Gigamon®

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

Product Version: 6.14

Document Version: 1.0

(See Change Notes for document updates.)

Copyright © 2026 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
6.14	1.0	07/10/2026	The original release of this document with 6.14.00 GA.

Contents

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration **1**
Change Notes 3
Contents 4
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration **9**
Overview of Third Party Orchestration **9**
Components for Third Party Orchestration 10
Cloud Overview Page (Third Party Orchestration) 11
Top Menu 13
Viewing Charts on the Overview Page 14
Viewing Monitoring Session Details 15
Introduction to Supported Features on GigaVUE Cloud Suite for Third Party Orchestration **16**
Secure Communication between GigaVUE Fabric Components 16
GigaVUE-FM acts as the PKI 17
Bring Your Own CA 18
Rules and Notes 18
Precryption™ 18
How Gigamon Precryption Technology Works 19
Why Gigamon Precryption 20
Key Features 20
Key Benefits 21
How Gigamon Precryption Technology Works 21
Supported Platforms 23
Prerequisites 24
Secure Tunnels 25
Prefiltering 27
Analytics for Virtual Resources 27
Virtual Inventory Statistics and Cloud Applications Dashboard 28
Cloud Health Monitoring 33
Customer Orchestrated Source - Use Case 33
Get Started with Third Party Orchestration **34**
License information 34

Default Trial Licenses 34
Volume-Based License 35
Base Bundles 36
Add-on Packages 37
How GigaVUE-FM Tracks Volume-Based License Usage 38
Network Firewall Requirement 42
GigaVUE FM 42
UCT-V Controller 44
UCT-V 46
GigaVUE V Series Node 46
Giga VUE V Series Proxy(Optional) 48
UCT-C Controller - deployed in Kubernetes worker mode 49
UCT-V Controller 50
GigaVUE V Series Node 50
GigaVUE V Series Proxy(Optional) 50
GigaVUE-FM Version Compatibility 51
Configure Role-Based Access for Third Party Orchestration 51
Users 51
Role 52
User Groups 52
Configure Tokens 54
Prerequisite 54
Rules and Notes 54
Create Token 55
Revoke Tokens 55
Export Token 56
Create a Token with Custom User Group 56
Modes of Deployments 56
Generic Mode 57
Integrated Mode 57

Deployment Options for GigaVUE Cloud Suite for Third Party Orchestration 57

Deploy GigaVUE Fabric Components using Generic Mode 58
Without Creating Monitoring Domain 58
By Creating Monitoring Domain 59
Deploy GigaVUE Fabric Components using Integrated Mode 60

Deploy GigaVUE Cloud Suite for Third Party Orchestration 61

Install GigaVUE-FM 62
Install UCT-V 63
Supported Platforms 63
Supported Operating Systems for UCT-V 64

Linux UCT-V Installation 64
Windows UCT-V Installation 74
Uninstall UCT-V 80
Upgrade or Reinstall UCT-V 81
Upgrade UCT-V through GigaVUE-FM (Recommended Method) 81
Upgrade UCT-V Manually 84
Integrate Private CA 84
Rules and Notes 84
Generate CSR 85
Upload CA Certificate 85
Adding Certificate Authority 86
Create Monitoring Domain 86
Edit SSL Configuration 89
Deploy Fabric Components using Generic Mode 89
Configure and Deploy GigaVUE Fabric Components using AWS - Generic Mode 90
Configure and Deploy GigaVUE Fabric Components using Azure - Generic Mode 99
Configure GigaVUE Fabric Components using GCP 109
Configure GigaVUE Fabric Components using Nutanix 119
Configure GigaVUE Fabric Components using OpenStack 145
Configure GigaVUE Fabric Components using VMware ESXi 154
Configure GigaVUE Fabric Components using VMware vCenter 166
Configure GigaVUE Fabric Components using Third Party Orchestration on NSX-T Federation Environment 176
Deploy and Register GigaVUE V Series Nodes on KVM Hypervisor 184
Deploy Fabric Components using Integrated Mode 187
Configure Secure Communication between Fabric Components in FMHA 187
Configure Secure Tunnel for Third Party Orchestration ... 188
Precrypted Traffic 188
Mirrored Traffic 188
Prerequisites 188
Notes 189
Configure Secure Tunnel from UCT-V to GigaVUE V Series Node 189
Configure Secure Tunnel between GigaVUE V Series Nodes 190
Viewing Status of Secure Tunnel 194
Create Prefiltering Policy Template 194
Create Precryption Template for UCT-V 196
Rules and Notes: 196
Create Precryption Template for Filtering based on Applications 196
Create Precryption Template for Filtering based on L3-L4 details 197

Configure Monitoring Session **201**
Create a Monitoring Session (Third Party Orchestration) 201
Monitoring Session Page (Third Party Orchestration) 202
Monitoring Session Options (Third Party Orchestration) 204
Create Ingress and Egress Tunnel (Third Party Orchestration) 206
Create Raw Endpoint (Third Party Orchestration) 213
Create a New Map (Third Party Orchestration) 214
Example- Create a New Map using Inclusion and Exclusion Maps 217
Map Library 218
Add Applications to Monitoring Session 219
Interface Mapping 220
Deploy Monitoring Session 220
View Monitoring Session Statistics 224
Visualize the Network Topology (Third Party Orchestration) 224
Configure Precryption in UCT-V **225**
Rules and Notes 226
Validate Precryption connection 226
Limitations 227
Migrate Application Intelligence Session to Monitoring Session **227**
Post Migration Notes for Application Intelligence 228
Monitor Cloud Health **230**
Configuration Health Monitoring 230
Traffic Health Monitoring 230
Supported Resources and Metrics 232
Create Threshold Templates 234
Apply Threshold Template 235
Clear Thresholds 236
View Health Status 237
View Health Status of an Application 237
View Operational Health Status of an Application 237
View Health Status for Individual GigaVUE V Series Nodes 239
View Application Health Status for Individual V Series Nodes 240
Administer GigaVUE Cloud Suite for Third Party Orchestration **240**
Configure Certificate Settings 240
Configure Third Party Orchestration Settings 241
Role Based Access Control 243
About Audit Logs 244

Debuggability and Troubleshooting **245**
Sysdumps 246
Sysdumps—Rules and Notes 246
Generate a Sysdump File 246
FAQs - Secure Communication between GigaVUE Fabric Components (Third Party Orchestration) **247**
Additional Sources of Information **251**
Documentation 251
How to Download Software and Release Notes from My Gigamon 254
Documentation Feedback 254
Contact Technical Support 255
Contact Sales 256
Premium Support 256
The VÜE Community 256
Glossary **257**

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

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

Topics:

- Overview of Third Party Orchestration
- Introduction to Supported Features on GigaVUE Cloud Suite for Third Party Orchestration
- Get Started with Third Party Orchestration
- Deployment Options for GigaVUE Cloud Suite for Third Party Orchestration
- Deploy GigaVUE Cloud Suite for Third Party Orchestration
- Configure Secure Tunnel for Third Party Orchestration
- Create Prefiltering Policy Template
- Create Precryption Template for UCT-V
- Configure Monitoring Session
- Configure Precryption in UCT-V
- Migrate Application Intelligence Session to Monitoring Session
- Monitor Cloud Health
- Administer GigaVUE Cloud Suite for Third Party Orchestration

Overview of Third Party Orchestration

You can use your orchestration system, instead of GigaVUE-FM to deploy GigaVUE fabric components. The Third Party orchestration feature allows you to register these fabric components, after deployment, with GigaVUE-FM using the information you provide. After registering, you can set up monitoring sessions and other services in GigaVUE-FM.

Components in Third Party Orchestration

The GigaVUE Cloud Suite for Third Party Orchestration consists of the following components:

- GigaVUE-FM
- UCT-Vs
- UCT-V Controllers
- GigaVUE V Series Proxy
- GigaVUE V Series Nodes

GigaVUE-FM is a key component of the GigaVUE Cloud Suite Cloud solution. GigaVUE-FM is a web-based fabric management interface that provides a single-pane-of-glass to manage and view both physical and virtual network traffic.

What You Need to Do

If you prefer to use the Third Party orchestration deployment option, you need to:

- Install and start GigaVUE-FM on a supported cloud or enterprise platform.
- Launch the fabric components in your environment.
- Register the fabric components with GigaVUE-FM.
- Delete the fabric components from the platform when you no longer need them.

Getting the Images of Components

- Download the component images from the Gigamon Customer Portal
- Get public cloud images from the respective marketplace.

NOTE: Contact Gigamon Technical Support team if your platform doesn't support the available Gigamon images.

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

Components for Third Party Orchestration

The following table provides a brief description of the components that you can deploy using the Third Party orchestration:

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

Component	Description
	The UCT-V is offered as a Debian (.deb), Red Hat Package Manager (.rpm), or Windows package. For details, refer to Install UCT-Vs.
Next generation UCT-V (earlier known as Next Generation G-vTAP Agent)	**Next generation UCT-V** is a lightweight solution that: • Acquires traffic from VMs and improves UCT-V mirroring capability with a lightweight solution. • Reduces the traffic flow from the UCT-V to the V Series node with tap-level prefiltering, lowering the V Series load. • Activates UCT-V on Linux systems with a Kernel version above 5.4. • Allows you to prefilter traffic at UCT-Vs before sending it to V Series nodes. • Allows you to create a prefiltering policy template to apply on a monitoring session.
UCT-V Controller (earlier known as G-vTAP Controller)	• Manages multiple UCT-Vs and orchestrates the mirrored traffic flow to GigaVUE V Series nodes. • GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs.
GigaVUE® V Series Proxy (optional)	• Manages multiple V Series nodes and orchestrates the traffic flow from GigaVUE V Series nodes to the monitoring tools. • GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series nodes.
GigaVUE® V Series Node	GigaVUE® V Series Node is a visibility node that: • Aggregates mirrored traffic from multiple UCT-Vs. • Applies filters and manipulates the packets using GigaSMART applications. • Distributes the optimized traffic to cloud-based tools or backhauls it to GigaVUE Cloud Suite Cloud using GRE or VXLAN tunnels, when the platform supports.

