



GigaVUE Cloud Suite Deployment Guide - OpenStack

GigaVUE Cloud Suite

Product Version: 6.9

Document Version: 1.2

(See Change Notes for document updates.)

Copyright 2025 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.9	1.2	04/04/2025	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.9	1.1	01/18/2025	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.9	1.0	12/06/2024	The original release of this document with 6.9.00 GA.

Contents

GigaVUE Cloud Suite Deployment Guide - OpenStack	1
Change Notes	3
Contents	4
GigaVUE Cloud Suite Deployment Guide - OpenStack	8
Overview of GigaVUE Cloud Suite for OpenStack	8
GigaVUE-FM	9
UCT-V	9
UCT-V Controller	10
GigaVUE V Series Node	10
GigaVUE V Series Proxy	11
Monitoring Domain	11
Monitoring Session	11
Cloud Overview Page (OpenStack)	11
Top Menu	12
Viewing Charts	13
Viewing Monitoring Session Details	14
Introduction to the Supported Features for OpenStack	15
Precryption™	15
How Gigamon Precryption Technology Works	16
Why Gigamon Precryption	17
Key Features	17
Key Benefits	17
How Gigamon Precryption Technology Works	18
Supported Platforms	20
Prerequisites	20
Secure Tunnels	21
Prefiltering	23
Customer Orchestrated Source - Use Case	23
Licensing GigaVUE Cloud Suite	24
Default Trial Licenses	24
Volume Based License (VBL)	25
Base Bundles	26
Add-on Packages	26
How GigaVUE-FM Tracks Volume-Based License Usage	27

Activate Volume-Based Licenses	27
Manage Volume-Based Licenses	28
Get Started with GigaVUE Cloud Suite for OpenStack	
Deployment	31
Before You Begin	31
Supported Hypervisor for OpenStack	31
Minimum Compute Requirements	32
Network Requirements	33
Virtual Network Interface Cards (vNICs)	34
Security Group for OpenStack	34
Key Pairs	40
Prerequisites for OVS Mirroring	40
OVS-Mirror Requirements	40
OpenStack Cloud Environment Requirements	41
GigaVUE-FM Version Compatibility	43
Default Login Credentials	43
Install and Upgrade GigaVUE-FM	44
Deploy GigaVUE Cloud Suite for OpenStack	45
Deployment Options for GigaVUE Cloud Suite for OpenStack	45
Deploy GigaVUE Fabric Components using OpenStack	46
Deploy GigaVUE Fabric Components using GigaVUE-FM	46
Upload Fabric Images	48
Install GigaVUE-FM on OpenStack	50
Initial GigaVUE-FM Configuration	52
Install UCT-V	53
Supported Operating Systems for UCT-V	53
Modes of Installing UCT-V	54
Linux UCT-V Installation	54
Windows UCT-V Installation	64
Install UCT-V OVS Agent for OVS Mirroring	70
Uninstall UCT-V	73
Upgrade or Reinstall UCT-V	73
Upgrade UCT-V manually on Virtual Machine	74
Upgrade UCT-V through GigaVUE-FM	74
Pre-Configuration Checklist for OpenStack	77
Install Custom Certificate	77
Upload Custom Certificates using GigaVUE-FM	78
Upload Custom Certificate using Third Party Orchestration	78
Adding Certificate Authority	79
Create Monitoring Domain	79
Managing Monitoring Domain	82
Monitoring Domain	83

Connections Domain	84
Fabric	84
UCT-Vs	85
Configure GigaVUE Fabric Components in GigaVUE-FM	86
Configure UCT-V Controller	88
Configure GigaVUE V Series Proxy	92
Configure GigaVUE V Series Node	93
Configure Role-Based Access for Third Party Orchestration	95
Role	95
User Groups	96
Users	97
Configure GigaVUE Fabric Components in OpenStack	99
Configure V Series Nodes and Proxy in OpenStack	100
Configure UCT-V Controller in OpenStack	102
Configure UCT-V in OpenStack	107
Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack	109
Prerequisite	109
Upgrade UCT-V Controller	109
Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy	111
Configure Secure Tunnel (OpenStack)	113
Precrypted Traffic	113
Mirrored Traffic	114
Prerequisites	114
Notes	114
Configure Secure Tunnel from UCT-V to GigaVUE V Series Node	114
Configure Secure Tunnel between GigaVUE V Series Nodes	116
Viewing Status of Secure Tunnel	119
Create Prefiltering Policy Template	120
Create Precryption Template for UCT-V	121
Rules and Notes:	121
Create Precryption Template for Filtering based on Applications	122
Create Precryption Template for Filtering based on L3-L4 details	122
Configure Monitoring Session	124
Create a Monitoring Session (OpenStack)	124
Monitoring Session Page (OpenStack)	125
Configure Monitoring Session Options (OpenStack)	126
Create Ingress and Egress Tunnels (OpenStack)	130
Create Raw Endpoint (OpenStack)	137
Create a New Map (OpenStack)	138
Example- Create a New Map using Inclusion and Exclusion Maps	142
Map Library	143

Add Applications to Monitoring Session	143
Interface Mapping (OpenStack)	144
Deploy Monitoring Session	145
View Monitoring Session Statistics	145
Visualize the Network Topology	146
Visualize the Network Topology	146
Configure Precryption in UCT-V	147
Rules and Notes	148
Validate Precryption connection	148
Limitations	149
Configuration Health Monitoring	149
Traffic Health Monitoring	150
Supported Resources and Metrics	151
Create Threshold Templates	153
Apply Threshold Template	154
Clear Thresholds	154
View Health Status	155
Analytics for Virtual Resources	156
Virtual Inventory Statistics and Cloud Applications Dashboard	156
Administer GigaVUE Cloud Suite for OpenStack	162
Configure the OpenStack Settings	162
Shutdown or Restart of OVS traffic	164
Manual shutdown or restart of OVS traffic	165
Automatic shutdown or restart of OVS traffic	165
Role Based Access Control	166
About Audit Logs	167
About Events	169
Troubleshooting	172
OpenStack Connection Failed	172
Handshake Alert: unrecognized_name	172
GigaVUE V Series Node or UCT-V Controller is Unreachable	173
Additional Sources of Information	174
Documentation	174
How to Download Software and Release Notes from My Gigamon	176
Documentation Feedback	177
Contact Technical Support	178
Contact Sales	178
Premium Support	179
The VUE Community	179
Glossary	180

GigaVUE Cloud Suite Deployment Guide - OpenStack

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

Refer to the following sections for details:

- [Overview of GigaVUE Cloud Suite for OpenStack](#)
- [Introduction to the Supported Features for OpenStack](#)
- [Licensing GigaVUE Cloud Suite](#)
- [Get Started with GigaVUE Cloud Suite for OpenStack Deployment](#)
- [Deploy GigaVUE Cloud Suite for OpenStack](#)
- [Configure Secure Tunnel \(OpenStack\)](#)
- [Create Prefiltering Policy Template](#)
- [Create Precryption Template for UCT-V](#)
- [Configure Monitoring Session](#)
- [Configure Precryption in UCT-V](#)
- [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:](#)
- [Analytics for Virtual Resources](#)
- [Administer GigaVUE Cloud Suite for OpenStack](#)
- [Troubleshooting](#)

Overview of GigaVUE Cloud Suite for OpenStack

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

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

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

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

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

Refer [Deploying Gigamon CloudSuite on OpenStack to scale-in and Open vSwitch with Hardware offload and scale-out monitoring tools](#) for more detailed information.

GigaVUE-FM

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

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

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

UCT-V

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

Next generation UCT-V is a lightweight solution that acquires traffic from Virtual Machines and in-turn improves the performance of the UCT-V mirroring capability. The solution has a prefiltering capability at the tap level that reduces the traffic flow from the agent to GigaVUE V Series Node and in-turn reduces the load on the GigaVUE V Series Node. Next generation UCT-V gets activated on Windows and also on Linux systems with a Kernel version above 4.18.

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

For more information on installing the UCT-V see [Install UCT-V](#).

UCT-V Controller

UCT-V Controller (earlier known as G-vTAP Controller) manages multiple UCT-Vs and orchestrates the flow of mirrored traffic to GigaVUE V Series Nodes. GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs. A UCT-V Controller can only manage UCT-Vs that has the same version. For example, the UCT-V Controller 6.8.00 can only manage UCT-Vs 6.8.00. If you have the previous version of UCT-V still deployed in the Virtual Network, you must configure both UCT-V Controller 6.8.00 and the previous version. While configuring the UCT-V Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the UCT-Vs to the GigaVUE V Series Nodes.

NOTE: A single UCT-V Controller can manage up to 1000 UCT-Vs.

GigaVUE V Series Node

GigaVUE® V Series Node is a visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to on premise device or tools. GigaVUE Cloud Suite for AWS uses the TLS-PCAPNG, ERSPAN, L2GRE, UDPGRE and, VXLAN tunnels to deliver traffic to tool endpoints.

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

GigaVUE V Series Proxy

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

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

Monitoring Domain

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

For more information on creating a Monitoring Domain, see [Create Monitoring Domain](#).

Monitoring Session

Monitoring sessions are the rules created in GigaVUE-FM to collect inventory data from all target instances in your cloud environment. You can design your monitoring session to include or exclude the instances you want to monitor. You can also choose to monitor egress, ingress, or all traffic.

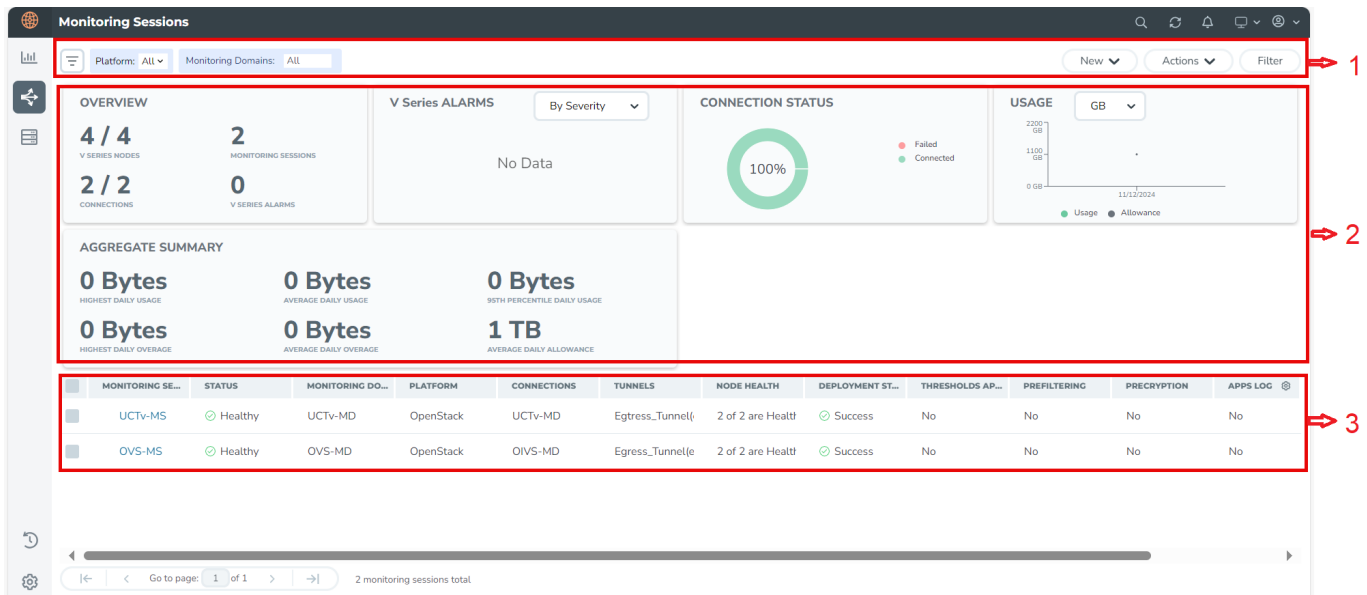
When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance to your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions.

For more information on creating a monitoring session, see [Configure Monitoring Session](#).

Cloud Overview Page (OpenStack)

The overview page 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 <i>Monitor Cloud</i> 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

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.
Precreation	Specifies whether Precreation 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 the Supported Features for OpenStack

GigaVUE Cloud Suite for OpenStack supports the following features:

- [Precreation™](#)
- [Secure Tunnels](#)
- [Prefiltering](#)
- [Load Balancer](#)
- [Analytics for Virtual Resources](#)
- [Traffic Health Monitoring](#)

Precreation™

License: Requires **SecureVUE Plus** license.

Gigamon Precreation™ technology¹ 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.

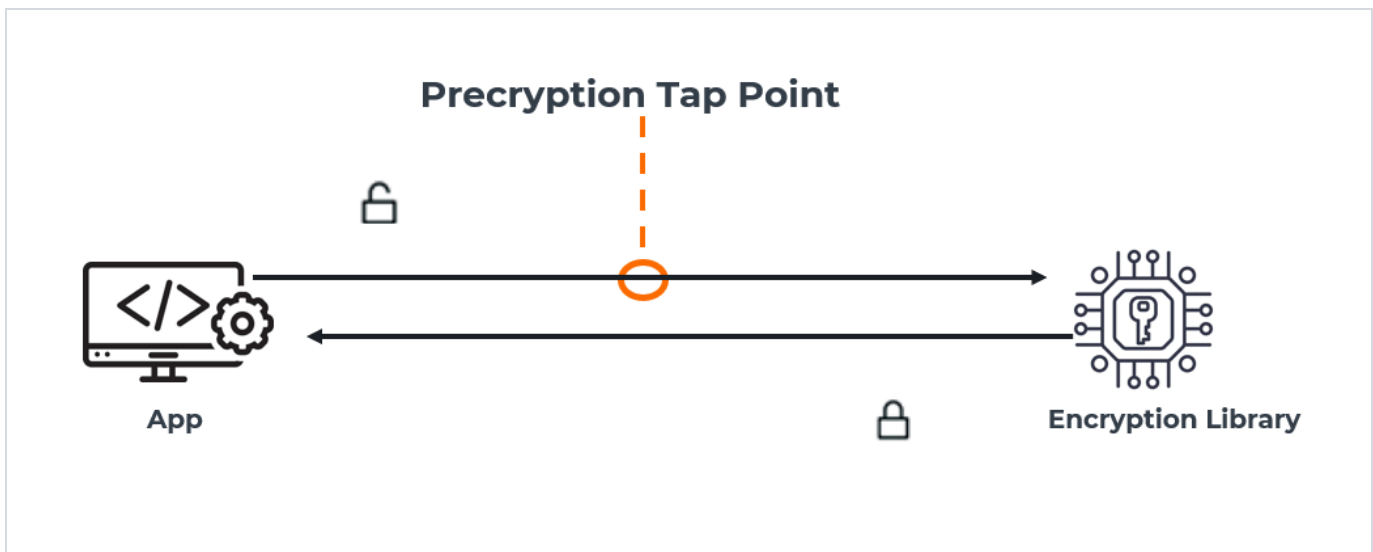
This section explains:

¹ **Disclaimer:** The Precreation 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 Precreation 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.

