series Nodes in CSV and XLSX formats.

Create a New Map

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

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

Keep in mind the following when creating a map:

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

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps** Below are the filter rule types that work in ATS: • mac Source • mac Destination • ipv4 Source • ipv4 Destination • ipv6 Source • ipv6 Destination • VM Name Destination • VM Name Source • VM Tag Destination - Not applicable to Nutanix. • VM Tag Source - Not applicable to Nutanix. • VM Category Source - Applicable only to Nutanix. • VM Category Destination - Applicable only to Nutanix. • Host Name -Applicable only to Nutanix and VMware. The traffic direction is as 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. **Notes:** • For OpenStack environment, Subnet Name Source and Subnet Name Destination are the exclusion filters available as part of Exclusion Maps with Traffic Acquisition method as OVS Mirroring in the Monitoring Domain. • If no ATS rule filters listed above are used, all VMs and vNICS are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.
- Loopback captures bidirectional traffic from both ingress and egress. To prevent duplicate tapping, only egress tapping is permitted.

- If you are running GigaVUE Cloud Suite on OpenStack, you can add a subnet to the exclusion map. To do this, create an exclusion map and select the Subnet name in the ruleset.
- If a packet is fragmented then all the fragments will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide* for detailed information.

To create a new map:

1. 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, click on **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. Click on **Rule Sets** tab.
   a. **To create a new rule set:**
      i. Click **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. Click **Actions > New Rule**.
      ii. Select a required condition from the drop-down list. Click ... and select **Add Condition** to add more conditions.
      iii. Select the rule to **Pass** or **Drop** through the map.
4. Click **Save**.

Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. Refer to Example- Create a New Map using Inclusion and Exclusion Maps for more detailed information on how to configure Inclusion and Exclusion maps using ATS.

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

- To edit a map, click the ⋮ menu button of the required map on the canvas and click **Details**, or click **Delete** to delete the map.
- To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, click on the Thresholds tab. For more details on how to create or apply threshold templates, refer to Monitor Cloud Health.
- Hover over the rules and apps buttons on the map to view the rule and applications configured for the selected map. Click 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. Click on the Expand icon at the bottom of the Monitoring session canvas. The Inclusion Maps and Exclusion Maps section appears.
5. Drag and drop a new map template to the Inclusion Maps region. The New Map quick view appears. Enter the Name and Description of the map.
    a. In the **GENERAL** tab, enter the name as Inclusionmap1 and enter the description. In the **RULESETS**, enter the priority and Application Endpoint ID.
    b. Select the condition as VM Name and enter the VM Name as **target-1**. Then the instance with VM name **target-1-1, target-1-2,** and **target-1-3** will be included.

6. Drag and drop a new map template to the Exclusion Maps region. The New Map quick view appears. Enter the details as mentioned in the above section.
   a. In the **GENERAL** tab, enter the name as Exclusionmap1 and enter the description. In the **RULESETS** tab, enter the priority and Application Endpoint ID.
   b. Select the condition as VM Name and enter the VM Name as **target-1-3**. Then the instance **target-1-3** will be excluded.

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

Map Library

To reuse a map,

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

The Map is saved to the **Map Library** in the **TRAFFIC PROCESSING** canvas page. This map can be used from any of the Monitoring Session. To reuse the map, drag and drop the saved map from the Map Library.

Add Applications to Monitoring Session

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

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- GENEVE Decap
- Header Stripping
- Application Metadata Exporter

- SSL Decrypt
- GigaSMART NetFlow Generation
- 5G-Service Based Interface Application
- 5G-Cloud Application

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

You can also configure the following GigaSMART operations from the **Traffic > Solutions > Application Intelligence**:

- Application Metadata Intelligence
- Application Filtering Intelligence

For more information, refer to these GigaSMART Operations in the *GigaVUE Fabric Management Guide*.

Interface Mapping

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

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Navigate to **V SERIES NODES** tab and click **Interface Mapping**.
3. The **Deploy Monitoring Session** dialog box appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.
4. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the Monitoring Session from the drop-down menu for the selected individual GigaVUE V Series Nodes. Then, click **Deploy**.