Cloud Overview Page (Third Party Orchestration)

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

This page shows key information at a glance, including:

- Basic statistics
- V Series alarms
- Connection status

- Volume usage vs. allowance
- A summary table of active monitoring sessions

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

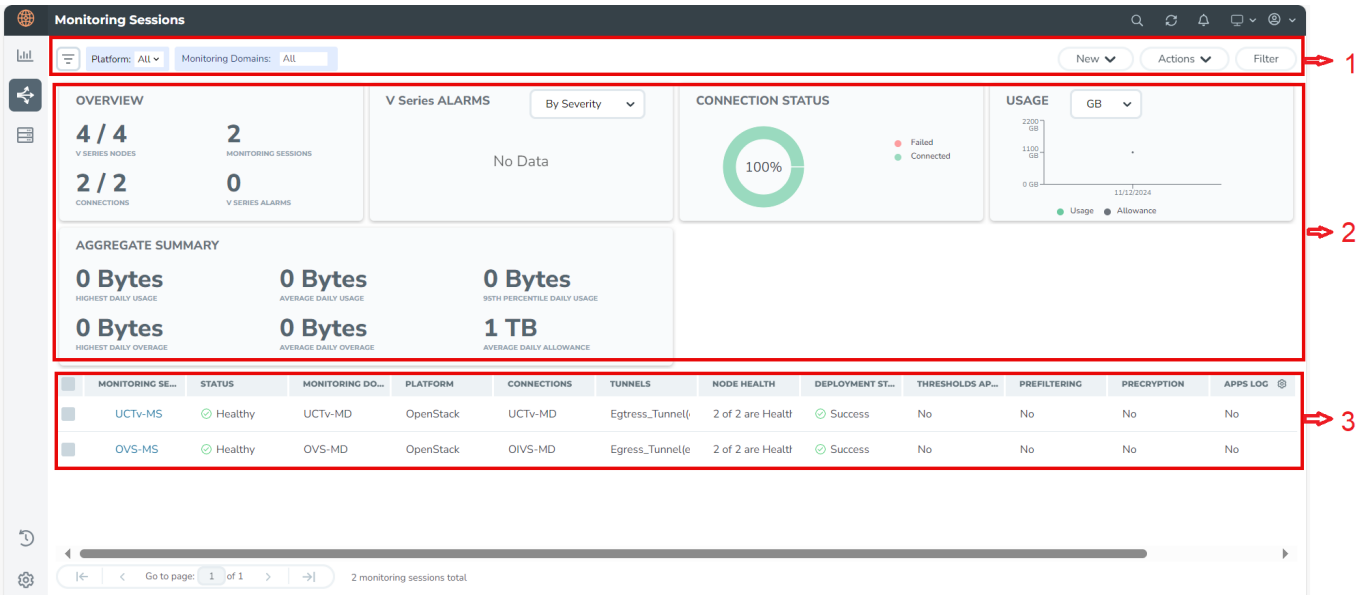
How to Access the Overview Page

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

Perform one of the following:

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

The **Monitoring Sessions** page appears.



Page Layout for Easy Use

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

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

Top Menu

The Top menu consists of the following options:

Options	Description
New	Allows to create a new Monitoring Session and new Monitoring Domain.
Actions	Allows the following actions: • **Edit:** Opens the edit page for the selected Monitoring Session. • **Delete**: Deletes the selected Monitoring Session. • **Clone**: Duplicates the selected Monitoring Session. • **Deploy**: Deploys the selected Monitoring Session. • **Undeploy**: Undeploys the selected Monitoring Session. • **Apply Threshold**: Applies the threshold template created for monitoring cloud traffic health. For details, refer to the *Monitor Cloud* section. • **Apply Policy:** Enables functions like Precryption, Prefiltering, or Secure Tunnel.
Filter	You can filter the Monitoring Session details based on a criterion or a combination of criteria. For more information, refer to Cloud Overview Page (Third Party Orchestration).

Filters

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

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

Filter on the left corner

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

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

Filter on the right corner Filter

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

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

Viewing Charts on the Overview Page

You can view the following charts on the overview page:

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

Overview

This chart shows:

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

V Series Alarms

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

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

Connection Status

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

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

Usage

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

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

Aggregate Summary

This summary shows key volume usage stats:

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

Viewing Monitoring Session Details

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

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

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

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

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

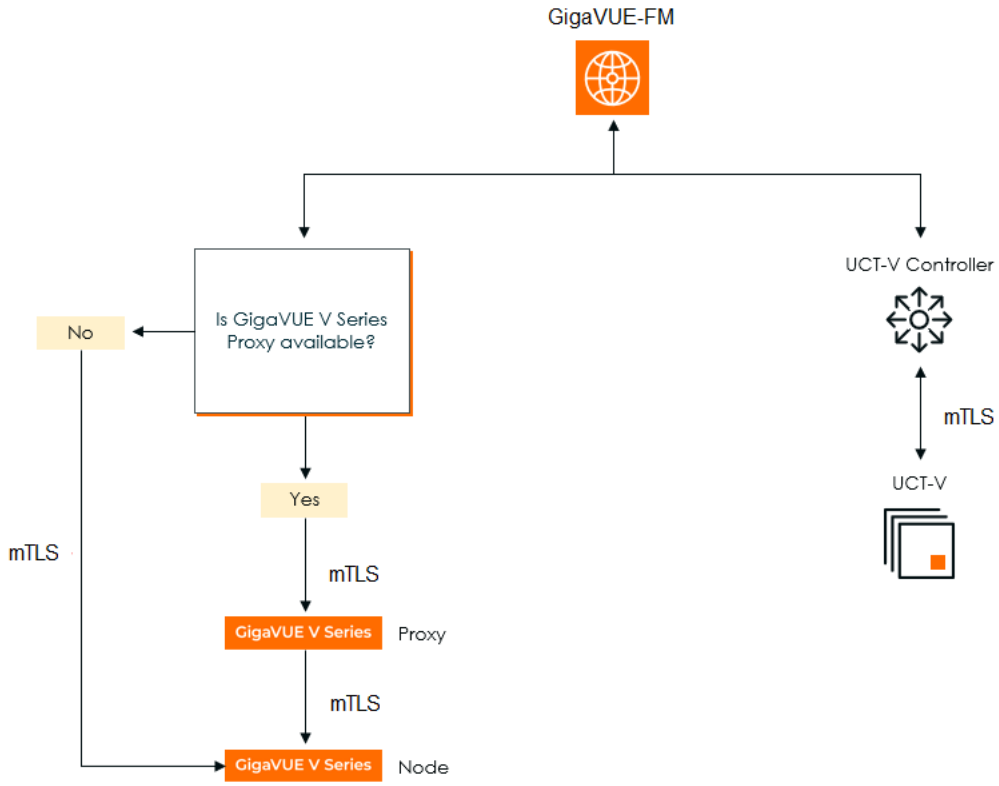
GigaVUE Cloud Suite for Third Party Orchestration supports the following features:

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

Secure Communication between GigaVUE Fabric Components

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

How it Works!



In this setup:

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

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

GigaVUE-FM acts as the PKI

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

Bring Your Own CA

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

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

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

Rules and Notes

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

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

Precryption™

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

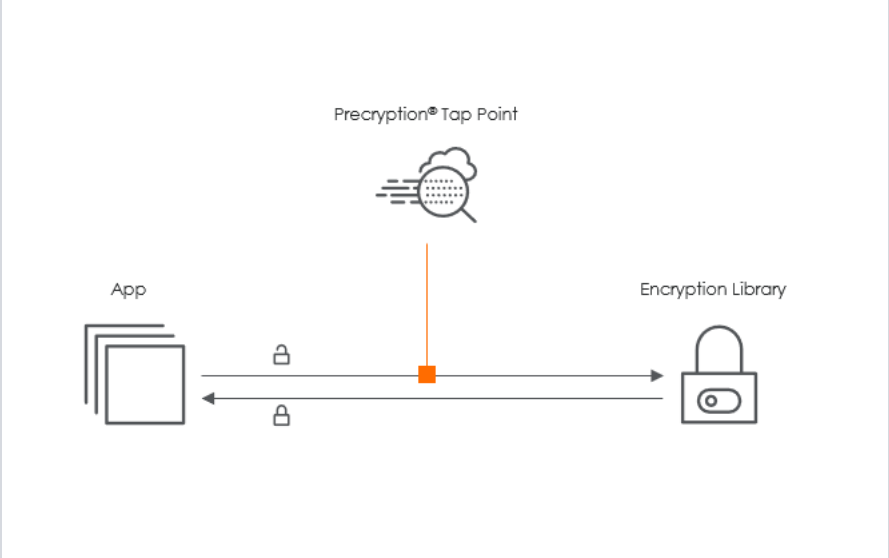
Gigamon Precryption™ technology[1] provides you clear-text visibility into encrypted network traffic without the need for traditional decryption. It works across virtual, cloud, and container environments, helping you get the full security stack without added complexity

In this section:

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



Key Highlights

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

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

Why Gigamon Precryption

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

Precryption helps you:

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

Key Features

The following are the key features of this technology:

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

- Integration with Gigamon Deep Observability Pipeline for the full suite of optimization, transformation, and brokering capabilities.

Key Benefits

The following are the key benefits of this technology:

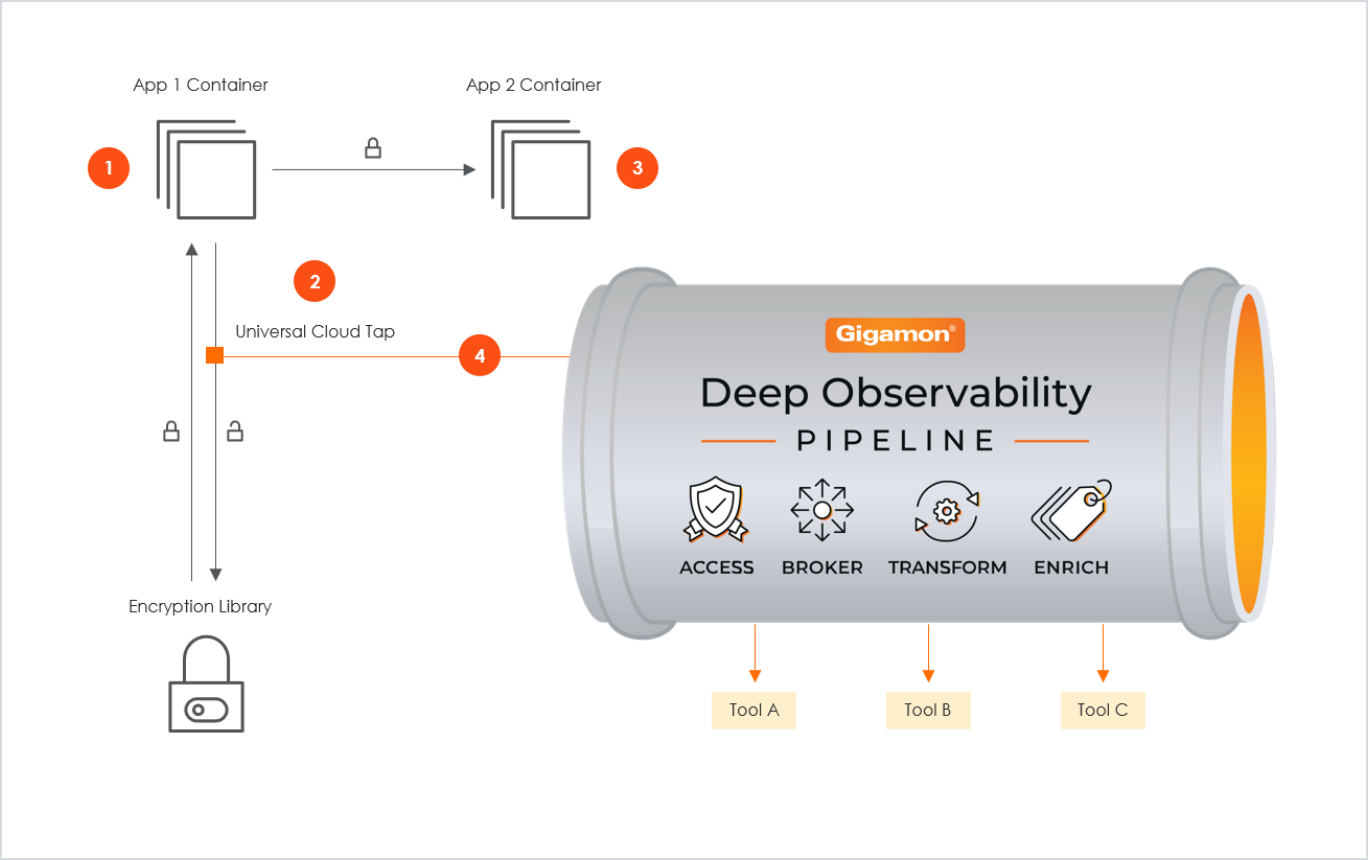
- Eliminates blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.
- Monitors application communications with an independent approach that enhances development team velocity.
- Extends security tools' visibility to all communications,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

How Gigamon Precryption Technology Works

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

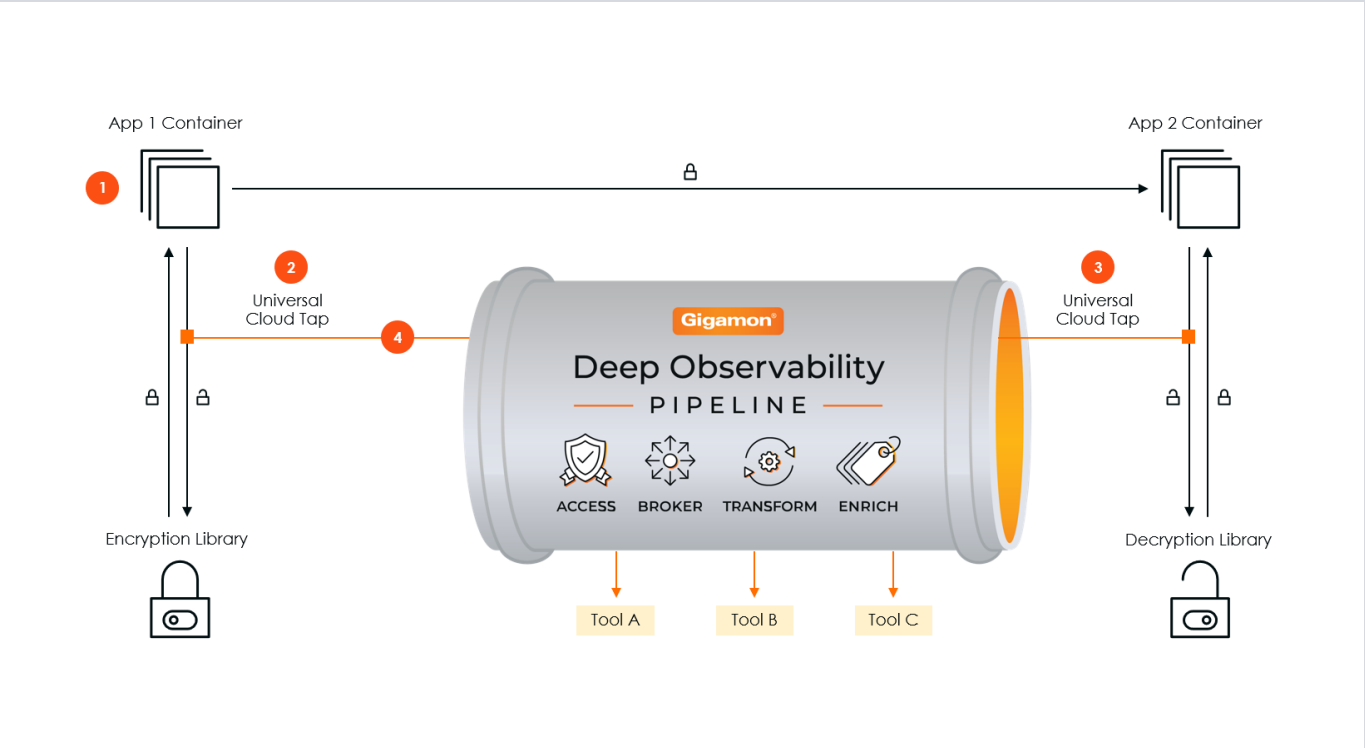
- Precryption Technology on Single Node
- Precryption Technology on Multi-Node

Precryption Technology on Single Node



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

Precryption Technology on Multi-Node



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

Supported Platforms

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

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

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

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

Prerequisites

Points to Note

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

License Prerequisite

- Precryption™ requires a SecureVUE Plus license.

Supported Kernel Version

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

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

For more details, refer to Gigamon TV.

Note

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

Secure Tunnels

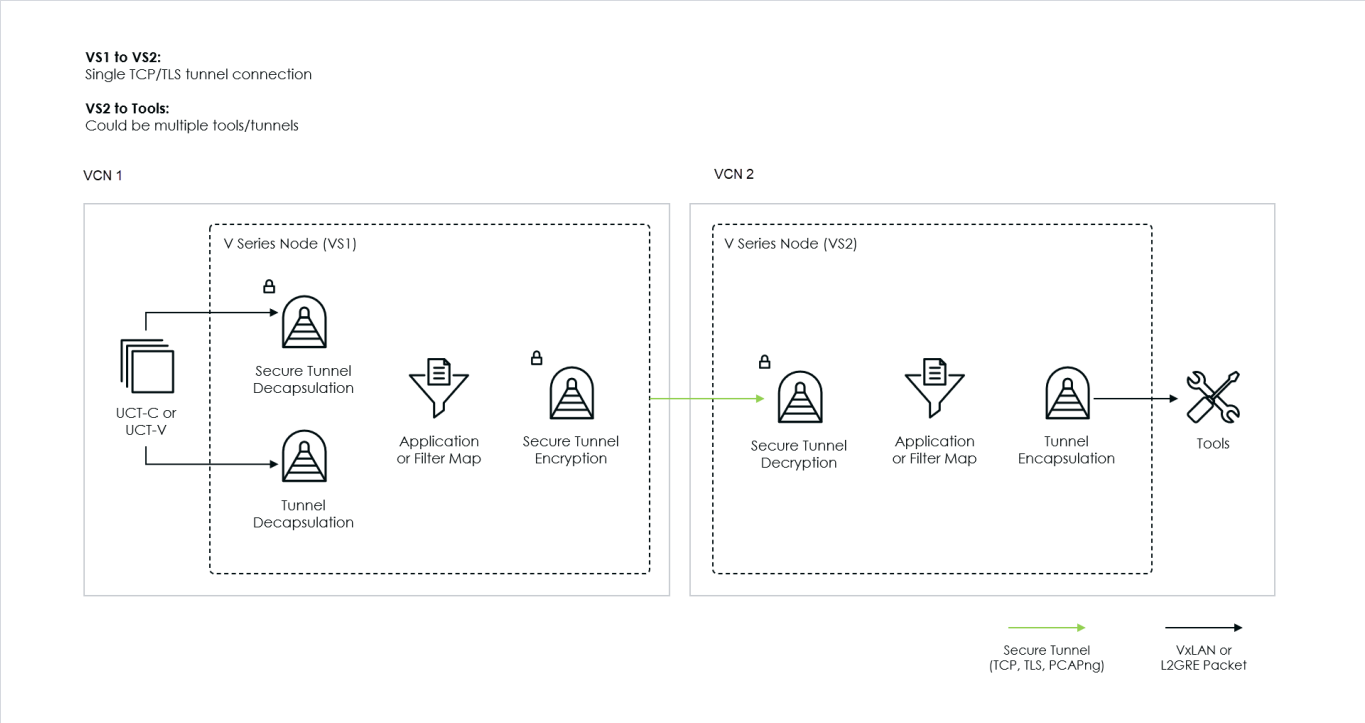
Secure Tunnel transfers the cloud captured packets from one GigaVUE V Series Node to another.

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

How Does it Work!

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

For more information, refer to PCAPng Application.



Supported Platforms

Secure Tunnels are supported on:

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

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

Prefiltering

Prefiltering allows you to filter the traffic at UCT-Vs before sending it to the GigaVUE V Series Nodes.

Create a Prefiltering policy template

In GigaVUE-FM, you can create a prefiltering policy template that includes rules and filter values.

- You can apply the template to multiple monitoring sessions.
- A monitoring session can use only one template at a time.
- You can define a maximum of 16 rules in a monitoring session.

Editing a Monitoring Session

While editing a session, you can modify the policy template with required rules and filter values. These changes apply only to that session. GigaVUE-FM does not save these changes to the template.

Guidelines for prefiltering in Next Generation UCT-Vs are:

- Prefiltering is supported on Next Generation UCT-Vs. It is not available in the classic mirroring mechanism.
- Both Linux and Windows UCT-Vs support Prefiltering.
- A monitoring session supports only one prefiltering policy. All agents in the session use the same policy.
- If multiple monitoring sessions share the same agent, and if one session does not use prefiltering, the system disables prefiltering. It applies a PassAll policy instead and forwards all traffic without filtering.

For details, refer to Configure Precryption in UCT-V

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics [1], you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards.