- [How Gigamon Precryption Technology Works](#)
- [Why Gigamon Precryption](#)
- [Key Features](#)
- [Key Benefits](#)
- [Precryption Technology on Single Node](#)
- [Precryption Technology on Multi-Node](#)
- [Supported Platforms](#)
- [Prerequisites](#)

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.



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. Moreover, UCT with Precryption technology operates independently of the application and does not need to be integrated into the application development lifecycle.

Why Gigamon Precryption

GigaVUE Universal Cloud Tap with Precryption technology is a lightweight, friction-free solution that eliminates blind spots present in modern hybrid cloud infrastructure. It provides comprehensive visibility into East-West and North-South traffic across virtual, cloud, and container platforms. As long as a packet interacts with the Virtual Machine, it is mirrored, ensuring complete traffic capture. This solution delivers unobscured visibility into all encryption types, including TLS 1.3, without the need to manage and maintain decryption keys. With these capabilities, IT organizations can manage compliance, maintain the privacy of communications, establish a robust foundation for Zero Trust, and enhance 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.

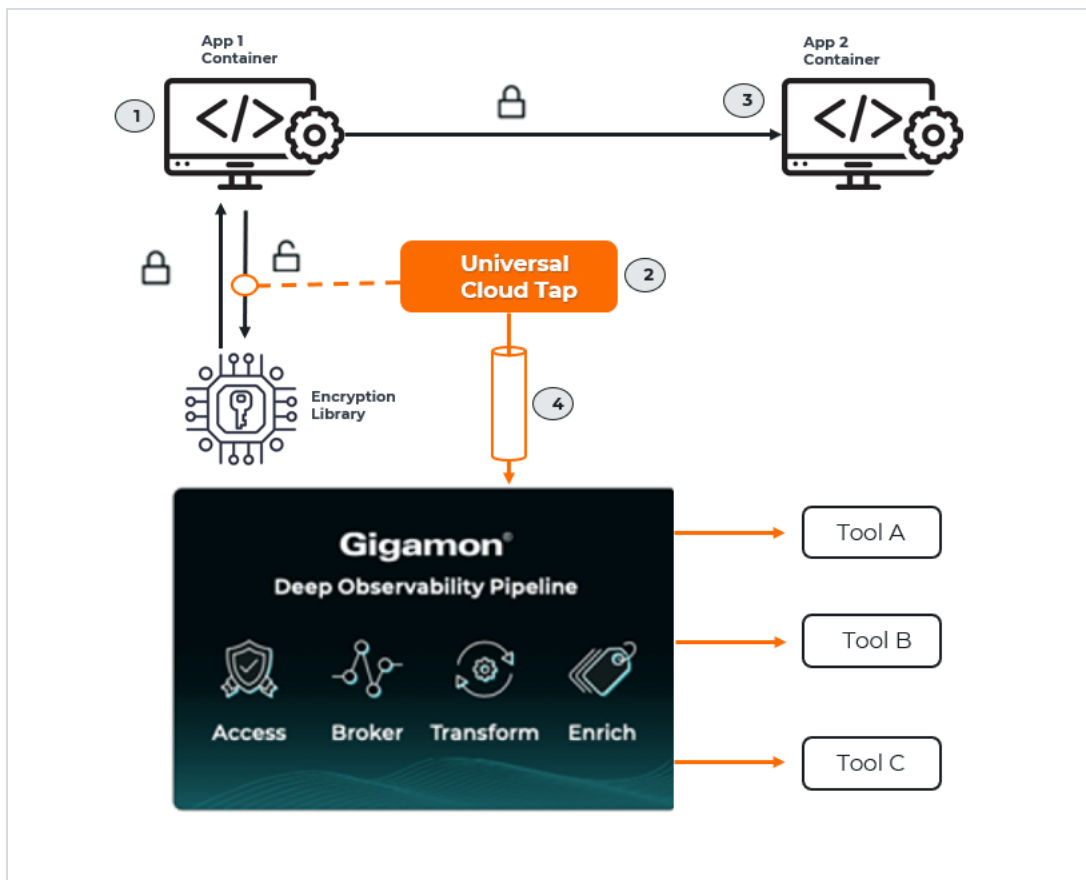
- Maintain privacy and compliance adherence associated with decrypted traffic management.

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](#)

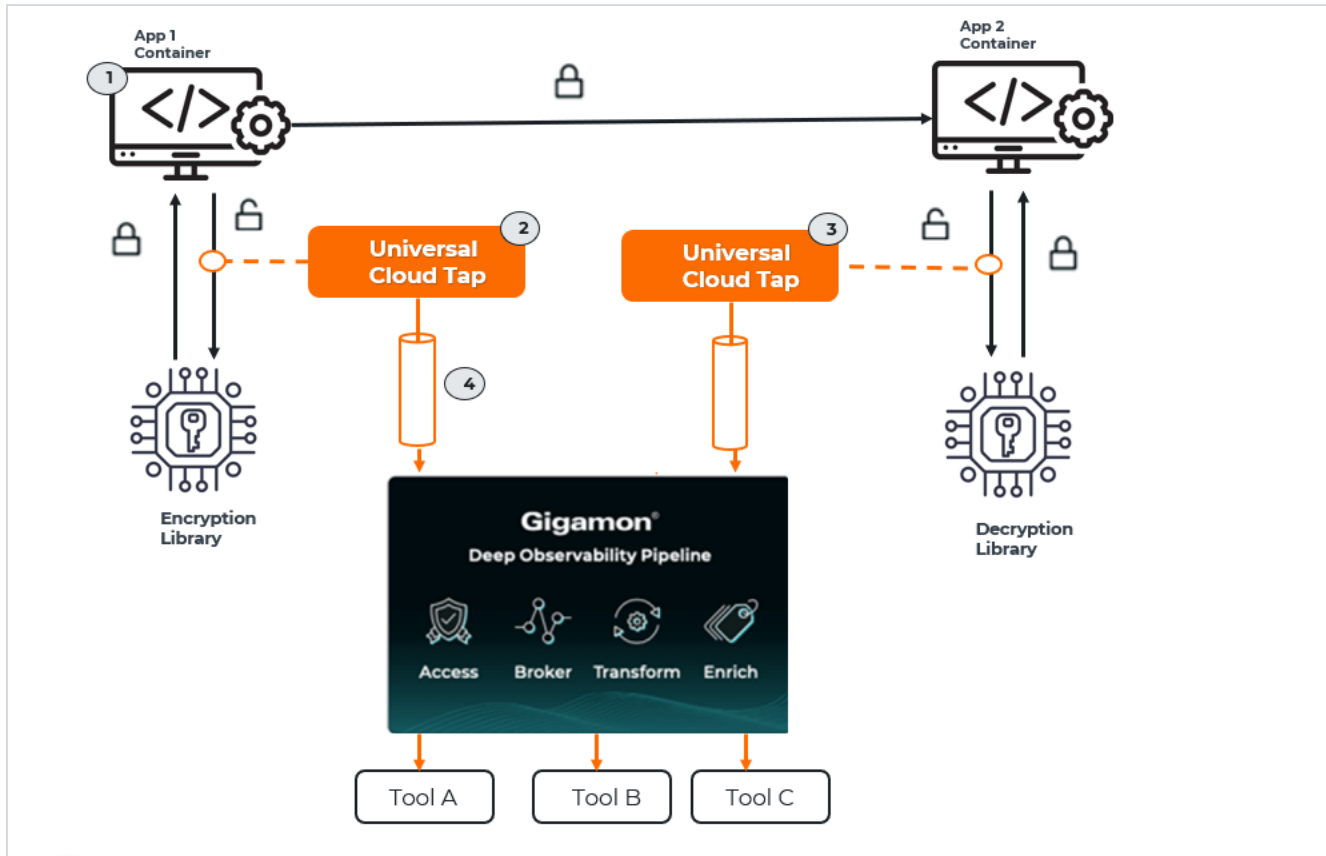
Precryption Technology on Single Node



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.

- 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.

Pre-encryption Technology on Multi-Node



- When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
- GigaVUE Universal Cloud Tap (UCT), enabled with Pre-encryption, gets a copy of this message before it's encrypted on the network.
- Optionally, GigaVUE UCT enabled with Pre-encryption can also acquire a copy of the message from the server end after the decryption.
- 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	<ul style="list-style-type: none"> • AWS • Azure • GCP (via Third Party Orchestration)
Private Cloud	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • EKS • AKS
Private Cloud	<ul style="list-style-type: none"> • 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)
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

Note

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

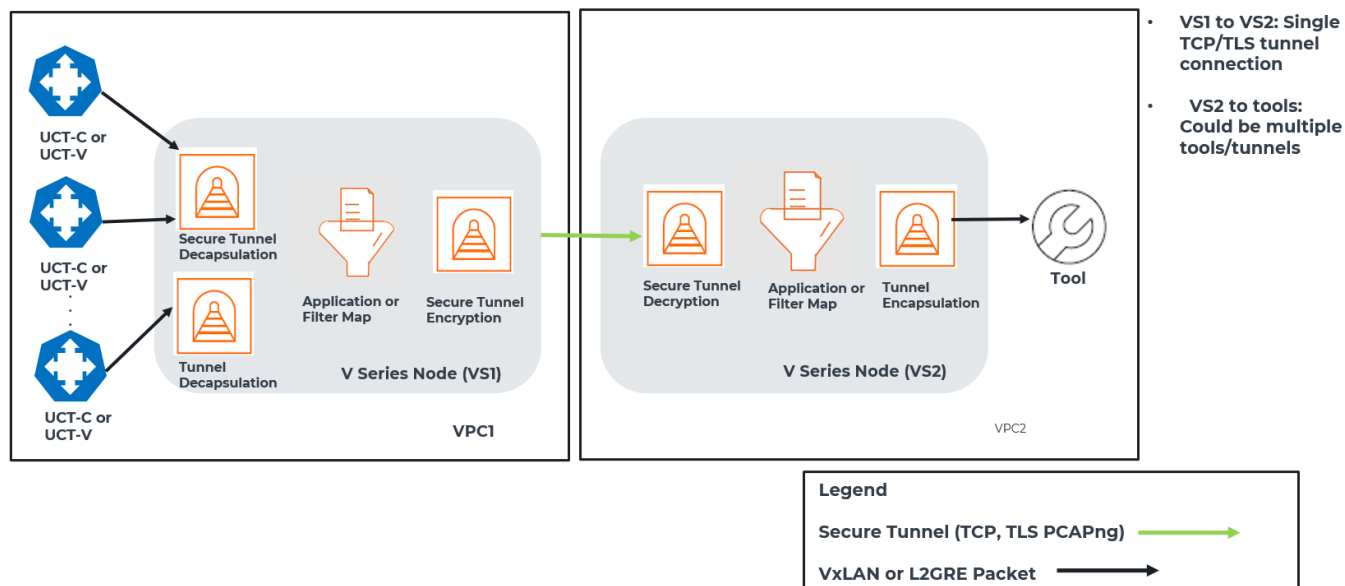
Secure Tunnels

Secure Tunnel 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 one GigaVUE V Series Node 1 is encapsulated using PCAPng format and transported to another GigaVUE V Series Node, where the traffic is decapped. The secure tunnels between two GigaVUE V Series Nodes 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 GigaVUE 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 \(OpenStack\)](#).

Prefiltering

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

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

Each monitoring session can have a maximum of 16 rules.

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

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

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

For more information on configuring a prefilter, refer to [Create Prefiltering Policy Template](#)

Customer Orchestrated Source - Use Case

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

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

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

Licensing GigaVUE Cloud Suite

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

- [Purchase GigaVUE Cloud Suite using CPPO](#)
- [Volume Based License \(VBL\)](#)

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

Default Trial Licenses

After 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.

SKU	BUNDLE	VOLUME	STARTS	ENDS	GRACE PERIOD	ACTIVATION ID	STATUS	TYPE
VBL-1T-BN-SVP-TRIAL	SecureVUEPlus	1024GB daily	10/16/2024	11/15/2024	0 days	4e8cb5a4-7e...	Active	Trial
VBL-2500T-BN-NV	NetVUE	2560000GB d...	10/04/2024	04/02/2025	30 days	62a2ba16-ba...	Active	Internal

This license includes the following applications:

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

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

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

Volume Based License (VBL)

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

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

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

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

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUEPlus

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

Bundle Replacement Policy

Refer to the following notes:

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

Add-on Packages

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

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

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:

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.

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

Get Started with GigaVUE Cloud Suite for OpenStack Deployment

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

- [License Information](#)
- [Before You Begin](#)
- [Install and Upgrade GigaVUE-FM](#)

Before You Begin

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

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

Supported Hypervisor for OpenStack

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

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

Minimum Compute Requirements

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

Compute Instances	vCPU	Memory	Disk Space	Description
UCT-V	2 vCPU	4GB	N/A	Available as rpm or Debian package. Instances can have a single vNIC or dual vNICs configured for monitoring the traffic.
UCT-V Controller	1 vCPU	4GB	8GB	Based on the number of agents being monitored, multiple controllers will be required to scale out horizontally.
GigaVUE V Series Node	2 vCPU	3.75GB	20GB	NIC 1: Monitored Network IP; Can be used as Tunnel IP NIC 2: Tunnel IP (optional) NIC 3: Management IP
GigaVUE V Series Proxy	1 vCPU	4GB	8GB	Based on the number of GigaVUE V Series nodes being monitored, multiple controllers will be required to scale out horizontally.
GigaVUE-FM	4 vCPU	8GB	40GB	GigaVUE-FM must be able to access the controller instance for relaying the commands. Use a flavor with a root disk of minimum 40GB and an ephemeral disk of minimum 41GB.

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

Network Requirements

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

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

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

Virtual Network Interface Cards (vNICs)

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

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

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

Security Group for OpenStack

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

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

NOTE: When using dual stack network, 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	TCP	443	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive registration requests from

used for Third Party Orchestration)				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 Node IP	Allows GigaVUE-FM to receive traffic health updates from GigaVUE V Series Nodes.
Inbound	TCP	5671	UCT-V Controller IP	Allows GigaVUE-FM to receive statistics from UCT-V Controllers.
Inbound	TCP	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	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 (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.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using Third Party Orchestration.
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	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
UCT-V				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9901	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller.
Direction	Protocol	Port	Destination 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.
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.
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 from UCT-V or Customer Orchestrated Source.
Inbound	IP Protocol (L2GRE)	L2GRE	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive L2GRE tunnel traffic from UCT-V or Customer Orchestrated Source.
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 (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	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	<ul style="list-style-type: none"> 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	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.
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 (This is the port	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests

used for Third Party Orchestration)				and heartbeat messages from GigaVUE V Series Node.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using Third Party Orchestration.
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.

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

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

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

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

Key Pairs

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

Prerequisites for OVS Mirroring

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

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

OVS-Mirror Requirements

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

OpenStack Cloud Environment Requirements

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

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

- Here are the APIs and commands required for OVS mirroring

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

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



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



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

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

GigaVUE-FM Version Compatibility

GigaVUE-FM version 6.8.00 supports the latest version (6.8.00) 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.