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

Deploy Monitoring Session

To deploy the Monitoring Session:

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

   NOTE: You can drag multiple arrows from a single map and connect them to different maps.
3. (Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method) Click **SOURCES** tab to view details about the subnets and monitored instances.
4. Click **Deploy** from the **Actions** menu to deploy the Monitoring Session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series Nodes.
5. You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab. When you click on the Status link, the Deployment Report is displayed. If the Monitoring Session is not deployed properly, then one of the following errors is displayed in the Status column.
   - Success—The session is not deployed on one or more instances due to V Series Node failure.
   - Failure—The session is not deployed on any of the V Series Nodes or Instances.

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

View Monitoring Session Statistics

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

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

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

- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.

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

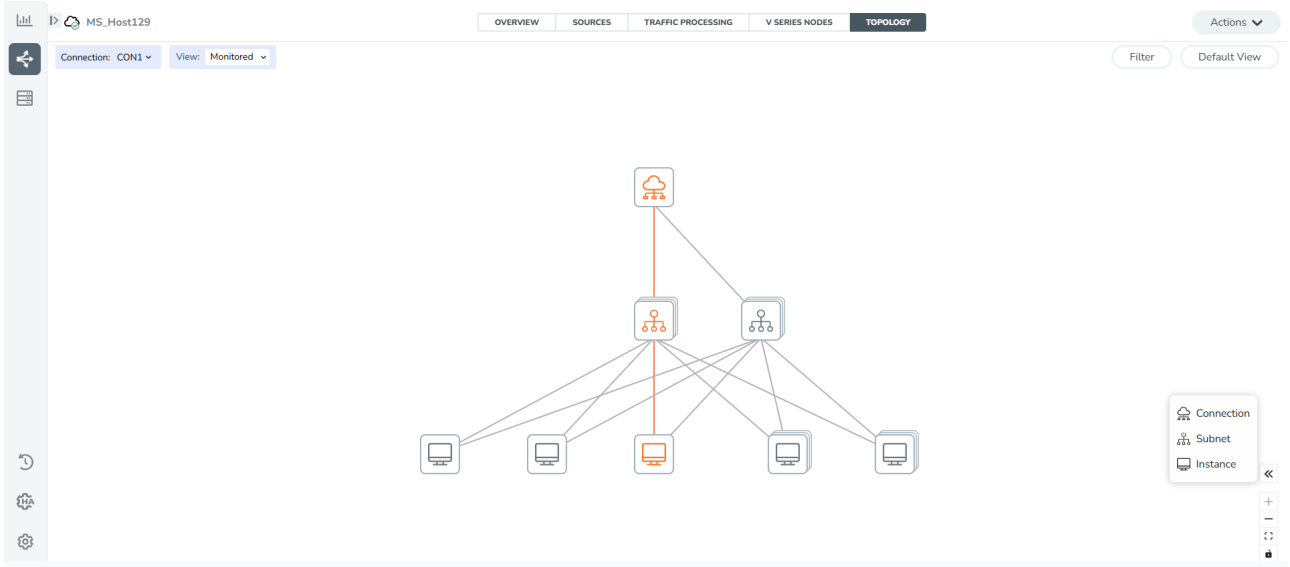
Visualize the Network Topology (Third Party Orchestration)

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

To view the topology in GigaVUE-FM:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TOPOLOGY** tab. The Topology page appears.
3. Select a connection from the **Connection** list. The topology view of the monitored subnets and instances in the selected session are displayed.

4. Select the instance type from **View**. The available instance types are Fabric and Monitored.



5. (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. Click the subnet or VM group icons to explore the subnets or instances within the group.

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

- Use the **Filter** button to filter the instances based on the VM name, VM IP, 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.
- Use **+** or **-** icons to zoom in and zoom out the topology view.
- Click 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 enable or disable 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, you should change the option precryption-path-mtu in UCT-V configuration file (**/etc/uctv/uctv.conf**) within the range 1400-9000 based on the platform path MTU.

- Protocol version IPv4 and IPv6 are supported.
- If you wish to use IPv6 tunnels, your GigaVUE-FM and the fabric components version must be 6.6.00 or above.

To create a new monitoring session with Precryption, follow these steps:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page.
3. Enter the appropriate information for the monitoring session as described in the following table:

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

4. Click **Next**. The **Edit Monitoring Session** page appears with the new canvas.
5. Click **Options** button. The Monitoring Session Options appears.
6. Click **Precryption** tab.
7. Enable **Precryption**.
8. Click **Save**. The **Edit Monitoring Session** page appears. You can proceed to create map, tunnels, and adding applications.