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

You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects. For details, refer to Analytics.

Rules and Notes:

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

Virtual Inventory Statistics and Cloud Applications Dashboard

Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly.

For details, refer to the Analytics section in *GigaVUE Fabric Management Guide* for details on how to create a new dashboard, clone a dashboard, create a new visualization, and other information about the Discover page and Reports page.

How to access the dashboards

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

The following table lists the various virtual dashboards:

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

Dashboard	Displays	*Visualizations*	Displays
			each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*V Series Node Maximum CPU Usage Trend*	Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour. **Note**: The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V Series nodes do not have service cores, therefore the CPU usage is reported as 0.
		V Series Node with Most CPU Usage For Past 5 minutes	Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes. **Note**: You cannot use the time based filter options to filter and visualize the data.
		V Series Node Rx Trend	Receiving trend of the V Series node in 5 minutes interval, for the past one hour.
		V Series Network Interfaces with Most Rx for Past 5 mins	Total packets received by each of the V Series network interface

Dashboard	Displays	*Visualizations*	Displays
			for the past 5 minutes. **Note**: You cannot use the time based filter options to filter and visualize the data.
		V Series Node Tunnel Rx Packets/Errors	Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation.
		V Series Node Tunnel Tx Packets/Errors	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*Dedup Packets Detected/Dedup Packets Overload*	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload.
		Dedup Packets Detected/Dedup Packets Overload Percentage	Percentage of the de-duplicated packets received against the de-duplication application overload.
		Total Traffic In/Out Dedup	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get	*Tunnel Bytes*	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes. • For input tunnel, transmitted traffic is displayed as zero.

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

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

Dashboard	Displays	*Visualizations*	Displays
	• **Endpoint:** Management IP of the V Series node followed by the Network Interface (NIC)	*Endpoint Packets*	Displays received traffic vs transmitted traffic, as the number of packets.

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

Cloud Health Monitoring

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

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

Customer Orchestrated Source - Use Case

Customer Orchestrated Source is a traffic-acquisition method that tunnels traffic directly to the GigaVUE V Series Nodes. You can use this method to tunnel traffic to the node for processing when you cannot configure UCT-V or VPC Mirroring due to firewall or other restrictions.

In the monitoring session with Customer Orchestrated Source, you can configure tunnels or raw endpoints. You can then use applications like Slicing, Masking, Application Metadata, and Application Filtering to process the tunneled traffic.

For details, see the following:

- Create Ingress and Egress Tunnels
- Create Raw Endpoint (Third Party Orchestration)

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

Get Started with Third Party Orchestration

This chapter describes how to plan and start the Third Party orchestration deployment.

For details, refer to the following sections:

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

License information

GigaVUE Cloud Suite for Third Party Orchestration supports Volume-Based Licensing model.

For details, refer to the following topics:

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

Default Trial Licenses

After installing GigaVUE-FM, you receive a one-time, free 1TB SecureVUE Plus trial Volume-Based License (VBL) for 60 days, starting from the installation date.

This license includes the following applications:

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

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

NOTE: If you do not have any other volume-based licenses installed, the deployed monitoring sessions are undeployed from the existing GigaVUE V Series Nodes after 60 days at the expiration of the trial license.

When you install a new Volume-Based License (VBL), the existing trial license remains active alongside the new VBL. When the trial license period expires, it is automatically deactivated. After deactivation, the trial license moves to the Inactive tab on the VBL page.

License Requirements for Monitoring Sessions

You must use one of the following GigaVUE Cloud Suite™ licenses to deploy any supported application in a Monitoring Session:

- CoreVUE Base Bundle (minimum required)
- NetVUE
- SecureVUE Plus

The default GigaVUE-FM licenses do not provide entitlement for deploying Monitoring Session applications.

The default trial VBL license (SecureVUE Plus) will support deploying applications in Monitoring Sessions only for the duration of the trial license.

Volume-Based License

All the GigaVUE V Series Nodes connected to GigaVUE-FM periodically report statistics on the amount of traffic that flows through the V Series Nodes. The statistics reflect the data volume flowing through the V Series Nodes, with the usage statistics of all licensed applications that run on these nodes.

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

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

Related Information

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

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUE Plus

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

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

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

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

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

Bundle Replacement Policy

Refer to the following notes:

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

Add-on Packages

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

The following add-on SKUs are available:

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

Rules for add-on packages:

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

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

- GigaVUE Cloud Suite for VMware Data Sheet
- GigaVUE Cloud Suite for AWS Data Sheet
- GigaVUE Cloud Suite for Azure Data Sheet
- GigaVUE Cloud Suite for OpenStack
- GigaVUE Cloud Suite for Nutanix

How GigaVUE-FM Tracks Volume-Based License Usage

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

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only applications with active licenses.
- When a license expires, you are notified with an audit log. For more information, refer to the *About Audit Logs* section in the respective GigaVUE Cloud Suite Deployment Guide.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license are not undeployed.
- For releases prior to 6.4:
  - The Monitoring Sessions using the corresponding license are undeployed, but not deleted from the database.
  - Any undeployed monitoring sessions are redeployed when you renew a license or newly import the same.

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

Activate Volume-Based Licenses

To activate Volume-Based Licenses,

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

Manage Volume-Based Licenses

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

View active Volume-Based License

To view active Volume-Based License (VBL):

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

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

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

NOTE: The License Type and Activation ID are displayed by default in the Active tab in the VBL page.

To display the Entitlement ID field, select the column setting configuration option to enable the Entitlement ID field.

View Inactive Volume-Based License

To view inactive Volume-Based License (VBL):

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

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

Field	Description
SKU	Unique identifier associated with the license.
Bundle	Bundle to which the license belongs to.
Ends	License end date.
Deactivation Date	Date the license got deactivated.
Revocation Code	License revocation code.
Status	License status.

NOTE: The License Type, Activation ID and Entitlement ID fields are not displayed by default in the Inactive tab of VBL page. To display these fields, select the column setting configuration option and enable these fields.

Activate Volume-Based Licenses

To activate Volume-Based Licenses,

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

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

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

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

Network Firewall Requirement

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

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

GigaVUE FM

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

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

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

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

UCT-V Controller

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

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

UCT-V

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

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9902	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller.
Inbound	TCP	8301	UCT-V Controller IP	Allows UCT-V to receive the ACME challenge requests from the UCT-V Controller.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	UDP (VXLAN)	VXLAN (default 4789)	GigaVUE V Series Node IP	Allows UCT-V to tunnel VXLAN traffic to GigaVUE V Series Nodes.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	GigaVUE V Series Node IP	Allows UCT-V to tunnel L2GRE traffic to GigaVUE V Series Nodes.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	GigaVUE V Series Node IP	Allows UCT-V to securely transfer the traffic to the GigaVUE V Series Node.
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V to send traffic health updates to UCT-V Controller.
Outbound (This is the port used for Third Party Orchestration)	TCP	8892	UCT-V Controller IP	Allows UCT-V to receive the registration requests and heartbeat to UCT-V Controller.
Outbound	TCP	8300	UCT-V Controller IP	Allows UCT-V to receive ACME validation flow from UCT-V Controller.

GigaVUE V Series Node

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

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8889	GigaVUE-FM IP	Allows GigaVUE V Series Node to communicate control and

				management plane traffic with GigaVUE-FM.
Inbound	TCP	8889	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	UDP (VXLAN)	VXLAN (default 4789)	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive VXLAN tunnel traffic to UCT-V.
Inbound	IP Protocol (L2GRE)	L2GRE	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive L2GRE tunnel traffic to UCT-V.
Inbound	UDPGRE	4754	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from UDPGRE Tunnel.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Node to receive the ACME challenge requests from GigaVUE-FM.
Inbound	TCP	80	GigaVUE V Series Proxy IP	Allows UCT-V to receive the ACME challenge requests from the GigaVUE V Series Proxy.
Inbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	UCT-V subnet	Allows to securely transfer the traffic to GigaVUE V Series Nodes.
Inbound (Optional - This port is used only for configuring AWS Gateway Load Balancer)	UDP (GENEVE)	6081	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from AWS Gateway Load Balancer.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM.
Outbound	UDP (VXLAN)	VXLAN (default 4789)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	UDP	2056	GigaVUE-FM IP	Allows GigaVUE V Series Node to send Application Intelligence

				and Application Visualization reports to GigaVUE-FM.
Outbound	UDP	2055	Tool IP	Allows GigaVUE V Series Node to send NetFlow Generation traffic to an external tool.
Outbound	UDP	8892	GigaVUE V Series Proxy	Allows GigaVUE V Series Node to send certificate request to GigaVUE V Series Proxy IP.
Outbound	TCP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	• echo request • echo reply	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE-FM when GigaVUE V Series Proxy is not used.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	Tool IP	Allows to securely transfer the traffic to an external tool.

Giga VUE V Series Proxy(Optional)

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

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

				configured params and provides the certificate using those parameters.
Inbound	TCP	8892	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate control and management plane traffic with GigaVUE V Series Node.

UCT-C Controller - deployed in Kubernetes worker mode

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

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

Ports for Backward Compatibility

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

UCT-V Controller

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

Direction	Protocol	Port	Source CIDR	Purpose
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests from UCT-V.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs.

GigaVUE V Series Node

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

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

GigaVUE V Series Proxy(Optional)

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

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

GigaVUE-FM Version Compatibility

GigaVUE-FM version 6.14.00 supports the latest version (6.14.00) of GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, and UCT-V, as well as (n-2) versions. For better compatibility, we recommend to use the latest version of fabric components with GigaVUE-FM.

Configure Role-Based Access for Third Party Orchestration

Before deploying the fabric components using a third-party orchestrator, you need to create the required users, roles, and user groups in GigaVUE-FM.

To deploy fabric components through your orchestrator, you can use the username and password from the User Management page in the registration data.

For detailed steps, refer to the following topics:

- Users
- Role
- User Groups

Users

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

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
    - **Name:** Actual name of the user
    - **Username**: User name configured in GigaVUE-FM
    - **Email**: Email ID of the user
    - **Password/Confirm Password**: Password for the user.
    - **User Group:** Select the desired User Group to associate the user.

    GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Role

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

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

To create a role:

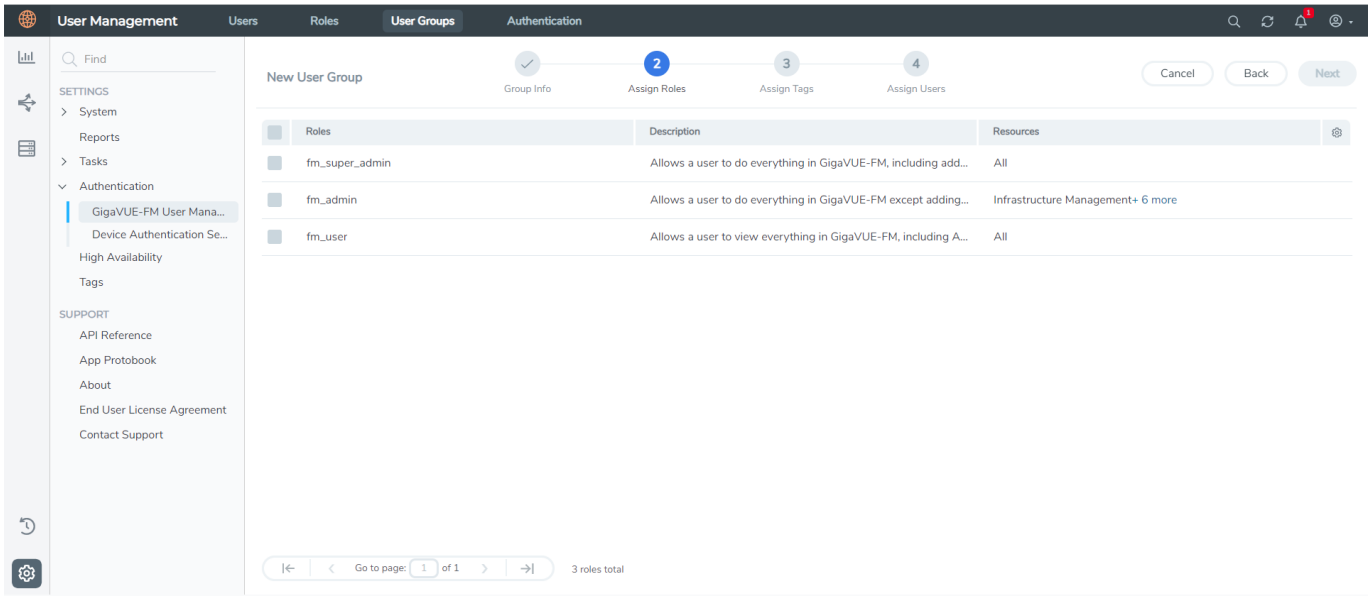
1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select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

User Groups

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

To create a new user group,

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



3. In the Wizard, perform the following steps.

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

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

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

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

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

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

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

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

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

Select the ellipses to perform the following operations:

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

Configure Tokens

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

This feature generates tokens to verify the identity of a user for accessing theGigaVUE-FM

If you are authenticated, GigaVUE-FM allows you to generate a token based on your access privileges. You can copy the generated tokens from the GUI to access the REST APIs. Token inherits the read or write Role-Based Access (RBAC) privileges of the groups assigned to its user.

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

Prerequisite

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

Rules and Notes

- Token authentication is an additional mechanism to access GigaVUE-FM REST APIs without replacing the existing GigaVUE-FM authentication mechanism.
- Only authenticated users can create tokens.
- A token expires or becomes invalid in the following cases:
    - The token reaches the configured expiry or default period. The default value is 30 days, and the maximum value is 105 days.
    - You delete a user group associated with the token.
    - You change the password of the local user who owns the token.
    - You change the authentication type. GigaVUE-FM deletes all tokens when this occurs.
- When you back up and restore of the GigaVUE-FM, previously generated tokens become unavailable.
- During an FMHA role changeover, active GigaVUE-FM tokens are active.
- For basic authentication, GigaVUE-FM restricts activities such as creating, revoking, and reviewing of Token APIs.
- If you use an expired or invalid token, GigaVUE-FM returns a 401 Unauthorized error when accessing the REST API.

This section explains about the following:

- Create Token
- Revoke Tokens
- Export Token
- Create a Token with Custom User Group

Create Token

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

To create a token,

1. Go to , select **Authentication** > **GigaVUE-FM User Management**.

   The **User Management** page appears.
2. In the **User Management** page, select **Tokens**.

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

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

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

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

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

Revoke Tokens

You can revoke tokens that other users create only if you have write access in GigaVUE-FM Security Management.

To revoke tokens,

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

3. From the drop-down list, select **Token Management**.
4. You can view the token created by other users.
5. Select the token that you want to revoke.
6. Select **Action**, and then select **Revoke**.

Export Token

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

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

Create a Token with Custom User Group

GigaVUE-FM allows you to create a token with different user groups.

To create a token,

1. Create a custom user.

   NOTE: Do not assign this user to any existing user group.

   - **Example**: orchestration
2. Set up a custom role with the required permissions.
   - **Example**: orchestrationRole
   - Assign “Third Party Orchestration” with write permission
3. Create a user group, assign the custom role to it, and add the user to the group.
   - **Example**: orchestrationGroup
   - Assign the orchestration Role to this group.
   - Add the orchestration user to this group.
4. Log in to GigaVUE-FM using the custom user, go to the token page, and select the custom group.

The token is generated.

Modes of Deployments

Using a third-party orchestration, you can deploy GigaVUE fabric components in one of the two modes:

- Generic Mode
- Integrated Mode

Generic Mode

In generic mode, when deploying the fabric components, you can directly provide the monitoring domain and connection name in your orchestrator.

You can use one of the two options:

- Let your orchestrator create a monitoring domain automatically in GigaVUE-FM under the **Third Party Orchestration** monitoring domain page. Your GigaVUE fabric components are deployed in that monitoring domain.
- Manually create the monitoring domain in GigaVUE-FM under Third Party Orchestration, and then include the monitoring domain name and connection name in your orchestrator's user data.

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

Integrated Mode

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

In integrated mode, the platform credentials are shared with GigaVUE-FM. Only deployment of the GigaVUE fabric components takes place on the platform.

Deployment Options for GigaVUE Cloud Suite for Third Party Orchestration

This topic provides details on how you can configure GigaVUE Cloud Suite for Third Party Orchestration in multiple ways to gain visibility into both physical and virtual traffic. The configuration options depend on two factors:

- The traffic acquisition method
- The deployment method for fabric components

GigaVUE-FM supports five deployment options based on these variables.

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

Deploy GigaVUE Fabric Components using Generic Mode

You can deploy GigaVUE fabric components using generic mode using one of the four options.

Without Creating Monitoring Domain

In generic mode, when deploying the fabric components, you can provide the monitoring domain and connection name directly in your orchestrator.

- A Monitoring Domain is created under the **Third Party Orchestration** monitoring domain page in GigaVUE-FM.
- Your GigaVUE fabric components is deployed in that monitoring domain.

Traffic Acquisition Method as UCT-V

Use UCT-V to acquire traffic directly from virtual machines and send it to GigaVUE V Series Nodes. Follow the instructions in the table below to configure UCT-V as your traffic acquisition method.

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

Step No	Task	Refer the following topics
		Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as Customer Orchestrated Source

Use Customer Orchestrated Source to tunnel traffic directly to GigaVUE V Series Nodes without deploying UCT-V or its controllers. Follow the instructions in the table below to configure this traffic acquisition method using tunnels as the source.

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

By Creating Monitoring Domain

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

Traffic Acquisition Method as UCT-V

Use UCT-V to acquire traffic from virtual machines and forward it to GigaVUE V Series Nodes. Follow the configuration steps in the table below to set up UCT-V as your traffic acquisition method.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Install UCT-V	Install UCT-V
3	Create User and Password	Configure Role-Based Access for Third

Step No	Task	Refer the following topics
		Party Orchestration
4	Create a Monitoring Domain	Create Monitoring Domain
5	Configure GigaVUE Fabric Components	Deploy Fabric Components using Generic Mode
6	Create Monitoring session	Configure Monitoring Session
7	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
8	Deploy Monitoring Session	Deploy Monitoring Session
9	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as Customer Orchestrated Source

Use Customer Orchestrated Source to tunnel traffic directly to GigaVUE V Series Nodes, without deploying UCT-V or its controllers. Refer to the table below for detailed instructions on how to configure this method using tunnels as the traffic source.

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

Deploy GigaVUE Fabric Components using Integrated Mode

In integrated mode, GigaVUE-FM allows you to use your cloud platform as an orchestrator to deploy GigaVUE fabric components. After deployment, you use GigaVUE-FM to configure and manage advanced features supported by the nodes.

How It Works

- Create a monitoring domain in your GigaVUE Cloud Suite within GigaVUE-FM.
- Use your cloud orchestration system to deploy the GigaVUE V Series Nodes.
- GigaVUE-FM automatically detects and displays the deployed nodes under the specified monitoring domain.

NOTE: Make sure the monitoring domain and connection name in GigaVUE-FM match the groupName and subGroupName values in your orchestrator's user data.

Refer to the table below for instructions.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Create User and Password in GigaVUE-FM.	Configure Role-Based Access for Third Party Orchestration
3	Install UCT-V	Install UCT-V
4	Create a Monitoring Domain **Note**: Ensure that the Use FM to Launch Fabric toggle button is disabled.	Refer to the *Create Monitoring Domain* section in the respective cloud guide.
5	Configure GigaVUE Fabric Components **Note**: Select UCT-V as the Traffic Acquisition Method. When using integrated mode you can only use UCT-V as the traffic acquisition method.	Deploy Fabric Components using Integrated Mode
6	Create Monitoring session	Configure Monitoring Session
7	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
8	Deploy Monitoring Session	Deploy Monitoring Session
9	View Monitoring Session Statistics	View Monitoring Session Statistics

Deploy GigaVUE Cloud Suite for Third Party Orchestration

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

This feature lets you launch and register fabric components with GigaVUE-FM using the information you provide. After registration, you can configure monitoring sessions and related services in GigaVUE-FM.

Deployment Options

You can deploy fabric components using two options:

- **Manual Deployment:** Use a configuration file to launch and register the components.
- **Automated Deployment:** Use your orchestration portal to launch instances. Supply user data to deploy and register the components automatically.

In both cases, the fabric components use the information you provide to register with GigaVUE-FM.

GigaVUE-FM uses the group name and subgroup name in the user data to place the components in the correct monitoring domain and connection.

Each node sends heartbeat messages to GigaVUE-FM that uses them to monitor the health status of the nodes.