Default Login Credentials

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

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

Install and Upgrade GigaVUE-FM

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

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

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

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

Deploy GigaVUE Cloud Suite for OpenStack

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

Refer to the following sections for details:

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

Deployment Options for GigaVUE Cloud Suite for OpenStack

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

- [Deploy GigaVUE Fabric Components using OpenStack](#)
- [Deploy GigaVUE Fabric Components using GigaVUE-FM](#)
 - [Traffic Acquisition Method as UCT-V](#)
 - [Traffic Acquisition Method as OVS Mirroring](#)
 - [Traffic Acquisition Method as Tunnel](#)

Deploy GigaVUE Fabric Components using OpenStack

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

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

Deploy GigaVUE Fabric Components using GigaVUE-FM

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

Traffic Acquisition Method as UCT-V

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

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on OpenStack	Install GigaVUE-FM on OpenStack
2	Install UCT-Vs	For Linux: Linux UCT-V Installation For Windows: Windows UCT-V Installation
3	Create a Monitoring Domain	Create Monitoring Domain

Step No	Task	Refer the following topics
	NOTE: Ensure that the 'Use FM to Launch Fabric' toggle button is enabled.	
4	Configure GigaVUE Fabric Components NOTE: Select UCT-V as the Traffic Acquisition Method.	Configure GigaVUE Fabric Components in GigaVUE-FM
5	Create Monitoring session	Create a Monitoring Session (OpenStack)
6	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as OVS Mirroring

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

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on OpenStack	Install GigaVUE-FM on OpenStack
2	Install UCT-V OVS Agents	Install UCT-V OVS Agent for OVS Mirroring
3	Create a Monitoring Domain NOTE: Ensure that the 'Use FM to Launch Fabric' toggle button is enabled.	Create Monitoring Domain
4	Configure GigaVUE Fabric Components NOTE: Select OVS Mirroring as the Traffic Acquisition Method.	Configure GigaVUE Fabric Components in GigaVUE-FM
5	Create Monitoring session	Create a Monitoring Session (OpenStack)
6	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as Tunnel

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

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

Upload Fabric Images

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

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

```
$ source admin_openrc.sh
```

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

```
GigaVUE-FM - glance image-create --disk-format qcow2 --visibility public --container-format bare --progress --name fm-6.9-uefiSec-boot --file gfm-6.9.qcow2
```

```
GigaVUE-FM with UEFI Boot - glance image-create --disk-format qcow2 --visibility public --container-format bare --property hw_firmware_type=uefi --progress --name fm-6.9-uefiSec-boot --file gfm-6.9.qcow2
```


GigaVUE-FM with UEFI secure Boot - **glance image-create --disk-format qcow2 --visibility public --container-format bare --property hw_firmware_type=uefi --property os_secure_boot=required --progress --name fm-6.9-uefiSec-boot --file gfm-6.9.qcow2**

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

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

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

UCT-V OVS Controller - **glance image-create --disk-format qcow2 --visibility public --container-format bare --progress --name gigamon-gigavue-uctv-ovs-cntlr-6.9 --file gigamon-gigavue-uctv-ovs-cntlr-6.9.qcow2**

UCT-V Controller - **glance image-create --disk-format qcow2 --visibility public --container-format bare --progress --name gigamon-gigavue-uctv-cntlr-6.9 --file gigamon-gigavue-uctv-cntlr-6.9.qcow2**

GigaVUE V Series Node - **glance image-create --disk-format qcow2 --visibility public --container-format bare --progress --name gigamon-gigavue-vseries-node-6.9 --file gigamon-gigavue-vseries-node-6.9.qcow2**

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

- gigamon-gigavue-vseries-node-6.9
- gigamon-gigavue-vseries-proxy-6.9
- gigamon-gigavue-uctv-cntlr-6.9
- gigamon-gigavue-uctv-ovs-cntlr-6.9

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

Install GigaVUE-FM on OpenStack

To launch the GigaVUE-FM instance inside the cloud:

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

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

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

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

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

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

Initial GigaVUE-FM Configuration

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

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.9.1.el7.x86_64 on an x86_64

123 login:

CentOS Linux 7 (Core)
Kernel 3.10.0-1062.9.1.el7.x86_64 on an x86_64

123 login: admin
Password:
You are required to change your password immediately (root enforced)
Changing password for admin.
(current) UNIX password:
New password:
Retype new password:
[admin@123 ~]$_
```

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

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

Install UCT-V

UCT-V is the primary Gigamon monitoring module that 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 consist of multiple source interfaces 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](#)
- [Install UCT-V OVS Agent for OVS Mirroring](#)

Supported Operating Systems for UCT-V

Supported Operating System for UCT-V¹ is 6.5.00, 6.6.00, 6.7.00, 6.8.00, 6.9.00

The following table lists the supported versions of the Operating Systems for UCT-V.

Operating System	Supported Versions
Ubuntu/Debian	Versions 16.04 through 24.04
CentOS	Versions 7.5 through 9.0

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

Operating System	Supported Versions
RHEL	Versions 7.5 through 9.4
Windows Server	Versions 2012 through 2022
Rocky OS	Versions 8.4 through 8.8

GigaVUE-FM version 6.9 supports UCT-V version 6.9 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 details.

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	9901	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=9901/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. 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.

By default, most modern Linux operating systems come pre-installed with all the necessary packages for the UCT-V to function without additional configuration.

Before installing UCT-V, you can provide your own configuration file (uctv.conf) /etc/gigamon-cloud.conf in the tmp directory.

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 **6.8.00** 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_6.8.00_amd64.deb
$ sudo dpkg -i gigamon-gigavue_uctv_6.8.00_amd64.deb
```

2. To install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS:

- a. Download the UCT-V **6.8.00** 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_6.8.00_x86_64.rpm
$ sudo rpm -i gigamon-gigavue_uctv_6.8.00_x86_64.rpm
```

- 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	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

- 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.
- 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.
- 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-V6.8.00 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_6.8.00_amd64.deb
$ sudo dpkg -i gigamon-gigavue_uctv_6.8.00_amd64.deb
```

- 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 `eth1`; 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.

- Save the file.
- 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-V6.8.00 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_6.8.00_x86_64.rpm
$ sudo rpm -i gigamon-gigavue_uctv_6.8.00_x86_64.rpm
```

- 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.

- Save the file.
- 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
```

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

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.

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	9901	TCP	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller
Outbound	8891	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](#)



The Windows UCT-V MSI is a self-contained package that includes all necessary dependencies. However, during setup, it will automatically install the following components:

- **Visual C++ Redistributable 2019 (x86)**
- **Npcap (v1.55 OEM)**

Before installing the Windows Agent, ensure that Npcap is not already present on the system. If an existing version of Npcap is found, it must be manually uninstalled to avoid conflicts and ensure compatibility with the version bundled in the UCT-V.

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 **6.8.00** 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.

uctv-wizard

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

Options	Use Command	Description
pre-check	uctv-wizard pre-check	<p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: It is recommended that the send buffer size of network adapters be increased to 128 MB during the installation to optimize performance and minimize traffic disruption.</p> </div>
adapter-setup	uctv-wizard adapter-setup	<p>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.</p> <p>You can choose between the following:</p> <ul style="list-style-type: none"> • 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	uctv-wizard adapter-restore	<p>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.</p> <p>You can choose between the following:</p> <ul style="list-style-type: none"> • If you wish to skip the prompts for restoring the buffer size of the compatible network adapters, enter the option as y. • Enter N if you wish to restore it manually. Refer to the Install

Options	Use Command	Description
		Windows UCT-Vs using Manual Configuration section for more details.
configure	uctv-wizard configure	<p>First, it checks for any existing configured file in the tmp directory. If available, UCT-V will use that configuration.</p> <p>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).</p> <p>You can add the required policy for the available port if a firewall is installed.</p> <ul style="list-style-type: none"> 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	uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

**Notes:**

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

Windows UCT-V Installation Scenarios

- 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.
- 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 **6.8.00** 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.

- 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::/64 mirror-dst
```

- Save the file.

- 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.

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

Install UCT-V OVS Agent for OVS Mirroring

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

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

You can install the UCT-V OVS agents either from Debian or RPM packages as follows:

- [Install the UCT-V OVS Agent from Ubuntu/Debian Package](#)
- [Install the UCT-V OVS Agent from RPM package](#)

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

To install from a Debian package:

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

```
$ ls gigamon-gigavue-uctv-ovs-agent_6.8.00_amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-ovs-agent_6.8.00_amd64.deb
```

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

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

```
br-int mirror-dst
```

```
# Changes for OVS Mirroring
```

```
# This Value will be used as local Ip in OVS Mirror Config
```

```
tunnel-src 172.20.20.11
```

```
# This Value will be used as Next Hop for Tunneled Packets
```

```
tunnel-gw 172.20.20.1
```

```
This Value will be used as local Ipv6 in OVS Mirror Config
```

```
tunnel-src-v6 2001::161
```

```
This Value will be used as Next Hop ipv6 addr for Tunneled Packets
```

```
tunnel-gw-v6 2001::1
```

```
# OVS Agent Mode, Values: auto|standard|dpdk|hw-offload
```

```
ovs-agent-mode auto
```

```
# VLAN Tag value (valid: 0-4094)
```

```
ovs-vlan-tag 2020
```

```
# Egress Interface for OVS Mirrored Traffic
```

```
ovs-egress-if vlan2020
```

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

```
$ sudo service uctv start
```

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

```
$ sudo service uctv status
```

```
UCT-V is running
```

Install the UCT-V OVS Agent from RPM package

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

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


```
$ ls gigamon-gigavue-uctv-ovs-agent_6.8.00_x86_64.rpm
$ sudo rpm -ivh gigamon-gigavue-uctv-ovs-agent_6.8.00_x86_64.rpm
```
3. Once the OVS agent package is installed, modify the file **/etc/uctv/uctv.conf** to configure and grant permission to monitor ingress and egress traffic and transmit the mirrored packets.

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

```
# br-int mirror-dst

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

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

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




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



To upgrade UCT-V OVS agent:

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

Uninstall UCT-V

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

- 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.

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

Pre-Configuration Checklist for OpenStack

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

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

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

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

	Required Information
<input type="checkbox"/>	Authentication URL
<input type="checkbox"/>	Project Name
<input type="checkbox"/>	Floating IP
<input type="checkbox"/>	Region name for the Project
<input type="checkbox"/>	Domain
<input type="checkbox"/>	SSH Key Pair
<input type="checkbox"/>	Networks
<input type="checkbox"/>	Security groups

Install Custom Certificate

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

You can upload the custom certificate in two ways:

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

Upload Custom Certificates using GigaVUE-FM

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

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

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

4. Click **Save**.

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

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

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

Upload Custom Certificate using Third Party Orchestration

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

For integrated mode:

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

For generic mode:

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

Adding Certificate Authority

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

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

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

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

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

4. Click **Save**.

Create Monitoring Domain

To create a monitoring domain in GigaVUE-FM:

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

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

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

Field	Description
Monitoring Domain	<p>A name for the monitoring domain.</p> <p>NOTE: You can only view and delete the existing configuration for V Series node 1. You cannot create and perform any other actions on the existing configuration for GigaVUE V Series node 1 as the features are deprecated from GigaVUE-FM fabric manager.</p>
Alias	An alias used to identify the monitoring domain.
URL	<p>The authentication URL is the Keystone URL of the OpenStack cloud. This IP address must be DNS resolvable.</p> <p>Refer to the OpenStack User Manual for more information on retrieving the authentication URL from the OpenStack.</p> <p>NOTE: To ensure the validity of OpenStack certificates issued by a trusted Certificate Authority (CA), you must enable the Trust Store. Refer to the Trust Store section in GigaVUE Administration Guide for more detailed information.</p>
User Domain Name	<p>The domain name of your OpenStack authentication domain.</p> <ul style="list-style-type: none"> • If you are using a separate domain for AUTH, enter that domain name as User Domain Name. • If you are not using a separate domain, you can use the same domain for User and Project Domain Name.
Project Domain Name	The domain name of your OpenStack project.
Project Name	The name of the project used for OpenStack authentication.
Region	<p>The region where the Project resides. You can find your region by running one of these commands, depending on your OpenStack version.</p> <p>keystone endpoint-list or openstack endpoint list or looking at the RC file in OpenStack to view your credentials.</p>
Username	<p>The username used to connect to your OpenStack cloud.</p> <p>NOTE: If you are using OVS mirroring, you must belong to a role that meets the OpenStack minimum requirements for OVS Mirroring. Refer to OVS Mirroring Prerequisites for more information.</p>
Password	The password of your OpenStack cloud.
Traffic	Select the type of agent used to capture traffic for monitoring:

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

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


NOTE: If GigaVUE-FM fails to connect to OpenStack, an error message is displayed specifying the cause of failure. The connection status is also displayed in Audit Logs, refer to [About Audit Logs](#) for more information.


Managing Monitoring Domain

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

- [Monitoring Domain](#)
- [Connections Domain](#)
- [Fabric](#)
- [UCT-Vs](#)

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

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

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

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

Monitoring Domain

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

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

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

Use the following buttons to manage your Monitoring Domain:

Button	Description
New	Use to create new connection
Actions	<p>You can select a Monitoring Domain and then perform the following options:</p> <ul style="list-style-type: none"> • Edit Monitoring Domain- Select a Monitoring Domain and then click Edit Monitoring Domain to update the configuration. • Delete Domain - You can select a monitoring domain or multiple monitoring domains to delete them. • Deploy Fabric - -You can select a monitoring domain to deploy a fabric, you cannot choose multiple monitoring domains at the same time to deploy fabrics. This option is only enabled when there is No FABRIC (launch configuration) for that specific monitoring domain and GigaVUE-FM orchestration is enabled.. You must create a fabric in the monitoring domain, if the option is disabled • Upgrade Fabric-You can select a monitoring domain or multiple monitoring

Button	Description
	<p>domains to upgrade the fabric. You can upgrade the V Series nodes using this option.</p> <ul style="list-style-type: none"> • Delete Fabric- You can delete all the fabrics associated with the monitoring domain of the selected Fabric. • Edit SSL Configuration - You can use this option to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Filter	<p>Filters the Monitoring Domain based on the list view options that are configured:</p> <ul style="list-style-type: none"> • Tunnel MTU • Acquisition Method • Centralised Connection • Management Subnet <p>You can view the filters applied on the top of the Monitoring Domain page as a button. You can remove the filters by closing the button.</p>

Connections Domain

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

The list view shows the following details:

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

Fabric

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

The list view shows the following details:

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

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

- **Edit Fabric** - You can select one fabric or multiple fabrics of the same Monitoring Domain to edit a fabric. You cannot choose different fabrics of multiple Monitoring Domains at the same time and edit their fabric components.
- **Delete Fabric** - You can delete all the fabrics associated with the Monitoring Domain of the selected fabric.
- **Upgrade Fabric** - You can select a Monitoring Domain or multiple Monitoring Domains to upgrade the fabric. You can upgrade the GigaVUE V Series Nodes using this option.
- **Restart OVS Traffic** - You can restart the OVS traffic. You can view the **Restart OVS Traffic** option only when you enable the check box **OVS Agent Traffic when V Series unreachable** in **Advanced Settings**. For more information on settings, refer to [Configure the OpenStack Settings](#).
- **Shut Down OVS Traffic** - You can shut down the OVS traffic. You can view the **Shut down OVS Traffic** option only when you enable the check box **OVS Agent Traffic when V Series unreachable** in **Advanced Settings**. For more information on settings, refer to [Configure the OpenStack Settings](#).