NOTE: It is recommended to enable the secure tunnel feature whenever the Precryption feature is enabled. Secure tunnel helps to securely transfer the cloud captured packets or precrypted data to a GigaVUE V Series Node. For more information, refer to Secure Tunnel .

Validate Precryption connection

To validate the Precryption connection, follow the steps:

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

Limitations

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

Migrate Application Intelligence Session to Monitoring Session

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

- View Details
- Delete
- Forced Delete

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

Points to Note:

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

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

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

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

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

Post Migration Notes for Application Intelligence

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

1. If you wish to enable Secure tunnels after migrating the Application Intelligence Session, follow the steps given below.
   a. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
   b. Select a Monitoring Session from the Monitoring Sessions list view on the left side of the screen and click the **TRAFFIC ACQUISITION** tab.
   c. Enable Secure tunnels. Refer to the *Configure Monitoring Session Options* topic in the respective GigaVUE Cloud Suite Deployment Guide for information about how to enable secure tunnel for a Monitoring Session.
   d. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Undeploy**. The Monitoring Session is undeployed.
   e. Select the Monitoring Session for which you enabled Secure Tunnels and edit the Monitoring Session.
   f. Add the Application Intelligence applications.
   g. Modify the Number of Flows as per the below table:

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

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

   h. Click **Deploy**. Refer to Application Intelligence section in the GigaVUE V Series Applications Guide for more detailed information on how to deploy the Application Intelligence applications.

2. When GigaVUE-FM version is 6.5.00, and the GigaVUE V Series Node version is below 6.5.00, after migrating theApplication Intelligence Session to the Monitoring Session and redeploying the monitoring session, a momentary loss in the statistical data of the Application Visualization application will be seen while redeploying the monitoring session.

3. After migrating the Application Intelligence Session to monitoring session, if you wish to make any configuration changes, then the GigaVUE V Series Node version must be greater than or equal to 6.3.00.

Monitor Cloud Health

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

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

Configuration Health Monitoring

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

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

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

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

Traffic Health Monitoring

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

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

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

For V Series Nodes:

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

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

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

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

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

- Threshold configuration can be 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

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

Dedup	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
HeaderStripping	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
TunnelEncapsulation	1. Tx Packets 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
AMI Exporter	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

5G-SBI	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SBIPOE	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
PCAPNG	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

Create Threshold Templates

To create threshold templates:

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

Field	Description
Threshold Template Name	The name of the threshold template.
Thresholds	
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. Click **Save**. The newly created threshold template is saved, and it appears on the **Threshold** templates page.

Apply Threshold Template

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

Apply Threshold Template to Monitoring Session

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

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

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

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

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

Clear Thresholds

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

Clear Thresholds for Applications

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

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

Clear Thresholds across the Monitoring Session

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

1. In GigaVUE-FM, on the left navigation pane, 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**, click **Clear Thresholds**.
3. The **Clear Threshold** pop-up appears. Click **Ok**.

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

View Health Status

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

View Health Status of an Application

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

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

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

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

View Health Status for Individual GigaVUE V Series Nodes

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

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

Administer GigaVUE Cloud Suite for Third Party Orchestration

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

- Configure Third Party Orchestration Settings
- Role Based Access Control

Configure Certificate Settings

To configure certificate settings:

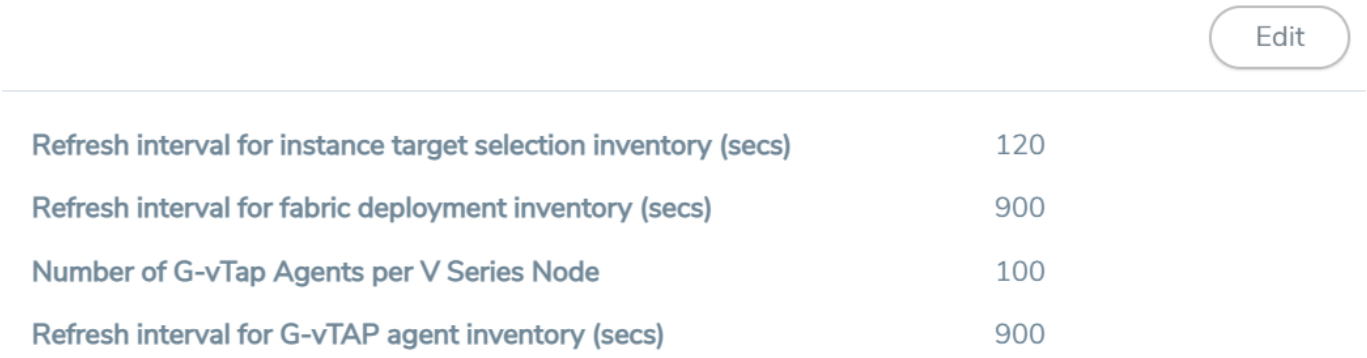
1. Go to **Inventory > VIRTUAL**. Select your cloud platform.
2. Click **Settings > Certificate Settings**. The **Certificate Settings** page appears.
3. From the **Algorithm** drop-down list, select the algorithm that determines the cryptographic security of the certificate.

   NOTE: If selecting RSA 8192, note that certificate generation may take longer due to the increased key size.
4. In the **Validity** field, enter the total validity period of the certificate.
5. In the **Auto Renewal** field, enter the number of days before expiration the auto-renewal process should begin.
6. Click **Save**.

Configure Third Party Orchestration Settings

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

Go to **Inventory > VIRTUAL > Third Party Orchestration**, and then click **Settings** to edit the Third Party Orchestration settings.



In the Settings page, select **Advanced** tab to edit these Third Party Orchestration settings.

Settings	Description
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of the instances.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for deploying the fabric components
Number of UCT-Vs per V Series Node	Specifies the maximum number of UCT-Vs that can be assigned to the GigaVUE V Series Node. **Points to Note:** • At the time of GigaVUE V Series Node deployment, GigaVUE-FM maps the UCT-Vs equally to all the available GigaVUE V Series Node. For example, there are 10 UCT-Vs, two GigaVUE V Series Nodes, and the Number of UCT-Vs per V Series Node is ten. Even though the first GigaVUE V Series Node can accommodate all the ten UCT-Vs, it will be shared equally between the two GigaVUE V Series Node to balance the traffic load. • When a new GigaVUE V Series Node is added to the deployment, GigaVUE-FM does not re-balance the UCT-Vs to the new GigaVUE V Series Node unless the number of UCT-Vs mapped to the GigaVUE V Series Node is greater than the Number of UCT-Vs per V Series Node.
Refresh interval for UCT-V inventory (secs)	Specifies the frequency for discovering the UCT-Vs

Settings	Description
	available.
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.
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.

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 Proxy Server (for AWS and Azure) • Cloud Fabric Deployment • Cloud Configurations • Sys Dump • Syslog • Cloud licenses • Cloud Inventory	• Configure GigaVUE Cloud Components • Create Monitoring Domain and Launch Visibility Fabric • Configure Proxy Server (applicable only for AWS and Azure)
Traffic Control Management: This includes the following traffic control resources: • Monitoring session	• Create, Clone, and Deploy Monitoring Session • Add Applications to Monitoring Session • Create Maps • View Statistics

Resource Category	Cloud Configuration Task
• Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps	• Create Tunnel End Points