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

- Install GigaVUE-FM
- Install UCT-V
- Uninstall UCT-V
- Upgrade or Reinstall UCT-V
- Adding Certificate Authority
- Create Monitoring Domain
- Deploy Fabric Components using Generic Mode
- Deploy Fabric Components using Integrated Mode

Install GigaVUE-FM

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

After you deploy GigaVUE-FM complete an initial configuration before you start using GigaVUE-FM. For more information, refer to the *GigaVUE-FM Installation and Upgrade Guide*.

To install GigaVUE-FM in your cloud environment, refer to the following topics:

Install UCT-V

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

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

The Workflow

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

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

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

Supported Platforms

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

- AWS
- Azure
- OpenStack

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

- AWS
- Azure
- OpenStack
- VMware ESXi
- VMware NSX-T

Refer to the following sections for more information:

- Supported Operating Systems for UCT-V
- Linux UCT-V Installation
- Windows UCT-V Installation

Supported Operating Systems for UCT-V

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

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

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

GigaVUE-FM version 6.14 supports UCT-V version 6.14 as well as (n-2) versions. We recommend to use the latest version of UCT-V with GigaVUE-FM for better compatibility.

Linux UCT-V Installation

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

Refer to the following sections:

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

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

Single Network Interface Configuration

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

Example

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

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

Sample Configuration

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

Grant permission to monitor ingress and egress traffic at iface

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

Multiple Network Interface Configuration

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

Example

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

In the UCT-V configuration, you can configure:

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

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

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

Grant permission to monitor ingress and egress traffic at iface

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

```
# eth1 mirror-dst
```

Loopback Network Interface Configuration

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

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

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

Linux Network Firewall Requirements

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

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

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

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

Install Linux UCT-Vs

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

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

Prerequisites

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

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

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

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

Install Linux UCT-Vs using Installation Script

Using installation script, you can complete installation.

Perform the following steps:

1. **To install UCT-V from Ubuntu/Debian:**
    a. Download the UCT-V**6.14.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
    b. Copy this package to your instance and Install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
    $ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
    ```

2. **To install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS:**
    a. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
    b. Copy this package to your instance and install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    $ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    ```

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

```
sudo uctv-wizard
```

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

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

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

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

Notes:

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

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

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

  ```
  sudo uctv-wizard help
  ```

Linux UCT-V Installation Scenarios

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

Install Linux UCT-Vs using Manual Configuration

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

Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

1. Download the UCT-V**6.14.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance.

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

```
$ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance.
3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
$ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
$ sudo service uctv status
```

Notes:

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

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

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

Post Deployment Check:

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

1. Enter the command:

   ```
   sudo uctvl uctv-show
   ```

2. Manually execute the following command:

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

Register Linux UCT-V

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

Third Party Orchestration: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of the user to register with GigaVUE-FM. You can register UCT-V toGigaVUE-FM using Third Party Orchestration with the following two modes:

- Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
- Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

For more information, refer to Modes of Deployment section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

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

Windows UCT-V Installation

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

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

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

Windows Network Firewall Requirements

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

Notes:

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

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

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

Install Windows UCT-Vs

Rules and Notes:

- VXLAN is the only tunnel type supported for Windows UCT-V.
- Loopback Interface is not supported for Windows UCT-V.
- Before registering Windows UCT-V, generate a token and place it in the **C:\ProgramData\uctv\gigamon-cloud.conf** configuration file. Refer to Configure Tokens.
- Do not manually edit the UCT-V Windows service registry settings. Use the supported installation and upgrade workflows instead.

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

- Install Windows UCT-Vs using Installation Script

- Install Windows UCT-Vs using Manual Configuration

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

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

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V**6.14.00** MSI package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator**.
   The UCT-V service starts automatically.

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

   ```
   uctv-wizard
   ```

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

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

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

Notes:

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

```
uctv-wizard help
```

Windows UCT-V Installation Scenarios

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

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V**6.14.00** MSI package from the Gigamon Customer Portal. For assistance, contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator**. The UCT-V service starts automatically.

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

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

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

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

   For IPv4:

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

   For IPv6:

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

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

   For IPv4:

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

   For IPv6:

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

4. Save the file.

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

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

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

Register Windows UCT-V

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

Third Party Orchestration: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of user to register with GigaVUE-FM.
UCT-V can register with GigaVUE-FM using Third Party Orchestration in one of the following two modes:

- Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
- Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

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

Uninstall UCT-V

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

Uninstallation Method

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

- Use the following command: **`CMD uctv-wizard uninstall`**

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

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

Upgrade or Reinstall UCT-V

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

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

Refer to the below sections for detailed information and instructions.

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

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

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

Refer to the sections below for details and instructions:

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

Rules and Notes:

- Upgrade is allowed only to versions 6.9.00 or later. Ensure that the UCT-V Controller version is compatible with the version to which you are upgrading.
- Do not trigger system upgrades or other upgrades at the same time as the UCT-V upgrade.
- You should have Infrastructure Management permission to upgrade the UCT-Vs.
- Currently, you can upgrade the UCT-Vs to n+2 versions and any number of patch releases through GigaVUE-FM.
- Before you proceed with the upgrade, ensure that the UCT-Vs are in a healthy state.

- Make sure that a UCT-V is performing only one active job at a time. If the selected UCT-V is part of another job, you cannot trigger the immediate job using the same UCT-V.
- You must upload a compatible image type to upgrade the UCT-V; otherwise, the UCT-V is rejected for the upgrade job.
- Upgrade through GigaVUE-FM is not applicable to OVS Modules. For OVS tapping, you should upgrade the UCT-Vs manually.

Upload the UCT-V Images

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

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

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

Delete the file

You can delete one or multiple images.

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

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

Upgrade the UCT-V

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

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

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

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

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

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

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

Upgrade UCT-V Manually

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

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

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

Integrate Private CA

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

Rules and Notes

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

To integrate private CA

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

Generate CSR

To create an intermediate CA certificate:

1. Go to > **System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list, select **CSR**. The **Generate Intermediate CA Certificate** page appears.
3. Enter details in the following fields:
   - **Country:** Enter the name of your country.
   - **Organization**: Enter the name of your organization.
   - **Organization Unit:** Enter the name of the department or unit.
   - **Common Name**: Enter the common name associated with the certificate.
4. From the **Algorithm** drop-down list, select the desired encryption algorithm used to encrypt your private key.
5. Select **Generate CSR**.

The CSR is downloaded successfully.

Upload CA Certificate

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

To upload the signed CA certificate to GigaVUE-FM:

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

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

Adding Certificate Authority

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

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

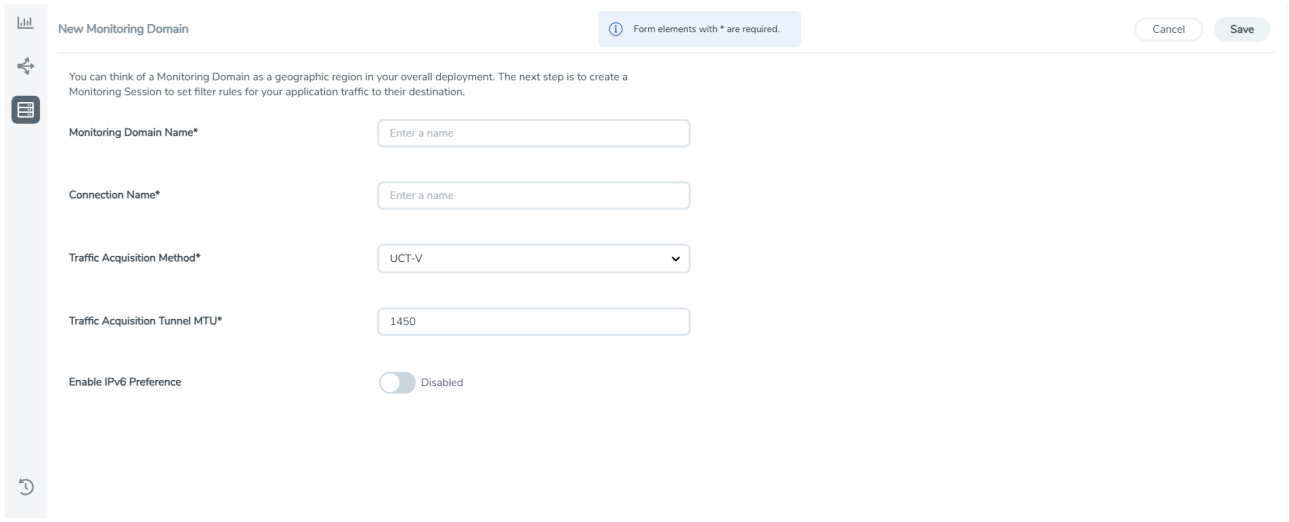
To upload the CA Certificate chain using GigaVUE-FM, follow these steps:

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

Create Monitoring Domain

To create a monitoring domain in Third Party Orchestration:

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



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

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

4. Click **Save**.

Notes:

- Ensure that all V Series Nodes within a single Monitoring Domain are running the same version. Mixing different versions in the same Monitoring Domain may lead to inconsistencies when configuring Monitoring Session traffic elements.
- Similarly, when upgrading a V Series Node, ensure that the GigaVUE-FM version is the same or higher than the V Series Node version.

From the Monitoring Domain page, use the Actions dropdown list in the top-right corner to perform the following actions:

Actions	Description
Manage Certificates	You can use this button to perform the following actions: • **Re-issue**- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments. • **Renew**- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime. Auto-renewal is performed based on the duration specified in the **Certificate Settings** page. Refer to Configure Certificate Settings for more details.
Edit Monitoring Domain	Use to edit a monitoring domain.
Delete Monitoring Domain	Use to delete a Monitoring Domain.
Edit SSL Configuration	Use to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Generate Sysdump	You can select one or multiple GigaVUE V Series Nodes (Maximum 10) to generate the system files. The generation of sysdump takes a few minutes in a GigaVUE V Series Node. You can proceed with other tasks, and upon completion, the status appears in the GUI. These system files are helpful for troubleshooting. For more information, refer to Debuggability and Troubleshooting.
Download Cloud Configuration File	Use this option to download the cloud configuration file (for example, md_gigamon-cloud.conf). The file contains monitoring domain connection details such as groupName, subGroupName, and token, and can be used to register fabric components in GigaVUE-FM using third party orchestration. For more information on registration of fabric components, refer to Deploy GigaVUE Cloud Suite for Third Party Orchestration.

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

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

Edit SSL Configuration

You can add certificate authority and SSL keys to your fabric components after deploying it.