UCT-Vs

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

The list view shows the following details:

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

Refer to [Configure the OpenStack Settings](#), for information regarding **Settings**.

Configure GigaVUE Fabric Components in GigaVUE-FM

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

- [Configure UCT-V Controller](#)
- [Configure GigaVUE V Series Proxy](#)
- [Configure GigaVUE V Series Node](#)

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

Fields	Description
SSH Key Pair	The SSH key pair for the UCT-V Controller. For more information about SSH key pair, refer to Key Pairs .
Availability Zone	The distinct locations (zones) of the OpenStack region.
Security Groups	The security group created for the UCT-V Controller. For more information, refer to Security Group for OpenStack .
Prefer IPv6	Enables IPv6 to deploy all the Fabric Controllers, and the tunnel between hypervisor to GigaVUE V Series Nodes using IPv6 address. If the IPv6 address is unavailable, it uses an IPv4 address. NOTE: This option can be enabled only when deploying a new GigaVUE V Series Node. If you wish to enable this option after deploying the GigaVUE V Series Node, then you must delete the existing GigaVUE V Series Node and deploy it again with this option enabled.
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs. NOTE: If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate .

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

SSH Key Pair

Select SSH Key Pair...

Availability Zone

Select Availability Zone...

Security Groups

Select management subnet security group...

Configure a V Series Proxy

No

Configure UCT-V Controller

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

UCT-V Controller

Controller Version(s)	<input type="button" value="Add"/>
	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Image <input type="text" value="Select image..."/></p> <p>Flavor <input type="text" value="Select flavor..."/></p> <p>Number of Instances <input type="text" value="1"/></p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Image <input type="text" value="gigamon-gigavue-uctv-cntrl-6.4.00-392759"/></p> <p>Flavor <input type="text" value="m1.small"/></p> <p>Number of Instances <input type="text" value="1"/></p> </div>
Management Network	<p>IP Address Type <input type="radio"/> Private <input checked="" type="radio"/> Floating</p> <p>Network <input type="text" value="mgmt"/></p> <p>Floating IPs <input type="text" value="10.210.19.1"/></p> <p>Port <input type="text" value="Select Port"/></p>
Additional Network(s)	<input type="button" value="Add"/>
Tags	<input type="button" value="Add"/>
Cloud-Init User Data (Optional)	<input type="text" value="Enter cloud-init user data in YAML cloud-config format"/>
Agent Tunnel Type	<input type="text" value="VXLAN"/>
Agent Tunnel CA	<input type="text" value="Select CA"/>
UCT-V Controller Name	<input type="checkbox"/> Configuration Drive <input type="text" value="Gigamon-UCT-VController-"/> + <input type="text" value="1"/> <input type="text" value="Gigamon-UCT-VController-1"/>

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

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

Table Section Outside Table:

Table Row Outside Table:

Table Cell Outside Table:

Fields

Table Cell Outside Table:

Description

Table Row Outside Table:

Table Cell Outside Table:

Controller Version(s)

Table Cell Outside Table:

The UCT-V Controller version that you configure must always have the same version number as the UCT-Vs deployed in the instances. For more detailed information refer GigaVUE-FM Version Compatibility Matrix.

NOTE: Note: If there is a version mismatch between the UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the agents in the instances.

To add UCT-V Controllers:

- a. Under **Controller Versions**, click **Add**.
- b. From the **Image** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.
- c. From the **Flavor** drop-down list, select a size for the UCT-V Controller.
- d. In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.

Table Row Outside Table:

Table Cell Outside Table:
Management Network

Table Cell Outside Table:

This segment defines the management network that GigaVUE-FM uses to communicate with UCT-V Controllers, GigaVUE V Series Proxy, and GigaVUE V Series Nodes.

Network - Select the management network ID.

Ports - Select a port, you can choose a port related to the selected management network ID.

IP Address Type

The type of IP address GigaVUE-FM needs to communicate with UCT-V Controllers:

- o **Private**—A private IP can be used when GigaVUE-FM, the UCT-V Controller, or the GigaVUE V Series Proxy reside inside the same project.
- o **Floating**—A floating IP is needed only if GigaVUE-FM is not in the same project in the cloud or is outside the cloud. GigaVUE-FM needs a floating IP to communicate with the controllers from an external network.

Table Row Outside Table:

Table Cell Outside Table:
Additional Network(s)

Table Cell Outside Table:

(Optional) If there are UCT-Vs on networks that are not IP routable from the management network, additional networks or subnets must be specified so that the UCT-V Controller can communicate with all the UCT-Vs.

Click **Add** to specify additional networks (subnets), if needed. Also, make sure that you specify a list of security groups for each additional network.

Ports: Select a port associated with the network.

Table Row Outside Table:

Table Cell Outside Table:
Tag(s)

Table Cell Outside Table:

(Optional) The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-uctv-controllers. There is a specific UCT-V Controller Version for OVS Mirroring and OVS Mirroring + DPDK.

To add a tag:

- a. Click **Add**.
- b. In the **Key** field, enter the key. For example, enter Name.
- c. In the **Value** field, enter the key value. For example, us-west-2-uctv-controllers.

Table Row Outside Table:

Table Cell Outside Table: Cloud-Init User Data (Optional)

Table Cell Outside Table: Enter the cloud-init user data in cloud-config format.

Table Row Outside Table:

Table Cell Outside Table:
Agent Tunnel Type

Table Cell Outside Table:

The type of tunnel used for sending the traffic from UCT-Vs to GigaVUE V Series nodes. The options are GRE, VXLAN, and Secure tunnels (TLS-PCAPNG).

Table Row Outside Table:

Table Cell Outside Table:
Agent Tunnel CA

Table Cell Outside Table:

The Certificate Authority (CA) that should be used in the UCT-V Controller for connecting the tunnel.

Table Row Outside Table:

Table Cell Outside Table:
UCT-V Controller Name

Table Cell Outside Table:

(Optional) Enter the name of the UCT-V Controller.

The UCT-V Controller name must meet the following criteria:

- o The entire name can be a minimum of 1 to a maximum of 128 characters.
- o The suffix must only be a numeral and it should range between 0 to 999999999.

- o When deploying multiple UCT-V Controllers, the suffix of the consecutive UCT-V Controller name is updated successively. E.g., 000, 001, 002, 003, etc..

Configure GigaVUE V Series Proxy

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

Configure GigaVUE V Series Node

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

Prerequisites

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

Parameter	Description
Image	Select the GigaVUE V Series node image file.
Flavor	Select the form of the GigaVUE V Series node.
Management Network	<p>For the GigaVUE V Series Node, the Management Network is what is used by the GigaVUE V Series Proxy to communicate with the GigaVUE V Series Nodes. Select the management network ID.</p> <p>Ports— Select a port, you can choose a port related to the selected management network ID.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: When both IPv4 and IPv6 addresses are available, IPv6 address is preferred, however if IPv6 address is not reachable then IPv4 address is used.</p> </div>
Data Network	<p>Click Add to add additional networks. This is the network that the GigaVUE V Series node uses to communicate with the monitoring tools. Multiple networks are supported.</p> <ul style="list-style-type: none"> • Tool Subnet—Select a tool subnet, this is the default subnet that the GigaVUE-FM use to egress traffic to your tools. This subnet must have proper connectivity to your endpoint. • IP Address Type <ul style="list-style-type: none"> ◦ Private—A private IP can be used when GigaVUE-FM, the UCT-V Controller, or the GigaVUE V Series Proxy, or the GigaVUE V Series node 2 reside inside the same project. ◦ Floating—A floating IP address specified here will be where V Series node 2x.x can be directly managed by GigaVUE-FM or can optionally managed by controllers. • Network 1—Select a network type. • Ports —Select a port associated with the network. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <ul style="list-style-type: none"> • For OVS Mirroring or OVS Mirroring + DPDK deployments, must select Floating in the Data Network section and then specify the IPs in the Floating IPs field. You can have multiple Floating IPs. • A network provider that is able to receive the monitored traffic may also be used here for OVS Mirroring and OVS Mirroring + DPDK. In this case, you would not need to provide a floating IP; but could select "private" and choose the provider network. </div>

Parameter	Description
Tag(s)	<p>(Optional) The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-uctv-controllers.</p> <p>To add a tag:</p> <ol style="list-style-type: none"> Click Add. In the Key field, enter the key. For example, enter Name. In the Value field, enter the key value. For example, us-west-2-uctv-controllers.
Cloud-Init User Data (Optional)	Enter the cloud-init user data in cloud-config format.
Min Instances	<p>The minimum number of GigaVUE V Series nodes to be launched in OpenStack. The minimum number can be 1.</p> <ul style="list-style-type: none"> When you deploy an OVS Mirroring or OVS Mirroring + DPDK monitoring session, the V Series nodes will automatically be deployed based on the # of hypervisors being monitored. When you deploy a UCT-V based monitoring session, the V Series nodes will automatically be deployed based on the # of VMs being monitored and the instance per V Series node ratio defined in the OpenStack Settings page. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.</p> </div>
Max Instances	The maximum number of GigaVUE V Series nodes that can be launched in OpenStack.
V Series Node Name	<p>(Optional) Enter the name of the V Series Node.</p> <p>The V Series Node name must meet the following criteria:</p> <ul style="list-style-type: none"> The entire name can be a minimum of 1 to a maximum of 128 characters. The suffix must only be a numeral and it should range between 0 to 999999999. When deploying multiple V Series Nodes, the suffix of the consecutive V Series Node name is updated successively. E.g., 000, 001, 002, 003, etc..
Tunnel MTU (Maximum Transmission Unit)	<p>The Maximum Transmission Unit (MTU) is applied on the outgoing tunnel endpoints of the GigaVUE-FM V Series node when a monitoring session is deployed. The default value is 1450. The value must be 42 bytes less than the default MTU for GRE tunneling, or 50 bytes less than default MTU for VXLAN tunnels.</p>

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

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

Configure Role-Based Access for Third Party Orchestration

Before deploying the fabric components using a third party orchestrator, we must create users, roles and the respective user groups in GigaVUE-FM. The Username and the Password provided in the User Management page will be used in the registration data that can be used to deploy the fabric components in your orchestrator.

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

- [Role](#)
- [User Groups](#)
- [Users](#)

Role

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




NOTE:

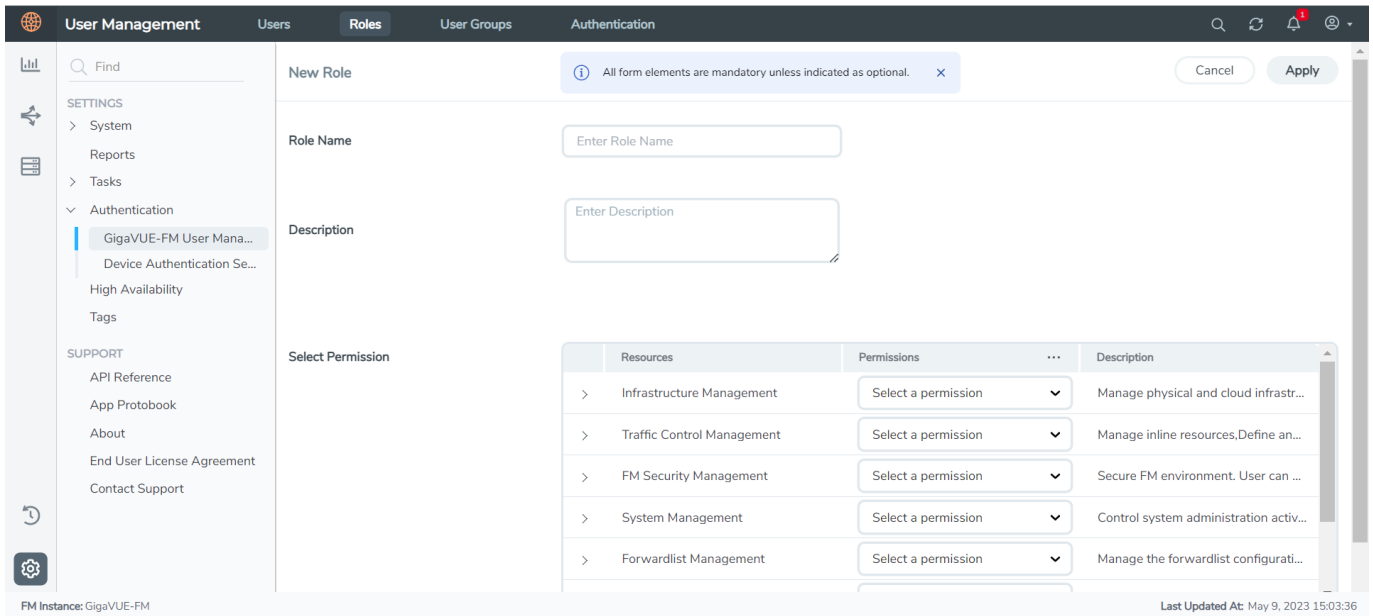
- If you are a user with read-only access you will be restricted from performing any configurations on the screen. The menus and action buttons in the UI pages will be disabled appropriately.
- If you are using the default roles available in GigaVUE-FM, you must have the **fm_super_admin** role for deploying fabric components using Third Party Orchestration.

Create Custom Roles for Third Party Orchestration

This section describes the steps for creating custom roles for Third Party Orchestration.

To create a role

1. On the left navigation pane, click  and select **Authentication > GigaVUE-FM User Management > Roles**.
2. Click **New Role**.




3. In the New Role page, select or enter the following details:
 - **Role Name:** Name of the role.
 - **Description:** Description of the role.
 - **Select Permission:** Under the **Select Permissions** tab select **Third Party Orchestration** and provide write permissions.
4. Click **Apply** to save the configuration.

User Groups

A user group consists of a set of roles and set of tags associated with users in that group. When a user is created they can be associated with one or more groups.

Create User Groups in GigaVUE-FM for Third Party Orchestration

Create a new User Group as mentioned in the steps below:

1. On the left navigation pane, click , and then select **Authentication > GigaVUE-FM User Management > User Groups**.
2. Click **New Group**. In the Wizard that appears, perform the following steps. Click **Next** to progress forward and click **Back** to navigate backward and change the details.

The screenshot shows the 'New User Group' configuration wizard in the 'Assign Roles' step. The wizard progress is indicated by a sequence of four steps: 1. Group Info, 2. Assign Roles (current), 3. Assign Tags, and 4. Assign Users. The 'Roles' table is displayed with the following data:

Roles	Description	Resources
fm_super_admin	Allows a user to do everything in GigaVUE-FM, including add...	All
fm_admin	Allows a user to do everything in GigaVUE-FM except adding...	Infrastructure Management+ 6 more
fm_user	Allows a user to view everything in GigaVUE-FM, including A...	All

The 'fm_admin' role is selected, and its resources are listed as 'Infrastructure Management+ 6 more'. The interface also includes a sidebar with navigation options and a footer indicating '3 roles total'.

- In the **Group Info** tab, enter the following details:
 - Group Name**
 - Description**
- In the **Assign Roles** tab, select the role that you want to assign to the user group.
- In the **Assign Tags** tab, select the required tag key and tag value.
- In the **Assign Users** tab, select the required users. Click **Apply** to save the configuration. Click **Skip and Apply** to skip this step and proceed without adding users.