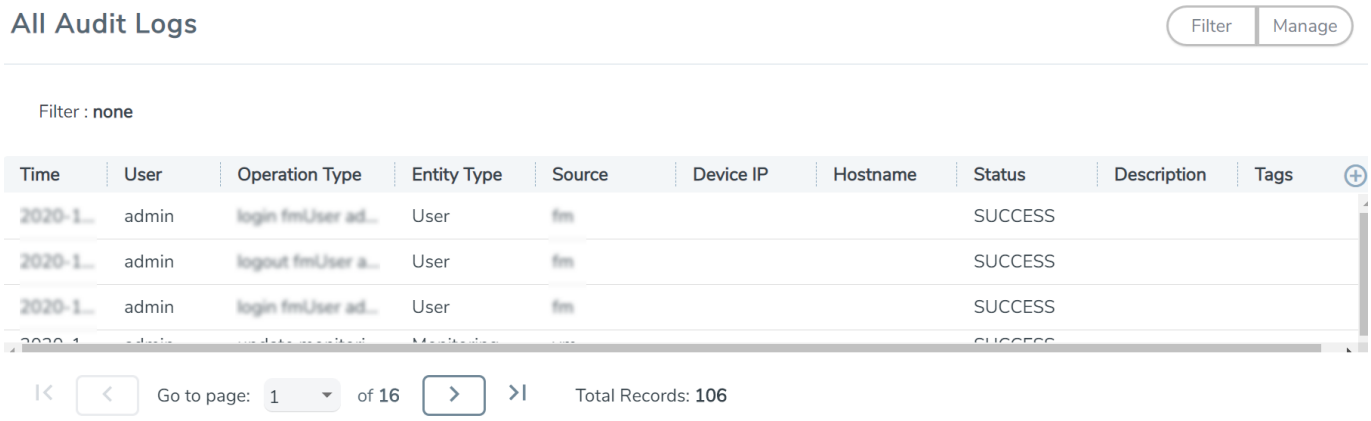
NOTE: Cloud APIs are also RBAC enabled.

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

About Audit Logs

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

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



The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: ▪ Log in and Log out based on users. ▪ Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.

Parameters	Description
Source	Provides details on whether the user was in GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

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

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

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

To filter the audit logs, do the following:

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

Debuggability and Troubleshooting

Refer to the following topics for details:

Sysdumps

A sysdump is a collection of logs and system data that are used for debugging purposes. A sysdump is generated when a GigaVUE V Series Node crashes (e.g., kernel, application, or hardware crash).

NOTE: If the fabric component is deleted or unreachable, the sysdump files cannot be downloaded.

Sysdumps—Rules and Notes

Keep in mind 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 another sysdump file generation 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 will 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.