To add certificate authority and SSL keys when using secure tunnels,

1. Go to **Inventory > VIRTUAL > Third Party Orchestration**.
2. Select **Monitoring Domain**.

   The **Monitoring Domain** page appears.
3. From the page, select the desired monitoring domain to add the SSL key.
4. From the **Actions** drop down list, select **Edit SSL Configuration**.

   An **Edit SSL Configuration** window appears.
5. From the **UCT-V Agent Tunnel CA** drop down list, select **CA**.
6. From the **V Series Node SSL key** drop down list, select the SSL key.
7. Select **Save**.

Deploy Fabric Components using Generic Mode

In Generic Mode, you can deploy GigaVUE V Series Nodes using your own orchestration system. Provide the monitoring domain name and connection name in the user data during deployment.

GigaVUE-FM automatically creates the Monitoring Domain under the **Third Party Orchestration** monitoring domain page. It assigns the deployed fabric components to that domain after the deployment completes.

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

- Configure and Deploy GigaVUE Fabric Components using AWS - Generic Mode
- Configure and Deploy GigaVUE Fabric Components using Azure - Generic Mode
- Configure GigaVUE Fabric Components using GCP
- Configure GigaVUE Fabric Components using Nutanix
- Configure GigaVUE Fabric Components using OpenStack

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

Configure and Deploy GigaVUE Fabric Components using AWS - Generic Mode

This section provides instructions on how to register GigaVUE fabric components using AWS EC2 or a configuration file.

Recommended Instance Type

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

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

Deployment Guidelines

Points to remember before deploying the fabric components using generic mode:

- Set the correct MTU for tunnels: Use 8950 for IPv4 tunnels and 8930 for IPv6. To update the Traffic Acquisition Tunnel MTU:

    1. Select the monitoring domain.
    2. Select the **Edit Monitoring Domain** option.
    3. Enter the **Traffic Acquisition Tunnel MTU** value and select **Save**.

    NOTE: Set the correct MTU before deploying the Monitoring Session. If not, you must undeploy and redeploy the session after updating the MTU.

- When deploying the fabric components using generic mode, you must use subGroupName in the registration data as the connection name.
- You can also create a Monitoring Domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. For details, refer to Create Monitoring Domain.
- You can use only **UCT-V** or **Customer Orchestrated Source** as the traffic acquisition method when using generic mode.
- When you deploy the fabric components using Third Party Orchestration, you cannot delete the Monitoring Domain without unregistering the registered fabric components.

- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in AWS. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to Configure Tokens .
- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For details, refer to the Configure Role-Based Access for Third-Party Orchestration section in the v6.9 Documentation.

In your AWS EC2, you can configure the following GigaVUE fabric components:

Configure UCT-V Controller in AWS

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

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

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

Register UCT-V Controller during Instance Launch

In your AWS EC2 portal, you can launch the UCT-V Controller AMI instance and register UCT-V Controller using user data.

Perform the following steps:

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.

2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The UCT-V Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteAddress: <IP address of the GigaVUE-FM>
        sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
        remotePort: 443
```

3. Go to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

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

Register UCT-V Controller after Instance Launch

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

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

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC deployments
to specify which UCT-V Controller interface to use for communicating with GigaVUE-FM.)
    remotePort: 443
```

3. Restart theUCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

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

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

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

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

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   $ sudo netplan apply

6. Restart the UCT-V Controller service.

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

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

Configure UCT-V in AWS

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

You need to register UCT-V through the registered UCT-V Controller. It communicates through PORT 8891.

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

To register UCT-V using a configuration file, follow the steps:

1. Install the UCT-V in the Linux or Windows platform. For details, 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.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, follow the steps given below:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, click **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

   ```
   Registration:
       groupName: <Monitoring Domain Name>
       subGroupName: <Connection Name>
       token: <Token>
       remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
   Controller 2>
       sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
   specify which UCT-V interface to use for communicating with the UCT-V Controller.)
   ```

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

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

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

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

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

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

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

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

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

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

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

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

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

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

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

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

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

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

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

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

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

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

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

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   $ sudo netplan apply

6. Restart the GigaVUE V Series service.

   $ sudo service vseries-node restart

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

Configure and Deploy GigaVUE Fabric Components using Azure - Generic Mode

This topic provides instruction on how to register GigaVUE fabric components using Azure Portal or a configuration file.

Recommended Instance Type

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

NOTE: Additional instance types are supported. You can choose the instance type that best fits your deployment needs. If you're unsure which instance to select, contact Support, Sales, or Professional Services for deployment optimization.

Product	Instance Type	vCPU	RAM	Disk Size
GigaVUE V Series Node	Standard_D4s_v4	4 vCPU	16GB	10GB
	Standard_D8S_V4	8 vCPU	32GB	10GB
GigaVUE V Series Proxy	Standard_B1s	1 vCPU	1GB	
UCT-V Controller	Standard_B4ms	4 vCPU	16GB	4GB

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

Deployment Best Practices

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

- Set the correct MTU for tunnels: Use 1450 for IPv4 tunnels and 1430 for IPv6. To update the Traffic Acquisition Tunnel MTU:
    1. Select the monitoring domain.
    2. Select the **Edit Monitoring Domain** option.
    3. Enter the **Traffic Acquisition Tunnel MTU** value and select **Save**.

    NOTE: Set the correct MTU before deploying the Monitoring Session. If not, you must undeploy and redeploy the session after updating the MTU.

- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to Create Monitoring Domain for more detailed information on how to create monitoring domain under third party orchestration.
- When creating virtual machine for deploying the fabric components in Azure, **SSH public key** must only be used as the **Authentication type** in Azure.
- Create tokens in the **User Management** page in GigaVUE-FM. Refer to Configure Tokens for more detailed information.
- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For more details, refer to the *Configure Role-Based Access for Third-Party Orchestration* section in the 6.9 Documentation.

Prerequisites

Ensure that GigaVUE V Series Node has at least have two Networks Interfaces (NIC) attached to it:

- A management NIC
- A data NIC with Accelerated Networking enabled.

When creating a virtual machine for GigaVUE V Series Node using CLI, you can attach Management NIC and Data NIC at the time of the virtual machine creation. However, if you are using Azure GUI to create the virtual machine for GigaVUE V Series Node, then you can attach the data NIC only after creating the virtual machine.

For details, refer to the following topics:

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

NOTE:

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

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

1. Create the management NIC.

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

2. Create data NIC with Accelerated Networking enabled.

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

3. CreateGigaVUE V Series Node virtual machine using the above NICS.

   ```
   az vm create --resource-group <Resource group> --size <Standard_D4s_v4/Standard_D8S_V4> --name <GigaVUE V Series Node> --admin-username gigamon --generate-ssh-keys --image gigamon-inc:gigamon-gigavue-cloud-suite-v2:vseries-nodev6.13.00:6.13.00 --plan-name vseries-node-v6.13.00 --plan-product gigamon-gigavue-cloud-suite-v2 --plan-publisher gigamon-inc --nics <Management NIC and Data NIC>
   ```

NOTE: You can use the following command to view all the images from Gigamon.

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

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

Enable Management NIC when creating the GigaVUE V Series Node virtual machine.

For details, refer to the Create virtual machine topic in Azure Documentation.

Perform the following steps to attach the data NIC:

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

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

Configure UCT-V Controller in Azure

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

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

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

Register UCT-V Controller during Virtual Machine Launch

In your Azure portal, you canlaunch the UCT-V Controller init virtual machine and register UCT-V Controller using custom data,

Perform the following steps:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detais , refer to Create virtual machine topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The UCT-V Controller uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteAddress: <IP address of the GigaVUE-FM>
        sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
        remotePort: 443
```

The UCT-V Controller deployed in your Azure portal appears on the Monitoring Domain page ofGigaVUE-FM.

Register UCT-V Controller after Virtual Machine Launch

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

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

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
deployments to specify which UCT-V Controller interface to use for communicating with
GigaVUE-FM.)
    remotePort: 443
```

3. Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

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

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

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

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

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

Example netplan config:
```

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   ```
   $ sudo netplan apply
   ```

6. Restart the UCT-V Controller service.

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

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

Configure UCT-V in Azure

You need to register UCT-V through the registered UCT-V Controller. It communicates through PORT 8891.

NOTE: Deployment of UCT-Vs through third-party orchestrator is supported on both Linux and Windows platforms. For details, refer to Linux UCT-V Installation and Windows UCT-V Installation.

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

Register UCT-V during Virtual Machine Launch

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

In your Azure portal, you can launch the UCT-V init virtual machine and register the UCT-V using custom data,

Perform the following steps:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then, **Create a Virtual Machine** Page appears. For details, refer to Create virtual machine topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The UCT-V uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
         groupName: <Monitoring Domain Name>
         subGroupName: <Connection Name>
         token: <Token>
         remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
         sourceIP: <IP address of UCT-V> (Optional Field)
```

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

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

Register UCT-V after Virtual Machine Launch

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

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

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

3. Edit the local configuration file and enter the following custom data.

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, follow the steps given below:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, click **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
    sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
```

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

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

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

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

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

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

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

- Configure and Deploy GigaVUE Fabric Components using Azure - Generic Mode
- Register UCT-V Controller after Virtual Machine Launch

IMPORTANT: You must enable the basic authentication for launching GigaVUE V Series Nodes and GigaVUE V Series Proxy version 6.9 and below.

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

To register GigaVUE V Series Node and GigaVUE V Series Proxy using the custom data in Azure Portal, perform the following steps:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to Create virtual machine topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The GigaVUE V Series Node and GigaVUE V Series Proxy uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

Register GigaVUE V Series Proxy after Virtual Machine Launch

You can register GigaVUE V Series Proxy after launching the virtual machine using a configuration file.

To register,

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

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

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

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

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

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

Key Considerations for Upgrade

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

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

For the user created in GigaVUE-FM,

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

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

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

Configure GigaVUE Fabric Components using GCP

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

Minimum Requirements

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

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

Deployment Guideines

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

- Set the correct MTU for tunnels: With a default MTU of 1460 in GCP, use 1410 for IPv4 tunnels and 1390 for IPv6. To update the Traffic Acquisition Tunnel MTU:

  1. Select the monitoring domain.
  2. Select the **Edit Monitoring Domain** option.
  3. Enter the **Traffic Acquisition Tunnel MTU** value and select **Save**.

     For details, refer to Traffic Acquisition Tunnel MTU
- For successful registration of fabric components, configure firewall rules to open ports.
  - For details on how to configure firewall rules, refer to Use VPC firewall rules topic in GCP documentation.
  - For details on required ports, refer to Network Firewall Requirement.