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

Click on the ellipses to perform the following operations:

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


Users

You can also configure user's role and user groups to control the access privileges of the user in GigaVUE-FM.

Add Users

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

To add users perform the following steps:

1. On the left navigation pane, click  and select **Authentication > GigaVUE-FM User Management > Users**. The **User** page is displayed.

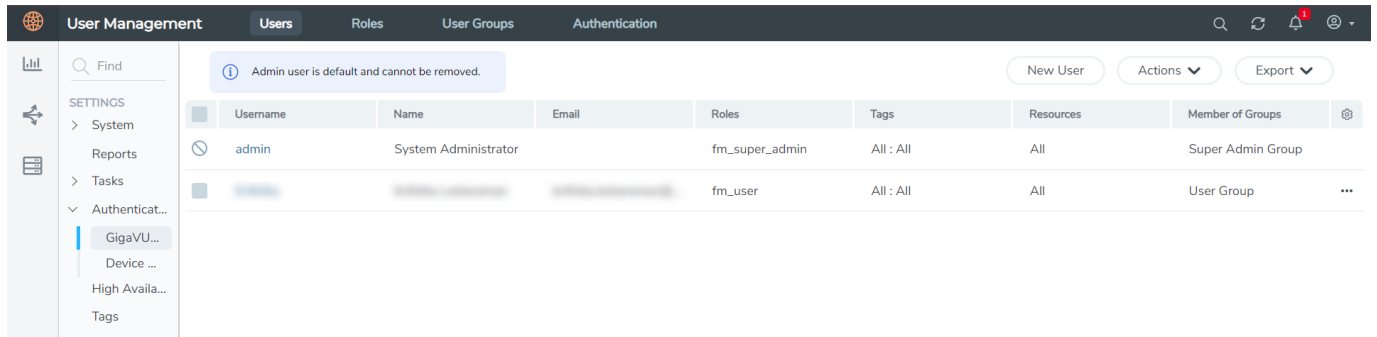


Figure 1 FM Users Page

2. Click **New User**. In the Add User wizard that appears perform the following steps.

Add User

All form elements are required unless indicated as optional. x

Name

Username

Password

Confirm password

Email

User Group

Select User Group

Your new password must contain:

- ✓ At least 8 characters and up to a maximum of 64 characters in length
- ✓ At least one numerical character
- ✓ At least one uppercase character
- ✓ At least one lowercase character
- ✓ At least one special character from -!@#%&*()+

Cancel Ok

Figure 2 Create User

- a. In the Add User pop-up box, enter the following details:
 - o **Name:** Actual name of the user
 - o **Username:** User name configured in GigaVUE-FM
 - o **Email:** Email ID of the user
 - o **Password/Confirm Password:** Password for the user.
 - o **User Group:** Select the User Group that you want to associate the user with.

NOTE: GigaVUE-FM will prompt for your password.

- b. Click **OK** to save the configuration.

The new user is added to the summary list view.

The username and password created in this section will be used in the registration data, used for deploying the fabric components.

Configure GigaVUE Fabric Components in OpenStack

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

Recommended Instance Type

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

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

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

- In the above mentioned case, the Traffic Acquisition Tunnel MTU is set to the default value 1500. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** and click Save.
- When you deploy the fabric components using 3rd party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- You can use OpenStack Orchestrator for GigaVUE Visibility Node configuration only using V Series 2 nodes.

- 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.

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

- [Configure V Series Nodes and Proxy in OpenStack](#)
- [Configure UCT-V Controller in OpenStack](#)
- [Configure UCT-V in OpenStack](#)

Configure V Series Nodes and Proxy in OpenStack

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

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

Register V Series Nodes or V Series Proxy using OpenStack GUI

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

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

The screenshot shows the OpenStack dashboard interface. The main content area is titled "Instances" and displays a table with the following data:

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
vSeries-node	gigamon-gigavue-vseries-node-2.3.2-281462_amd64.qcow2	traffics-test-network-1 10.42.2.101 mgmts-test-network 10.42.1.8	vseries2-4x8-flavor	vm_automation_test	Active	nova	None	Running	3 days	Create Snapshot

- 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.

Field	User Data
User data without custom certificate	<pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <Connection Name> user: <Username> password: <Password> remoteIP: <IP address of the GigaVUE-FM> or <IP address of the Proxy> remotePort: 443</pre>
User data with custom certificate	<pre>#cloud-config write_files: - path: /etc/cntlr-cert.conf owner: root:root permissions: "0644" content: -----BEGIN CERTIFICATE----- <certificate content> -----END CERTIFICATE----- - path: /etc/cntlr-key.conf owner: root:root permissions: "400" content: -----BEGIN PRIVATE KEY----- <private key content> -----END PRIVATE KEY----- - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <Connection Name> user: <Username> password: <Password> remoteIP: <IP address of the GigaVUE-FM> or <IP address of the Proxy> remotePort: 443</pre>



- You can register your V Series node directly with GigaVUE-FM or you can use V Series proxy to register your V Series node with GigaVUE-FM. If you wish to register V Series node directly, enter the `remotePort` value as 443 or if you wish to deploy V Series node using V Series proxy then, enter the `remotePort` value as 8891.
- User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the Username and Password created in the **Add Users** Section.

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

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

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

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

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

3. Restart the V Series node or proxy service.
 - V Series node:


```
$ sudo service vseries-node restart
```
 - V Series proxy:


```
$ sudo service vps restart
```

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

Configure UCT-V Controller in OpenStack

To configure GigaVUE fabric components in OpenStack platform:

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

The screenshot displays the 'Monitoring Domain Configuration' page in the OpenStack dashboard. The page title is 'OpenStack > Monitoring Domain'. The main content area contains a form with the following fields and values:

Field	Value
Use V Series 2	<input checked="" type="checkbox"/> Yes
Monitoring Domain	Enter a monitoring domain name
Alias	Alias
URL	URL
User Domain Name	User Domain Name
Project Domain Name	Project Domain Name
Project Name	Project Name
Region	Region
Username	Username
Password	Password
Traffic Acquisition Method	G-vTAP
Traffic Acquisition Tunnel MTU	1500
Use FM to Launch Fabric	<input type="checkbox"/> No

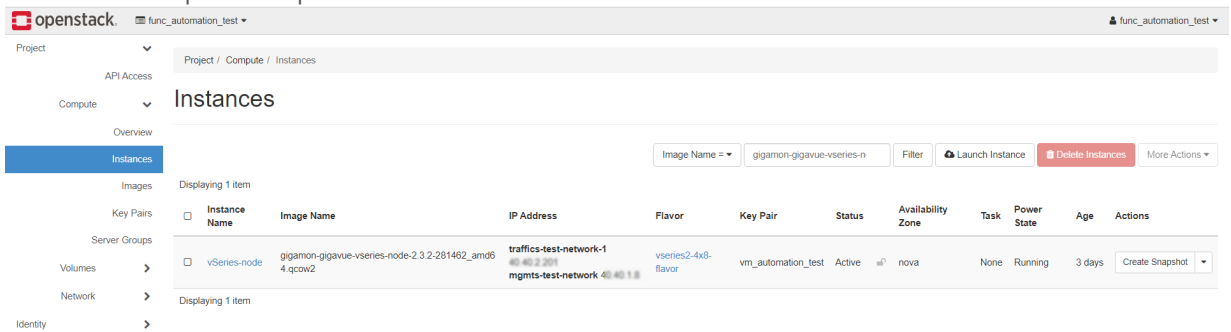
At the bottom of the page, it indicates 'FM Instance: GigaVUE-FM'. The page also features a 'Save' button and a 'Cancel' button in the top right corner.

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

Register UCT-V Controller using OpenStack GUI

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

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



The screenshot shows the OpenStack GUI interface for the 'func_automation_test' project. The 'Instances' page is active, displaying a table with one instance. The table columns are: Instance Name, Image Name, IP Address, Flavor, Key Pair, Status, Availability Zone, Task, Power State, Age, and Actions. The instance 'vSeries-node' is shown with image 'gigamon-gigavue-vseries-node-2.3.2-281492_amd64-qcow2', IP address '10.40.2.201', flavor 'vseries2-4x8-flavor', key pair 'vm_automation_test', status 'Active', availability zone 'nova', task 'None', power state 'Running', and age '3 days'. There is a 'Create Snapshot' button in the Actions column.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
<input type="checkbox"/> vSeries-node	gigamon-gigavue-vseries-node-2.3.2-281492_amd64-qcow2	traffics-test-network-1 10.40.2.201	vseries2-4x8-flavor	vm_automation_test	Active	nova	None	Running	3 days	Create Snapshot

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

Field	User Data
User data without custom certificate	<pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <Connection Name> user: <Username> password: <Password> remoteIP: <IP address of the GigaVUE-FM> sourceIP: <IP address of UCT-V Controller> (Optional Field) remotePort: 443</pre>
User data with custom certificate	<pre>#cloud-config write_files: - path: /etc/cntrlr-cert.conf owner: root:root permissions: "0644" content: -----BEGIN CERTIFICATE----- <certificate content> -----END CERTIFICATE----- - path: /etc/cntrlr-key.conf owner: root:root permissions: "400" content: -----BEGIN PRIVATE KEY----- <private key content> -----END PRIVATE KEY----- - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <Connection Name> user: <Username> password: <Password> remoteIP: <IP address of the GigaVUE-FM> sourceIP: <IP address of UCT-V Controller> (Optional Field) remotePort: 443</pre>



- User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the Username and Password created in the **Add Users** Section.

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

Register UCT-V Controller using a configuration file

To register UCT-V Controller using a configuration file:

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

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

- 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:

- a. Navigate to **/etc/netplan/** directory.
- b. Create a new **.yaml** file. (Other than the default 50-cloud-init.yaml file)
- c. 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>

```

- d. Save the file.
- e. 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 visibility node 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 OpenStack

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

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

To register UCT-V using a configuration file:

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to [Linux UCT-V Installation](#) and [Windows UCT-V Installation](#).
2. Log in to the UCT-V.

3. Create a local configuration file and enter the following user data.



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

Registration:

```

groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <IP address of the UCT-V Controller 1>,
          <IP address of the UCT-V Controller 2>

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

```



- User and Password must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.
- If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:


```

localInterface:<Interface to which UCT-V Controller is connected>

```

4. Restart the UCT-V service.

- Linux platform:


```

$ sudo service uctv restart

```
- Windows platform: Restart from the Task Manager.

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

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

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.

Upgrade GigaVUE Fabric Components in GigaVUE-FM for OpenStack

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

Refer to the following topic for more information:

- [Prerequisite](#)
- [Upgrade UCT-V Controller](#)
- [Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy](#)

Prerequisite

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

Upgrade UCT-V Controller

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

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

To change UCT-V Controller version between different major versions

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

- Under **Controller Versions**, click **Add**.
- From the **Image** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.
- From the **Flavor** drop-down list, select a size for the UCT-V Controller.
- In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.

The screenshot displays the configuration interface for UCT-V Controllers. It is organized into several sections:

- Controller Version(s):** Contains an 'Add' button and two configuration cards.
 - The first card is a template with 'Image' set to 'Select image...', 'Flavor' set to 'Select flavor...', and 'Number of Instances' set to '1'.
 - The second card is a populated instance with 'Image' set to 'gigamon-gvtap-ovs-cntlr-1.8-2', 'Flavor' set to 'm1.small', and 'Number of Instances' set to '1'.
- Management Network:** Contains 'IP Address Type' (radio buttons for Private and Floating, with Floating selected), 'Network' (dropdown set to 'mgmt-test-network'), and 'Floating IPs' (dropdown set to '10.115.176.108').
- Additional Network(s):** Contains an 'Add' button.
- Tags:** Contains an 'Add' button.

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

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

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

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

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

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



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

Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

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

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

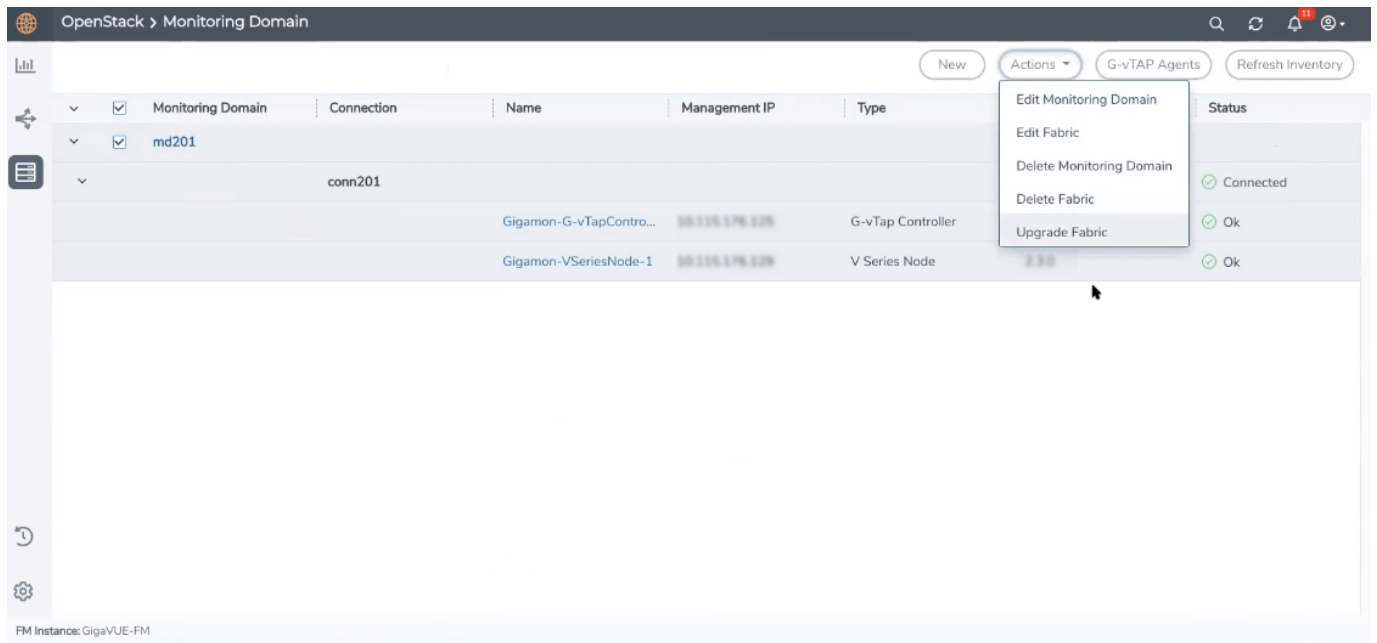
- Launch and replace the complete set of nodes and controllers at a time.

For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series nodes in your project, you can upgrade all of them at once. First, the new version of GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes are launched. Then, the old version of V Series Proxy and nodes are deleted from the project.
- NOTES:**
- When the new version of nodes and controllers are launched, the old version still exists in the project until they are deleted. Make sure the flavor determined during the configuration can accommodate the total number of new and old fabric nodes present in the project. If the flavor cannot support so many Virtual Machines, you can choose to upgrade in multiple batches.
 - If there is an error while upgrading the complete set of controllers and nodes present in the project, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
 - Prior to upgrading the GigaVUE V Series Proxy and Nodes, you must ensure that the required number of floating IP addresses are available in the respective subnets. Otherwise, the upgrade will fail.
- Launch and replace the nodes and controllers in multiple batches.

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

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

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



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

Fabric Nodes Upgrade

V Series Proxy

Upgrade

V Series Node

Upgrade

Current Version

2.3.2

Image

Select an image...

Change Flavor

Batch Size

1

Upgrade

Cancel

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

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

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

8. Click **Upgrade**.

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

The monitoring session is deployed automatically.

Configure Secure Tunnel (OpenStack)

The Secure tunnels can be configured on:

- [Precrypted Traffic](#)
- [Mirrored Traffic](#)

Precrypted Traffic

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

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

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

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

Mirrored Traffic

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

Refer to the following sections for Secure Tunnel Configuration:

- [Configure Secure Tunnel from UCT-V to GigaVUE V Series Node](#) in UCT-V
- [Configure Secure Tunnel between GigaVUE V Series Nodes](#)

Prerequisites

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

Notes

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

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

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

S.No	Task	Description						
1.	Upload a CA	<p>You must upload a Custom Authority (CA) Certificate to UCT-V Controller for establishing a connection with the GigaVUE V Series node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> Go to Inventory > Resources > Security > CA List. Click New, to add a new Custom Authority. The Add Custom Authority page appears. Enter or select the following information. <table border="1" data-bbox="662 583 1474 747"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <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> </tbody> </table> Click Save. <p>For more information, refer to Adding Certificate Authority section.</p>	Field	Action	Alias	Alias name of the CA.	File Upload	Choose the certificate from the desired location.
Field	Action							
Alias	Alias name of the CA.							
File Upload	Choose the certificate from the desired location.							
2.	Upload an SSL Key	<p>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.</p>						

S.No	Task	Description
3	Enable the secure tunnel	<p>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:</p> <ol style="list-style-type: none"> 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. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: When GigaVUE V Series is upgraded or deployed to 6.5 version, all the existing monitoring sessions will be redeployed, and individual TLS TEPs are created for each UCT-V agent in GigaVUE V Series node.</p> </div>
4.	Select the SSL Key	<p>You must select the added SSL Key in GigaVUE V Series node Key while creating a monitoring domain configuring the fabric components in GigaVUE-FM.</p> <p>To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM</p> <p>If the existing monitoring domain does not have a SSL key, you can add it by following the given steps:</p> <ol style="list-style-type: none"> 1. Select the monitoring domain for which you want to add the SSL key. 2. Click the Actions drop down list and select Edit SSL Configuration. An Edit SSL Configuration window appears. 3. Select the CA in the UCT-V Agent Tunnel CA drop down list. 4. Select the SSL key in the V Series Node SSL key drop down list. 5. Click Save.
5.	Select the CA	<p>You should select the added Certificate Authority (CA) in UCT-V Controller while creating the monitoring domain configuring the fabric components in GigaVUE-FM. To select the CA certificate, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM</p>

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:

S.No	Task	Description						
1.	Upload a CA.	<p>You must upload a CA Certificate to UCT-V Controller to establish a connection between the GigaVUE V Series node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> 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 border="1" data-bbox="576 636 1474 804"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <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> </tbody> </table> 4. Click Save. 5. Click Deploy All. <p>For more information, refer to the Adding Certificate Authority section.</p>	Field	Action	Alias	Alias name of the CA.	File Upload	Choose the certificate from the desired location.
Field	Action							
Alias	Alias name of the CA.							
File Upload	Choose the certificate from the desired location.							
2.	Upload an SSL Key.	You must add an SSL key to GigaVUE V Series node. To add an SSL Key, follow the steps in the section						
3.	Create a secure tunnel.	<p>You should create a secure tunnel to establish a connection between the UCT-V and first GigaVUE V Series Node. To enable the secure tunnel feature follow these steps:</p> <ol style="list-style-type: none"> 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 preencrypted traffic. 						
4.	Select the added SSL Key.	<p>Select the SSL Key added in Step 2, while creating a monitoring domain and configuring the fabric components in GigaVUE-FM for the first GigaVUE V Series Node.</p> <p>You must select the added SSL Key in the first GigaVUE V Series Node.</p> <p>To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM</p>						
5.	Select the added CA certificate.	You should select the added Certificate Authority (CA) in UCT-V Controller while creating the monitoring domain. To select the CA certificate, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM						
6.	Create an Egress tunnel from the first GigaVUE V Series Node.	You must create an egress tunnel for traffic to flow out from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session. Refer to Create a Monitoring Session to know about Monitoring Session.						

S.No	Task	Description												
		<p>To create the egress tunnel, follow these steps:</p> <ol style="list-style-type: none"> 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 border="1"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <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> <p>Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:</p> <ul style="list-style-type: none"> o MTU- The default value is 1500. o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64. o DSCP - Enter the Differentiated Services Code Point (DSCP) value. o Flow Label - Enter the Flow Label value. o Source L4 Port- Enter the Souce L4 Port value o Destination L4 Port - Enter the Destination L4 Port value. o Flow Label o Cipher- Only SHA 256 is supported. o TLS Version - Select TLS Version1.3. o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments. o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments. </td> </tr> <tr> <td>Remote Tunnel IP</td> <td>Enter the interface IP address of the second GigaVUE V Series Node (Destination IP).</td> </tr> </tbody> </table> <p>4. Click Save.</p>	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.	Type	Select TLS-PCAPNG for creating egress secure tunnel	Traffic Direction	<p>Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:</p> <ul style="list-style-type: none"> o MTU- The default value is 1500. o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64. o DSCP - Enter the Differentiated Services Code Point (DSCP) value. o Flow Label - Enter the Flow Label value. o Source L4 Port- Enter the Souce L4 Port value o Destination L4 Port - Enter the Destination L4 Port value. o Flow Label o Cipher- Only SHA 256 is supported. o TLS Version - Select TLS Version1.3. o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments. o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments. 	Remote Tunnel IP	Enter the interface IP address of the second GigaVUE V Series Node (Destination IP).
Field	Action													
Alias	The name of the tunnel endpoint.													
Description	The description of the tunnel endpoint.													
Type	Select TLS-PCAPNG for creating egress secure tunnel													
Traffic Direction	<p>Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:</p> <ul style="list-style-type: none"> o MTU- The default value is 1500. o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64. o DSCP - Enter the Differentiated Services Code Point (DSCP) value. o Flow Label - Enter the Flow Label value. o Source L4 Port- Enter the Souce L4 Port value o Destination L4 Port - Enter the Destination L4 Port value. o Flow Label o Cipher- Only SHA 256 is supported. o TLS Version - Select TLS Version1.3. o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments. o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments. 													
Remote Tunnel IP	Enter the interface IP address of the second GigaVUE V Series Node (Destination IP).													
7.	Select the added SSL Key in the GigaVUE V Series Node	You must select the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in the second GigaVUE V Series Node. To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM												
8	Create an ingress tunnel in the second GigaVUE	You must create a ingress tunnel for traffic to flow in from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session for the second GigaVUE V Series Node. Refer to Create a Monitoring												

S.No	Task	Description														
	V Series node.	<p>Session to know about monitoring session.</p> <p>To create the ingress tunnel, follow these steps:</p> <ol style="list-style-type: none"> 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 border="1"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>The name of the tunnel endpoint.</td> </tr> <tr> <td>Description</td> <td>The description of the tunnel endpoint.</td> </tr> <tr> <td>Type</td> <td>Select TLS-PCAPNG for creating egress secure tunnel. NOTE: If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.</td> </tr> <tr> <td>Traffic Direction</td> <td>Choose In (Decapsulation) for creating an ingress tunnel that receives traffic from the first GigaVUE V Series Node. 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> </tbody> </table> <ol style="list-style-type: none"> 4. Click Save. 	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.	Type	Select TLS-PCAPNG for creating egress secure tunnel. NOTE: If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.	Traffic Direction	Choose In (Decapsulation) for creating an ingress tunnel that receives traffic from the first GigaVUE V Series Node. Select or enter the values as described in Step 6:	IP Version	The version of the Internet Protocol. IPv4 and IPv6 are supported.	Remote Tunnel IP	Enter the interface IP address of the first GigaVUE V Series Node (Destination IP).
Field	Action															
Alias	The name of the tunnel endpoint.															
Description	The description of the tunnel endpoint.															
Type	Select TLS-PCAPNG for creating egress secure tunnel. NOTE: If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.															
Traffic Direction	Choose In (Decapsulation) for creating an ingress tunnel that receives traffic from the first GigaVUE V Series Node. Select or enter the values as described in Step 6:															
IP Version	The version of the Internet Protocol. IPv4 and IPv6 are supported.															
Remote Tunnel IP	Enter the interface IP address of the first GigaVUE V Series Node (Destination IP).															

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. Click **Add**.
4. In the **Template** field, enter the name of the precryption template.
5. From the **Priority** drop-down list, 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.
6. In the **Rule Name** field, enter the name of the rule.
7. From the **Traffic Action** drop-down list, select how the traffic should be handled.

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