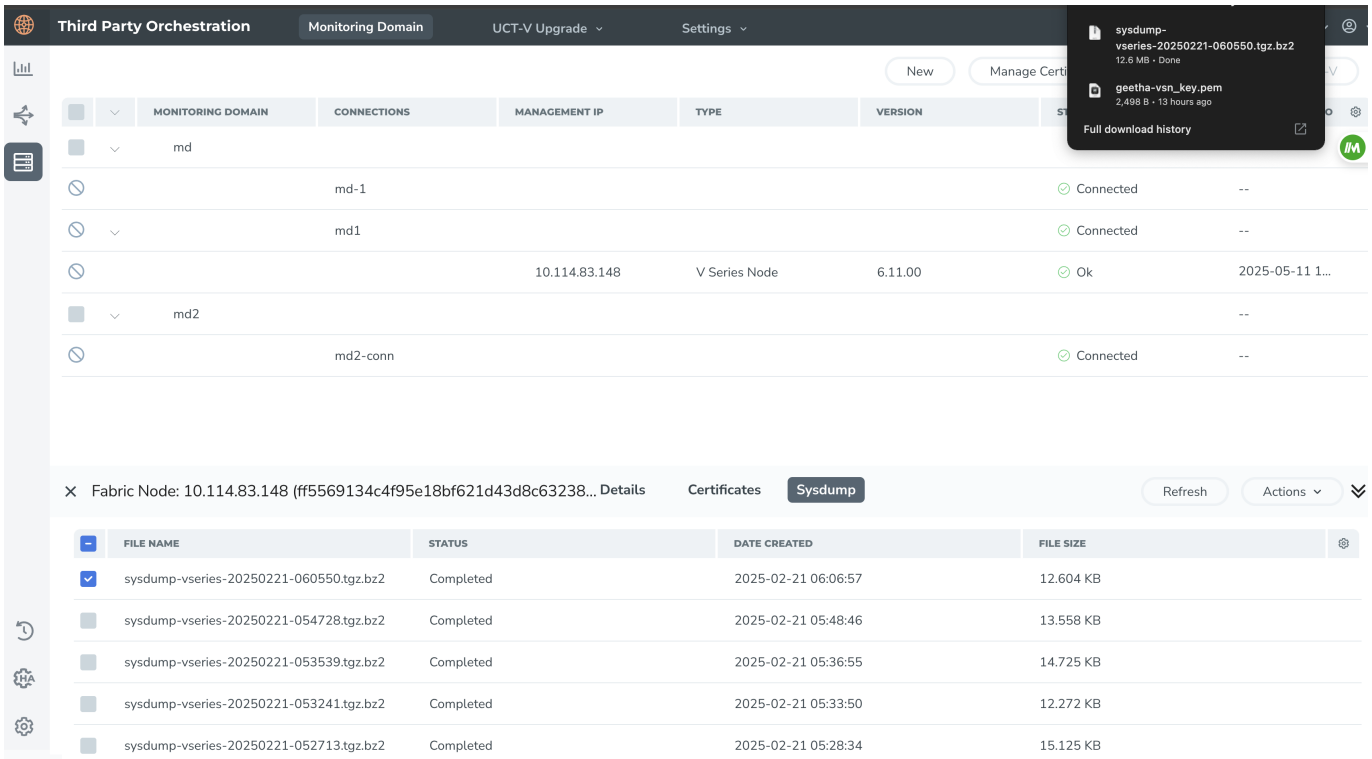
Generate a Sysdump File

To generate a sysdumps file:

1. Go to **Inventory > VIRTUAL > Third Party Orchestration > Monitoring Domain.** The **Monitoring Domain** page appears.
2. Select the required node, and use one of the following options to generate a sysdump file:

- Click **Actions > Generate Sysdump**.
- In the lower pane, go to **Sysdump**, and click **Actions > Generate Sysdump**.

To view the latest status, click **Refresh**.



To download a sysdump file, select the file in the lower pane, and then click **Actions > Download**.
To delete a sysdump file, select the file in the lower pane, and then select a sysdump file to delete. Click **Actions > Delete**. To bulk delete, select all the sysdump files, and then click **Actions > Delete All.**

FAQs - Secure Communication between GigaVUE Fabric Components

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?**

   There are no modifications to the behavior across any of the upgrade paths. You may proceed with upgrades without the necessity for any additional steps. Upon upgrading the nodes, the corresponding certificates will be deployed in accordance with the respective 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 ports numbers that needs to be opened for the respective fabric components.

Component	Port
GigaVUE-FM	9600
GigaVUE V Series Node	80
GigaVUE V Series Proxy	8300, 80
UCT-V Controller	8300, 80
UCT-V	8301, 8892, 9902 For more details, refer to .

4. **Are there any changes to the registration process for deploying the fabric components using Third Party Orchestration?**

   Starting from version 6.10, you must place tokens in the gigamon-cloud.conf file instead of username and password. To generate the token in GigaVUE-FM, go to **Settings > Authentication > User Management > Token**. Refer to Configure Tokens for Third Party Orchestration for more details.

   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. You must create a configuration file named gigamon-cloud.conf with the token and place it in the /tmp directory during UCT-V installation or after installing UCT-V you can add the configuration file in the /etc directory.

   NOTE: UCT-V will not be added to GigaVUE-FM without this token.

6. **Can you use your own PKI infrastructure to issue certificates for the Fabric Components?**

   Integrating your Public Key Infrastructure (PKI) with GigaVUE-FM is not feasible. 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 a fabric component with version 6.9 or earlier with custom certificates upgrades to version 6.10, new fabric components will be launched with certificates signed by the GigaVUE-FM, and custom certificates will no longer be used in fabric components with version 6.10 or above versions.
   - When GigaVUE-FM is running on version 6.10 and deploying fabric components with version 6.9 or earlier, selecting a custom certificate ensures that the fabric components are deployed with the specified custom certificates.

8. **How to issue certificates after upgrading the fabric components to 6.10?**

   When the upgrade process begins, GigaVUE-FM will transmit the certificate specifications to the new fabric components using the launch script. The fabric components will then utilize these specifications to generate its own certificate.

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. Refer to Configure Secure Communication between Fabric Components in FMHA for more details.

   NOTE: This step is essential exclusively if you are using cloud deployments in FMHA mode and need to deploy or upgrade the fabric components to version 6.10 or later.

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 6.10 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 6.10 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud TAP - Container Deployment Guide

GigaVUE Cloud Suite 6.10 Hardware and Software Guides
Gigamon Containerized Broker Deployment Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices Sanitization guidelines for GigaVUE Fabric Management Guide and GigavUE-OS devices.
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

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

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to 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)