NOTE: In the absence of a Precryption rule, traffic is implicitly allowed. 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.

8. From the **Direction** drop-down list, select the direction of traffic.
 - 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.
9. From the **L3/L4 Layer** drop-down list, select **L3** or **L4**.

NOTE: L4 Filter Type can only be used with L3.

10. From the **Condition** drop-down list, select the type of condition.
11. From the **Condition Relation** drop-down list, select any of the following:
 - Equal to
 - Not equal to
12. In the Value field, select or enter based on the selected **Condition**.

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

13. 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 [Configure Monitoring Session Options \(OpenStack\)](#) section.

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

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

Configure Monitoring Session

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

Refer to the following sections for details:

- [Create a Monitoring Session \(OpenStack\)](#)
- [Create Ingress and Egress Tunnels \(OpenStack\)](#)
- [Create Raw Endpoint \(OpenStack\)](#)
- [Create a New Map \(OpenStack\)](#)
- [Add Applications to Monitoring Session](#)
- [Interface Mapping \(OpenStack\)](#)
- [Deploy Monitoring Session](#)
- [View Monitoring Session Statistics](#)
- [Visualize the Network Topology](#)

Create a Monitoring Session (OpenStack)

You must a [Create Monitoring Domain](#) before creating a monitoring session.

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

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

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

You can create multiple Monitoring Sessions per Monitoring Domain.

To create a new Monitoring Session:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Click **New Monitoring Session** button to open the **New Monitoring Session** configuration page.
3. In the **Alias** field, enter a name for the Monitoring Session.
4. From the **Monitoring Domain** drop-down list, select the desired monitoring domain.
5. From the **Connections** drop-down list, select the appropriate connection.
6. Click **Save**. The Monitoring Session Overview page appears.



Monitoring Session Page (OpenStack)

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

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

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

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

- Delete
- Deploy
- Undeploy

Configure Monitoring Session Options (OpenStack)

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

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

Traffic Acquisition

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

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

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

- [Enable Prefiltering](#)
- [Enable Precryption](#)

Enable Prefiltering

To enable Prefiltering, follow the steps given below:

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

Enable Precryption

Rules and Notes

- To avoid packet fragmentation, you should change the option `precryption-path-mtu` in UCT-V configuration file (`/etc/uctv/uctv.conf`) within the range 1400-9000 based on the platform path MTU.
- Protocol version IPv4 and IPv6 are supported.
- If you wish to use IPv6 tunnels, your GigaVUE-FM and the fabric components version must be 6.6.00 or above.

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

To enable Precryption, follow the steps given below:

1. In the Monitoring Session **TRAFFIC ACQUISITION** page, click **Precryption** tab.
2. Enable the **Precryption** toggle button. Refer to [Precryption™](#) topic for more details on Precryption.

3. You can apply Precryption to a few selective components based on the traffic:

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

Applications:

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

L3-L4

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

Validate Precryption connection

To validate the Precryption connection, follow the steps:

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

Limitations

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

Traffic processing

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

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

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

- [Apply Threshold Template](#)
- [Enable User Defined Applications](#)
- [Enable Distributed De-duplication](#)

Apply Threshold Template

To apply threshold, follow the steps given below:

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

Enable User Defined Applications

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

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

Enable Distributed De-duplication

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



Notes:


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

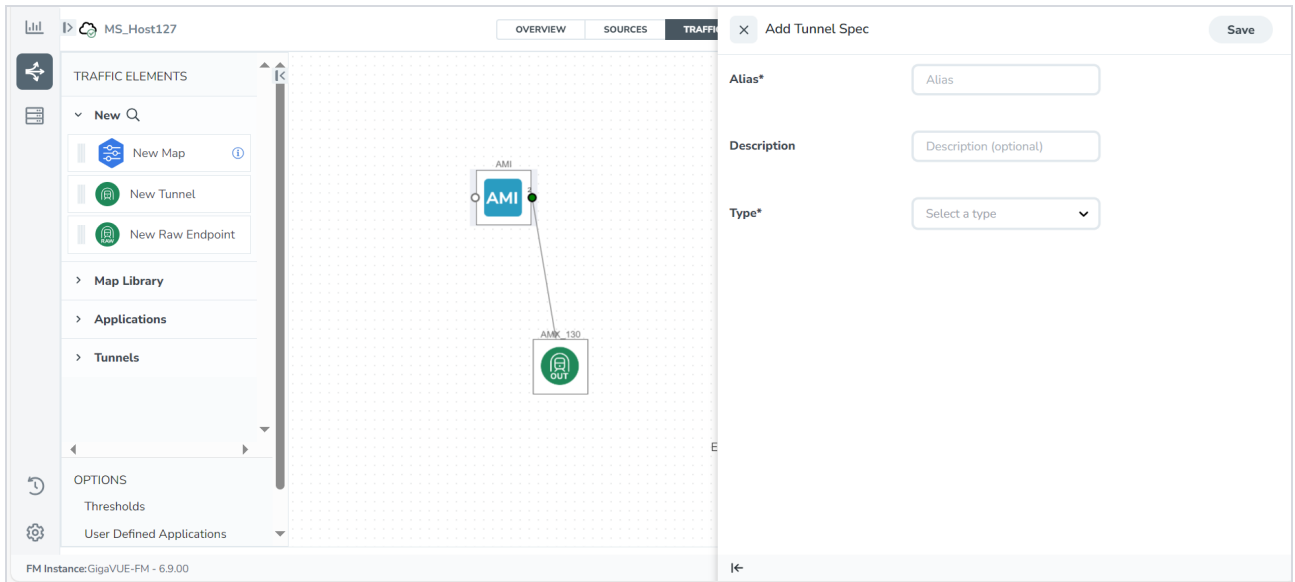
Create Ingress and Egress Tunnels (OpenStack)

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

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

To create a new tunnel endpoint:

1. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.
2. In the canvas, click the  icon on the left side of the page to view the traffic processing elements. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.



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

Field	Description	
Alias	The name of the tunnel endpoint.	
Description	The description of the tunnel endpoint.	
Admin State	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.	
NOTE: This option appears only after the Monitoring session deployment.		
Type	The type of the tunnel. Select from the below options to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE.	
VXLAN		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
NOTE: In the scenario where secure tunnels need to be established between a GigaVUE V Series Node and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device. Refer to the Secure Tunnels section.		
In	Choose In (Decapsulation) for creating an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose Out (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node to the destination endpoint.	
	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.

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

Field	Description	
device . Refer to the Secure Tunnels section.		
In	Choose In (Decapsulation) to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
Out	Choose Out (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint.	
	Remote Tunnel IP	For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that 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		

Field	Description	
	The direction of the traffic flowing through the GigaVUE V Series Node.	
	<p>NOTE: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . Refer to the Secure Tunnels section.</p>	
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:		
Out	L4 Destination IP Address	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. Refer to Application Metadata Exporter for more detailed information.
	Source L4 Port	The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.

4. Click **Save**.

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

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

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

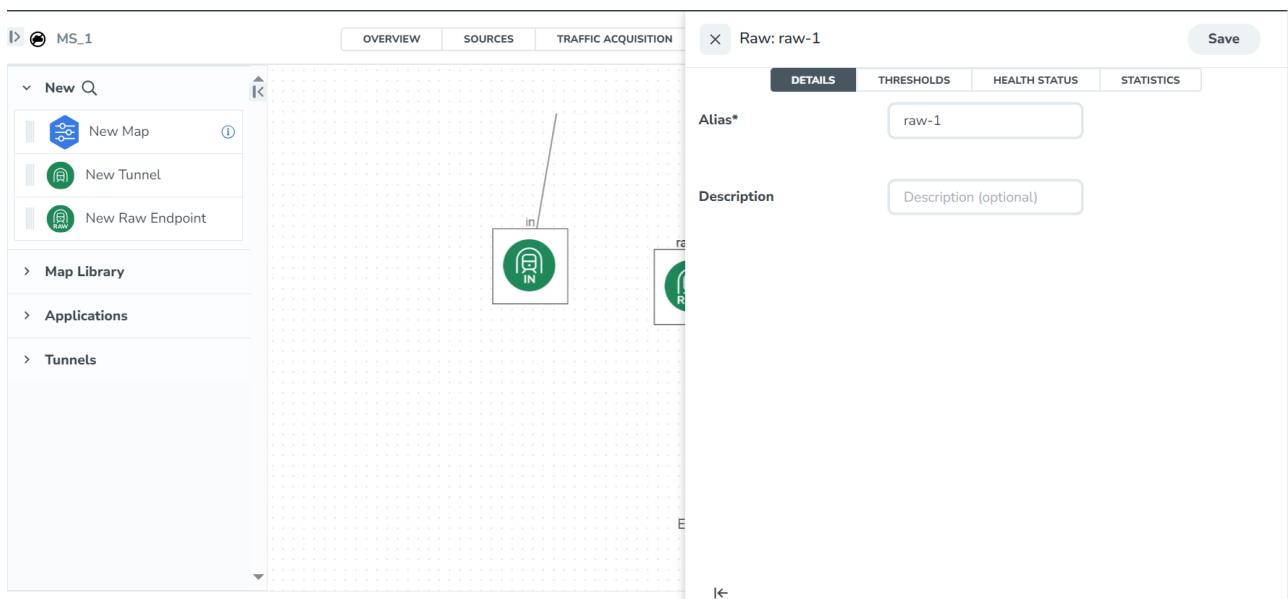
After configuring the tunnels and deploying the Monitoring Session, you can view the number of ingress and egress tunnels configured for a Monitoring Session. Click on the numbers of tunnels displayed to view the tunnel names and their respective **ADMIN STATUS** and **HEALTH STATUS**.

Create Raw Endpoint (OpenStack)

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

To add Raw Endpoint to the monitoring session:

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



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


Create a New Map (OpenStack)

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.

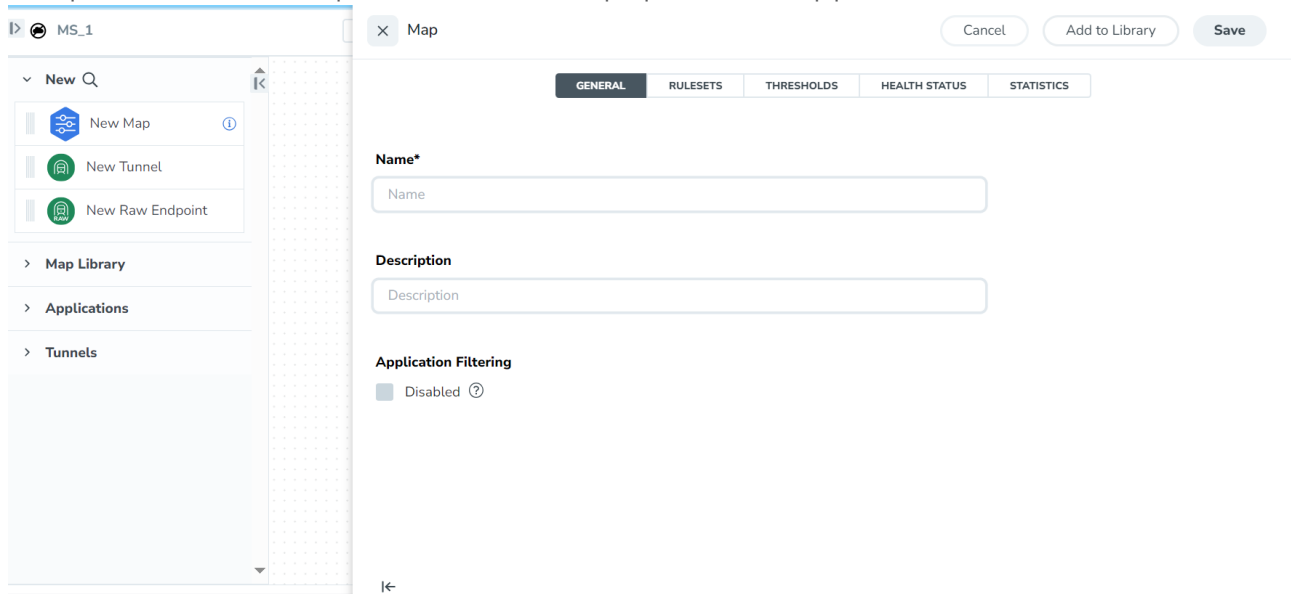
Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	<p>A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session.</p> <p>The below formula describes how ATS works:</p> <p>Selected Targets = Traffic Filter Maps \cap Inclusion Maps - Exclusion Maps</p> <p>Below are the filter rule types that work in ATS:</p> <ul style="list-style-type: none"> mac Source mac Destination ipv4 Source ipv4 Destination ipv6 Source ipv6 Destination VM Name Destination VM Name Source VM Tag Destination - 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. <p>The traffic direction is as follow:</p> <ul style="list-style-type: none"> For any rule type as Source - the traffic direction is egress. For Destination rule type - the traffic direction is ingress. For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. <div data-bbox="683 1199 1468 1570" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Notes:</p> <ul style="list-style-type: none"> 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. </div>
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.
- Loopback captures bidirectional traffic from both ingress and egress. To prevent duplicate tapping, only egress tapping is permitted.
- If you are running GigaVUE Cloud Suite on OpenStack, you can add a subnet to the exclusion map. To do this, create an exclusion map and select the Subnet name in the ruleset.
- If a packet is fragmented then all the fragments will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide* for detailed information.


To create a new map:

1. After creating a new Monitoring Session, or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas appears.
2. In the canvas, click on the  icon expand icon on the left side of the page to view the traffic processing elements. Select **New > New Map**, drag and drop a new map template to the workspace. The New Map quick view appears.




The screenshot displays the 'New Map' configuration window. On the left, a sidebar contains a search bar labeled 'New Q' and a list of actions: 'New Map', 'New Tunnel', and 'New Raw Endpoint'. Below this are expandable sections for 'Map Library', 'Applications', and 'Tunnels'. The main area shows a 'Map' configuration form with tabs for 'GENERAL', 'RULESETS', 'THRESHOLDS', 'HEALTH STATUS', and 'STATISTICS'. The 'GENERAL' tab is selected, showing a 'Name*' field, a 'Description' field, and an 'Application Filtering' section with a 'Disabled' checkbox and a help icon.

3. On the New Map quick view, click on **General** tab and enter the following details:
 - a. In the **Name** field, enter a name for the new map.
 - b. In the **Description** field, enter a description for the map.
 - c. Turn on the **Application Filtering** toggle, to configure Application Filtering Intelligence. Enabling this toggle button allows filtering of traffic based on application name or family. Refer to [Application Filtering Intelligence](#) for more details.

 Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:

- Traffic Map—Only Pass rules for ATS
- Inclusion Map—Only Pass rules for ATS
- Exclusion Map—Only Drop rules for ATS

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

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

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

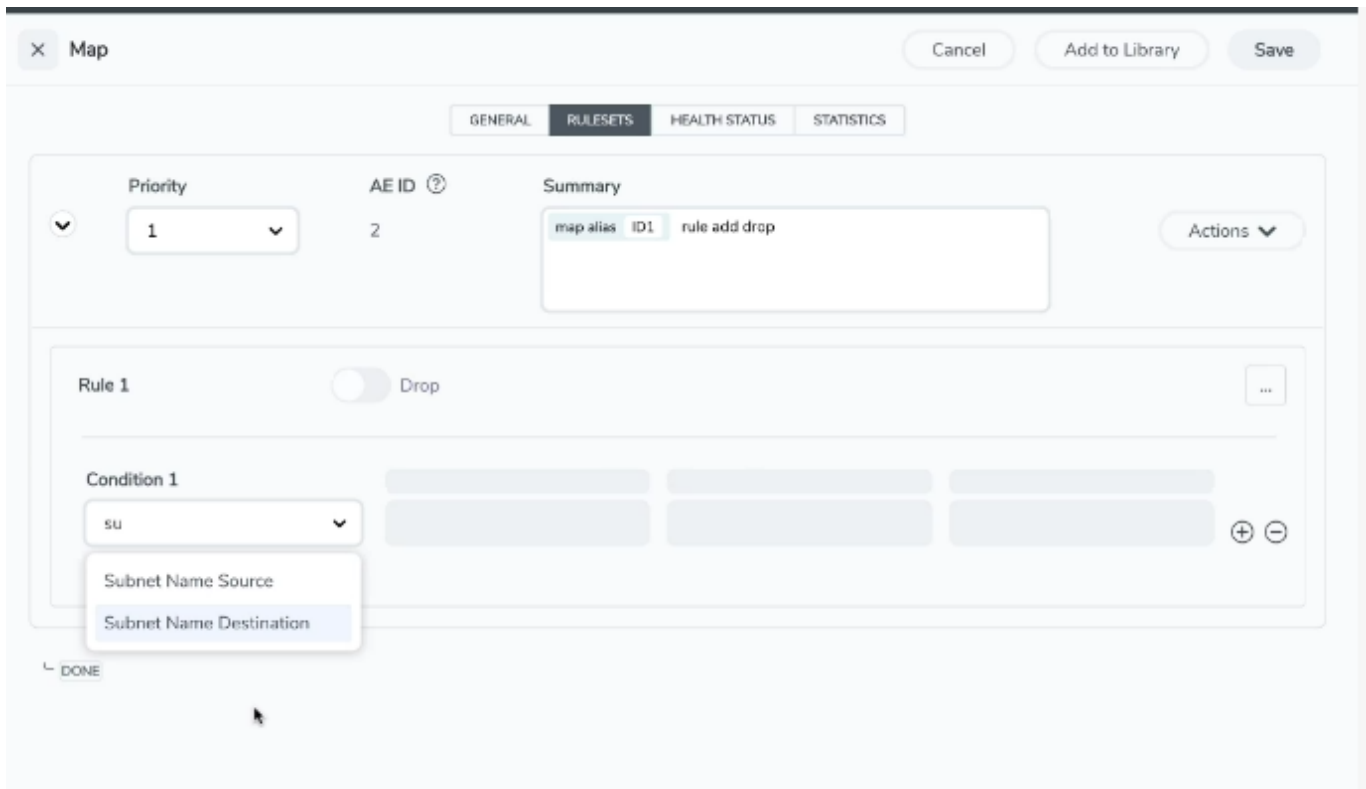
Example- Create a New Map using Inclusion and Exclusion Maps

Consider a Monitoring Session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

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

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

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



Map Library

To reuse a map,

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

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

Add Applications to Monitoring Session

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

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- GENEVE Decap
- Header Stripping
- Application Metadata Exporter
- SSL Decrypt
- GigaSMART NetFlow Generation
- 5G-Service Based Interface Application
- 5G-Cloud Application

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

Interface Mapping (OpenStack)

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

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

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

Deploy Monitoring Session

To deploy the Monitoring Session:

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

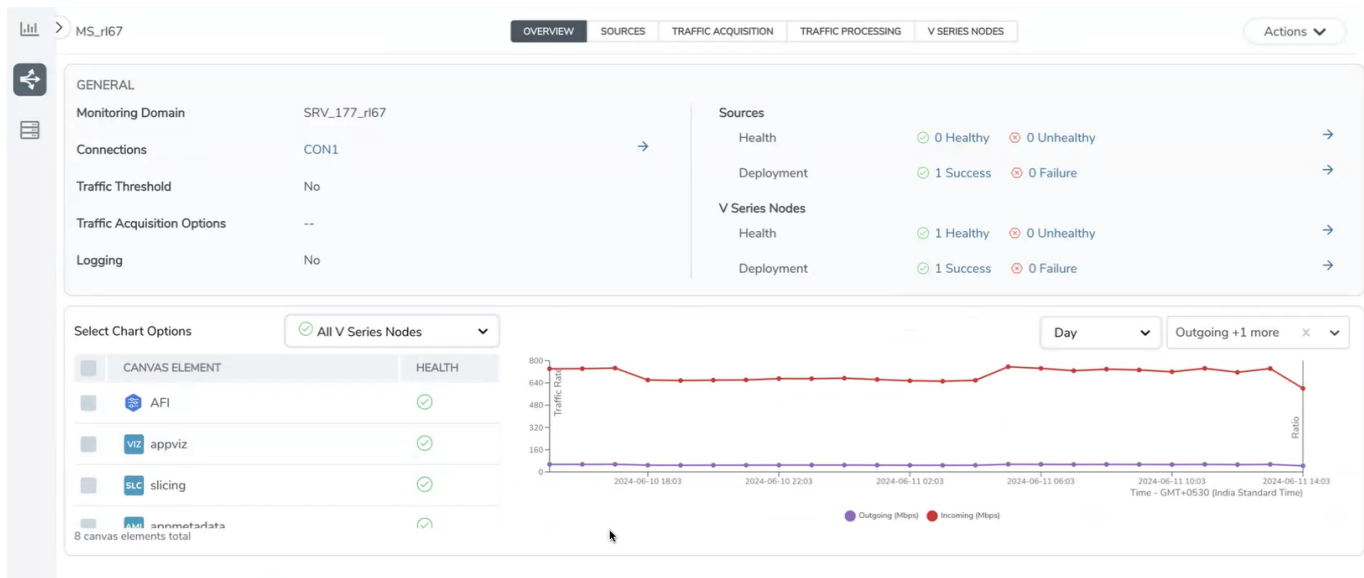
NOTE: You can drag multiple arrows from a single map and connect them to different maps.

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

View Monitoring Session Statistics

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

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



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

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

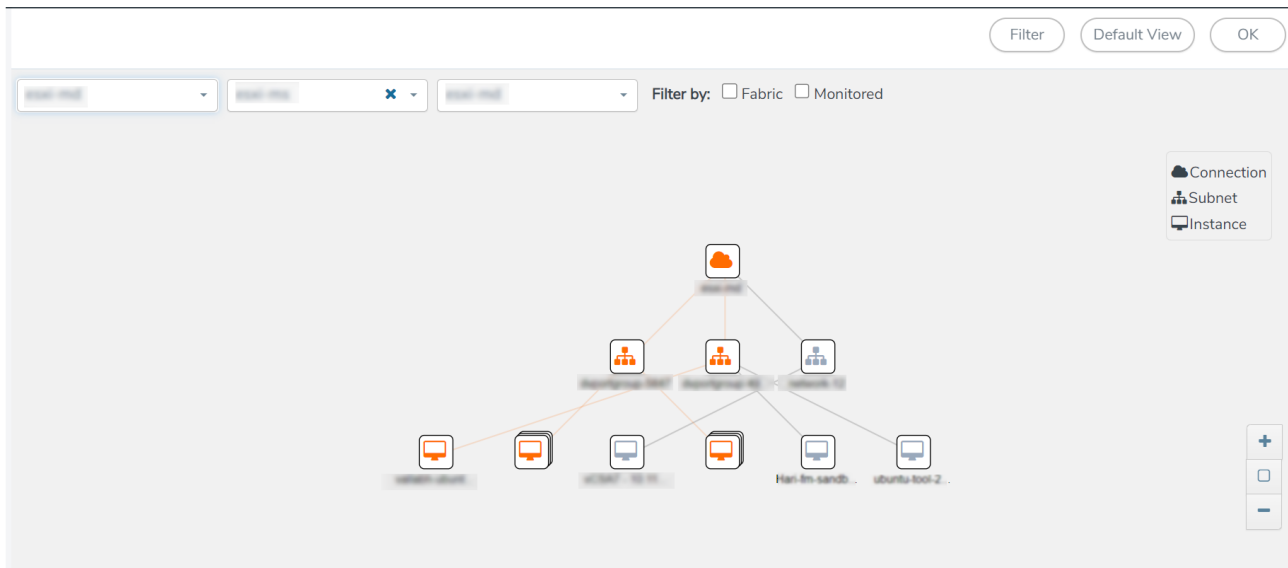
Visualize the Network Topology

Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

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



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

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

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

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 `preencryption-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.

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	✓	✓	✓	✗	✗
Traffic Mirroring	✓	✗	✗	✗	✗
OVS Mirroring and VLAN Trunk Port	✗	✗	✓	✗	✗

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

Traffic Health Monitoring

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

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

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

For V Series Nodes:

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

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

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

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

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

- After applying threshold template to a particular application, you need not deploy the Monitoring Session again.

Supported Resources and Metrics

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

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

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

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

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

Apply Threshold Template

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

Apply Threshold Template to Monitoring Session

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

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

Apply Threshold Template to Applications

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

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

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

Clear Thresholds

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

Clear Thresholds for Applications

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

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

Clear Thresholds across the Monitoring Session

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

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

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

View Health Status

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

View Health Status of an Application

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

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

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

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

View Health Status for Individual GigaVUE V Series Nodes

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

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

Analytics for Virtual Resources

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

Rules and Notes:

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


Virtual Inventory Statistics and Cloud Applications Dashboard

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

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

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)	<p>Statistical details of the virtual inventory based on the platform and the health status.</p> <p>You can view the following metric details at the top of the dashboard:</p> <ul style="list-style-type: none"> • Number of Monitoring Sessions • Number of V Series Nodes • Number of Connections • Number of GCB Nodes <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> • Platform • Health Status 	<i>V Series Node Status by Platform</i>	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		<i>Monitoring Session Status by Platform</i>	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		<i>Connection Status by Platform</i>	Number of healthy and unhealthy connections for each of the supported cloud platforms
		<i>GCB Node Status by Platform</i>	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	<p>Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> • Platform • Connection • V Series Node 	<i>V Series Node Maximum CPU Usage Trend</i>	<p>Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V Series nodes do not have service cores, therefore the CPU usage is reported as 0.</p> </div>

Dashboard	Displays	Visualizations	Displays
		<i>V Series Node with Most CPU Usage For Past 5 minutes</i>	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.
		<i>V Series Node Rx Trend</i>	Receiving trend of the V Series node in 5 minutes interval, for the past one hour.
		<i>V Series Network Interfaces with Most Rx for Past 5 mins</i>	Total packets received by each of the V Series network interface for the past 5 minutes. NOTE: You cannot use the time based filter options to filter and visualize the data.
		<i>V Series Node Tunnel Rx Packets/Errors</i>	Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation.
		<i>V Series Node Tunnel Tx Packets/Errors</i>	TX is for output tunnels from 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	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application

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

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

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

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

Administer GigaVUE Cloud Suite for OpenStack

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

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

Configure the OpenStack Settings

To configure the OpenStack Settings:

1. Go to **Inventory > VIRTUAL > OpenStack**, and then click **Settings**.
2. Click the **Settings** drop-down, and then select **Advanced Settings**.
3. Click **Edit** to edit the Advanced Settings fields.

Advanced Settings

Refresh interval for VM target selection inventory (secs)	120
Refresh interval for fabric deployment inventory (secs)	900
Number of UCT-Vs per V Series Node	100
Number of hypervisors per V Series Node	5
Refresh interval for UCT-V inventory (secs)	900
OVS Mirror tunnel range start	10000
OVS Mirror tunnel range end	30000
Traffic distribution tunnel range start	8000
Traffic distribution tunnel range end	8512
Traffic distribution tunnel MTU	9001
OVS Agent Traffic when V Series is down	Disabled
Reboot threshold limit for UCT-V Controller down ⓘ	2

Refer to the following table for descriptions of the Settings fields.

Settings	Description
Refresh interval for VM target selection inventory (secs)	Specifies the frequency for updating the inventory of VMs in OpenStack.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for updating the inventory of GigaVUE fabrics in OpenStack.
Number of UCT-Vs per V Series Node (applicable only for UCT-V based connections)	Specifies the maximum number of instances that can be assigned to the V Series node.
Number of hypervisors per V Series Node	Specifies the maximum number of hypervisors that can be assigned to the V Series node.

Settings	Description
(applicable only for OVS mirroring)	
Refresh interval for UCT-V inventory (secs)	Specifies the frequency for discovering the UCT-Vs available in the project. This is applicable for UCT-Vs only.
OVS Mirror tunnel range start	Specifies the startup range value of the OVS mirror tunnel ID. This is applicable for UCT-V OVS Agents only.
OVS Mirror tunnel range end	Specifies the closing range value of the OVS mirror tunnel ID. This is applicable for UCT-V OVS Agents only.
Traffic distribution tunnel range start	Specifies the start range value of the tunnel ID.
Traffic distribution tunnel range end	Specifies the closing range value of the tunnel ID.
OVS Agent Traffic when V Series is down	Enable this option to stop the OVS Agent from sending the traffic to the V Series node. You can stop the traffic either manually or automatically. Refer to Shutdown or Restart of OVS traffic to know more about the manual or automatic shut down and restart.
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.



- UCT-V OVS agent supports a maximum of 255 source interfaces per OpenStack node.
- A maximum of 100 OpenStack connections are allowed for an OpenStack module.

Shutdown or Restart of OVS traffic

GigaVUE-FM allows you to stop or restart the traffic through OVS Mirroring based on the availability of V Series node.

GigaVUE-FM helps you to stop the traffic when the V Series node is unreachable or unrecoverable, and restart it when the GigaVUE V Series Node is reachable again in the following ways:

- [Manual shutdown or restart of OVS traffic](#)
- [Automatic shutdown or restart of OVS traffic](#)

Manual shutdown or restart of OVS traffic

The traffic sent from the OVS Mirroring Agent can be manually stopped and started.

To shut down or restart the OVS traffic manually, follow these steps:

1. Go to **Inventory > VIRTUAL > OpenStack**, and then click **Settings**
2. Click the **Settings** drop-down, and then select **Advanced Settings**.
3. Enable the check box **OVS Agent Traffic when V Series is down**.
4. Click the **Fabric** tab.
5. Select the V Series node.
6. Click the **Actions** drop-down list and select **Shut down OVS Traffic** or **Restart OVS Traffic** as required.

NOTE: You can view the **Shut down OVS Traffic** or **Restart OVS Traffic** options only when you enable the check box **OVS Agent Traffic when V Series is down** in the Advanced Settings.

Automatic shutdown or restart of OVS traffic

When the GigaVUE Cloud Suite V Series node is deleted or changed to an unrecoverable state in the OpenStack platform, GigavUE-FM performs the action as explained in the following table:

V Series node Status in OpenStack	Action in GigaVUE-FM	Action in GigaVUE-FM when you enable the option
When a V Series node is deleted from the OpenStack platform	GigaVUE-FM automatically sets the status of that V Series node as terminated.	In the Advanced Settings , when the OVS Agent Traffic when V Series is down checkbox is enabled, GigaVUE-FM removes the source interfaces of OVS Mirroring agent
When a V Series Node is changed to a stopped or shutoff state in Openstack	GigaVUE-FM Health monitoring module	In the Advanced Settings , when the

V Series node Status in OpenStack	Action in GigaVUE-FM	Action in GigaVUE-FM when you enable the option
	tries to start the V Series node. If unsuccessful after two attempts, GigaVUE-FM considers the V Series node to be unrecoverable.	OVS Agent Traffic when V Series is down checkbox is enabled, GigaVUE-FM removes the source interfaces of OVS Mirroring agent.
When a V Series node is in an active state and its connection to GigaVUE-FM is restored	GigaVUE-FM Health Monitoring module determines V Series Node is in a healthy state.	In the Advanced Settings , when the OVS Agent Traffic when V Series is down checkbox is enabled, GigaVUE-FM adds the source interfaces of the OVS Mirroring agent and restarts the OVS traffic.

Role Based Access Control

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

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

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

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

NOTE: Cloud APIs are also RBAC enabled.

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

About Audit Logs

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

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

All Audit Logs Filter Manage

Filter : none

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

Go to page: 1 of 16 Total Records: 106

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: <ul style="list-style-type: none"> Log in and Log out based on users. Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details on whether the user was in GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

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

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

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

To filter the audit logs, do the following:

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

About Events

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

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

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

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

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

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

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

Controls/ Parameters	Description
Source	The source from where the events are generated. The criteria can be as follows: <ul style="list-style-type: none"> ▪ FM - indicates the event was flagged by the GigaVUE-FM fabric manager. ▪ VMM - indicates the event was flagged by the Virtual Machine Manager. ▪ FM Health - indicates the event was flagged due to the health status change of GigaVUE-FM.
Duration	The timestamp when the event occurred or the duration in which the event occurred. IMPORTANT: Timestamps or the duration are shown in the time zone of the client browser's computer and not the time zone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured time zone.
Scope	The category to which the events belong. Events can belong to the following category: Domain, Node, Card, Port, Stack, Cluster, Chassis, GigaVUE-FM, GigaVUE-VM, and so on. For example, if there is a notification generated for port utilization low threshold, the scope is displayed as Physical Node.
Alarm Type	The type of events that generate the alarms. The types of alarms can be Abnormal Fan Operation, Card Unhealthy, Circuit Tunnel Unhealthy, CPU Over Loaded, Device Upgrade Failed.
Event Severity	The severity is one of Critical, Major, Minor, Warning or Info. Info is informational messages. For example, when power status change notification is displayed, then the message is displayed as Info.
Event Status	The status of the event. The status can be Acknowledged or Unacknowledged.
Event Type	The type of event that generated the events. The type of events can be CPU utilization high, cluster updated, device discovery failed, fan tray changed, netflow generation statistics, and so on.
Affected Entity Type	The resource type associated with the event. For example, when low disk space notification is generated, 'Chassis' is displayed as the affected entity type.
Cluster ID	Enter the Cluster ID.
Affected Entity	The resource ID of the affected entity type. For example, when low disk space notification is generated, the IP address of the node with the low disk space is displayed as the affected entity.
Device IP	The IP address of the device.
Host Name	The host name of the device.
Alias	Event Alias
Monitoring Domain	The name of the Monitoring Domain.
Connection	The name of the Connection.
Show Non-taggable Entities	Enable to display the events for entities that cannot be tagged. For example, Policies, GigaVUE-FM instance and other such entities.
Tags	Select the Key and the Value from the drop-down list.

To filter the alarms and event:

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

Troubleshooting

This section provides the information needed to troubleshoot GigaVUE-FM integration with OpenStack.

OpenStack Connection Failed

The connFailed state indicates that the OpenStack connection has failed. Check the following troubleshoot tips to restore the connection:

- Verify if GigaVUE-FM is able to reach the OpenStack cloud controller.
- Check if the OpenStack cloud controller is DNS resolvable from GigaVUE-FM.
- Verify if the region name provided while launching the instance is accurate.
- Ensure that all the security group rules required for communication between GigaVUE-FM and OpenStack cloud controller OR GigaVUE-FM and DNS server are accurately setup.
- Check if the Compute Servers that the nova API returns are reachable from GigaVUE-FM. Refer to [Handshake Alert: unrecognized_name](#).

Handshake Alert: unrecognized_name

When setting up the OpenStack connection in GigaVUE-FM, the GigaVUE-FM logs might show a handshake alert: unrecognized_name error. This error is related to a Server Name Indication (SNI) error. Starting with Java 7, the JDK does not ignore the unrecognized name warning. To resolve this issue, perform either of the following:

- Fix the configuration on the server where the error is occurring.
- Ignore the warning on the client side (GigaVUE-FM server) by using the Java system property `--Djsse.enableSNIExtension=false` while launching GigaVUE-FM.

Contact support for information on how to use the Java system property. However, this is not recommended for security reasons.

GigaVUE V Series Node or UCT-V Controller is Unreachable

If GigaVUE V Series node or UCT-V Controller is unreachable, verify the following:

- The correct version of the image is uploaded.
- The network is reachable.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- [Documentation](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VUE Community](#)

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.9 Hardware and Software Guides
<p>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.</p>
<p>Hardware</p> <p>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</p>
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 6.9 Hardware and Software Guides

GigaVUE-TA200 Hardware Installation Guide

GigaVUE-TA200E Hardware Installation Guide

GigaVUE-TA400 Hardware Installation Guide

GigaVUE-OS Installation Guide for DELL S4112F-ON

G-TAP A Series 2 Installation Guide

GigaVUE M Series Hardware Installation Guide

GigaVUE-FM Hardware Appliances Guide

Software Installation and Upgrade Guides

GigaVUE-FM Installation, Migration, and Upgrade Guide

GigaVUE-OS Upgrade Guide

GigaVUE V Series Migration Guide

Fabric Management and Administration Guides

GigaVUE Administration Guide

covers both GigaVUE-OS and GigaVUE-FM

GigaVUE Fabric Management Guide

how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features

Cloud Guides

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

GigaVUE V Series Applications Guide

GigaVUE 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

Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite 6.9 Hardware and Software Guides	
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions	
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions	
Reference Guides	
GigaVUE-OS CLI Reference Guide	library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and 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	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to 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)