- When you deploy the fabric components using third party orchestration, you cannot delete the Monitoring Domain or change the MTU without unregistering the registered fabric components.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. For details, refer to Create Monitoring Domain.
- When launching an instance, to access it using a private key, add the SSH key. The default password is gigamon.
- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to Configure Tokens .
- When GigaVUE-FM version is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For details, refer to the *Configure Role-Based Access for Third-Party Orchestration* section.

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

Configure UCT-V Controller in GCP

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

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

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

Register UCT-V Controller during Instance Launch

In your GCP, you can launch the UCT-V Controller and to register UCT-V Controller using custom metadata.

Perform the following steps:

1. On the VM instances page of GCP, select **Create instances** . For details, refer to Create and Start instance topic in the GCP documentation.
2. Under the **Metadata** tab, enter the **key** as **user-data** and in the **value** field enter the below mentioned text in the following format and deploy the instance. The UCT-V Controller uses this Custom Metadata to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
```

```
    owner: root:root
    permissions: '0644'
    content: |
      Registration:
         groupName: <Monitoring Domain Name>
         subGroupName: <Connection Name>
         token: <Token>
         remoteAddress: <IP address of the GigaVUE-FM>
         sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
         remotePort: 443
```

Register UCT-V Controller after Instance Launch

You can register UCT-V Controller after launching a Virtual Machine using a configuration file.

Perform the following steps:

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

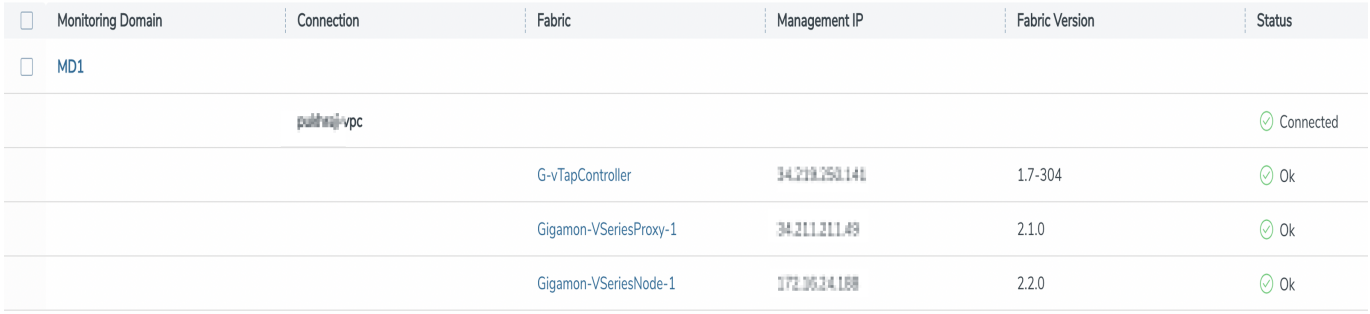
   ```
   Registration:
       groupName: <Monitoring Domain Name>
       subGroupName: <Connection Name>
       token: <Token>
       remoteAddress: <IP address of the GigaVUE-FM>
       sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
   deployments to specify which UCT-V Controller interface to use for communicating with
   GigaVUE-FM.)
       remotePort: 443
   ```

3. Restart the UCT-V Controller service.

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

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

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



Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
MD1					
	pathnai-vpc				Connected
		G-vTapController	34.219.250.141	1.7-304	Ok
		Gigamon-VSeriesProxy-1	34.211.211.49	2.1.0	Ok
		Gigamon-VSeriesNode-1	172.16.24.188	2.2.0	Ok

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

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

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

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

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

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
```

```
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   ```
   $ sudo netplan apply
   ```

6. Restart the UCT-V Controller service.

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

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

Configure UCT-V in GCP

Linux and Windows platforms support Deployment of GigaVUE fabric components through a third-party orchestrator.

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 takes place through another active Controller.

Install the Windows UCT-V

Perform the following steps:

1. Deploy Windows server in GCP. For details, refer to Create a Windows Server VM instance in Compute Engine topic in Google documentation.
2. Follow the instruction in the *Connect to the VM instance by using RDP* section of Set up Chrome Remote Desktop for Windows on Compute Engine topic in the GCP documentation.
3. Download UCT-V build in your desktop and copy it to the RDP session.

4. Turn off the Windows Firewall Defender.
5. Install the Windows UCT-V. For details, refer to Windows UCT-V Installation for step-by-step instructions on how to install Windows UCT-V.

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

Register UCT-V during Instance Launch

You need to register UCT-V through the registered UCT-V Controller. It communicates through PORT 8891.

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

In your GCP, to launch the instance and register the UCT-V using Custom Metadata, perform the following steps:

1. On the VM instances page of GCP, select **Create instances**. For details, refer to Create and Start instance topic in the GCP documentation.
2. Under the **Metadata** tab, enter the **key** as **user-data** and in the **value** field, enter the below mentioned text in the following format and deploy the instance. The UCT-V uses this Custom Metadata to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
         groupName: <Monitoring Domain Name>
         subGroupName: <Connection Name>
         token: <Token>
         remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
         sourceIP: <IP address of UCT-V> (Optional Field)
```

Register UCT-V after Instance Launch

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

1. Install the UCT-V in the Linux or Windows platform.
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.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, perform the following steps:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, select **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

   ```
   Registration:
       groupName: <Monitoring Domain Name>
       subGroupName: <Connection Name>
       token: <Token>
       remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
   Controller 2>
       sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
   specify which UCT-V interface to use for communicating with the UCT-V Controller.)
   ```

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

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

Configure GigaVUE V Series Nodes and V Series Proxy in GCP

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

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

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

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

1. On the VM instances page of GCP, select **Create an instance** . For details, refer to Create VMs with multiple network interfaces topic in the GCP documentation.
2. Under the **Metadata** tab, enter the **key** as **user-data** and in the **value** field, enter the below mentioned text in the following format and deploy the instance. The UCT-V uses this Custom Metadata to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

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

You can register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file.

To register,

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

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

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

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

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

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

Configure Packet Mirroring for GCP

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

> **NOTE:** When deploying GigaVUE V Series Nodes for configuring Application Intelligence Session, do not use Packet Mirroring. As Application Intelligence uses stateful traffic, you may experience packet drop due to GCP platform limitation.

Refer to the following topics for detailed information.

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

Rules and Notes

- Load Balancer forwards raw traffic. When configuring the monitoring session, use the Raw End Point as the first component that receives traffic.
- You must configure three NICs for GigaVUE V Series Node because REP and TEP cannot share the same interface.

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

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

Configure Packet Mirroring in GCP

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

1. Create an instance template in GCP to deploy the GigaVUE V Series Node in GCP using Third Party Orchestration. For details, refer to Configure GigaVUE Fabric Components using GCP.

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

2. Create Instance Group in GCP with autoscaling in Managed Instance Group. For details, refer Create a MIG with autoscaling enabled topic in Google Cloud Platform documentation.
3. Configure TCP or UDP internal Load balancer with packet forwarding enabled and ensure that the GigaVUE V Series Nodes data NICs are used to receive traffic. For details, refer to Create a load balancer for Packet Mirroring section in Google Cloud Platform documentation.
4. Configure packet mirroring in GCP. For instructions, refer to Use Packet Mirroring topic in Google Cloud documentation.

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

Configure Monitoring Session with Packet Mirroring

To configure monitoring session with packet mirroring enabled in GCP, perform the following steps:

Step 1: Edit the monitoring domain and update the following details:

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

Step 2: Create a monitoring session with the following instructions:

1. On the left page of GigaVUE-FM, select **Traffic > Virtual > Orchestrated Flows** and select **Third Party Orchestration**. The **Monitoring Sessions** page appears.
2. Select **New** to open the **Create a New Monitoring Session** page. For details, refer to Create a Monitoring Session (Third Party Orchestration).
3. In the **Edit Monitoring Session** page, add Raw End Point as the first component and Tunnel End Point as the final component. For details, refer to Create Raw Endpoint (Third Party Orchestration) and Create Ingress and Egress Tunnel (Third Party Orchestration).
4. Add your application to the monitoring session to connect your components.
5. Select the **Deploy** button in the edit monitoring session page to deploy the monitoring session after adding the Raw End Point.
6. In the **Select nodes to deploy the Monitoring Session** dialog box, from the drop-down menu, select the interface for REP and TEP.

Configure GigaVUE Fabric Components using Nutanix

This topic provides instructions on how to configure GigaVUE fabric components in Nutanix Prism Central using a configuration file. Gigamon supports two methods for acquiring traffic in Nutanix environments:

- Acquire Traffic using UCT-V
- Acquire Traffic using Customer Orchestrated Source

Acquire Traffic using UCT-V

This topic guides you through deploying Gigamon Cloud Suite for traffic visibility on Nutanix platforms running Prism Central version earlier than 5.0.

Recommended Instance Type

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

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

Deployment

This section outlines the workflow for acquiring traffic using UCT-V and deploying GigaVUE Fabric Components. It provides instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM
- Configure Role-Based Access for Third Party Orchestration
- Configure Tokens
- Create Monitoring Domain
- Configure UCT-V Controller in Nutanix
- Configure UCT-V in Nutanix
- Configure GigaVUE V Series Nodes and V Series Proxy in Nutanix
- Create a monitoring session in GigaVUE-FM.
- Deploy Monitoring Session
- View Monitoring Session Statistics

Install GigaVUE-FM

To launch the GigaVUE-FM instance from the Prism Central, refer to Create a VM topic in the Nutanix Prism Central documentation.

The following table lists the specific options you must select when creating a VM for GigaVUE-FM.

In the **Configuration** tab, enter the following details:

Field	Description
Name	Enter a name for the VM.
Description	Enter description for the VM. (optional)
Cluster	Select the cluster in which you want to deploy GigaVUE-FM.
Number of VMs	Enter the number of GigaVUE-FM you want to deploy.
VM Properties	• **CPU(s)**—number of vCPUs required. Minimum value is 1 vCPUs. However, the recommended value is 4 vCPUs. • **Cores Per vCPU**—number of cores per vCPU. The recommended value is 2 vCPUs. • **Memory**—memory size of the vCPU(s). Minimum value is 16GB.

In the **Resources** tab, enter or select the following details:

Field	Description

Disks	Click **Attach Disk**. The Attach Disk dialog box opens. Enter or select the following details:
	• **Type** - Select **Disk** from drop-down menu.
	• **Operation** - Select **Clone from Image** from the drop-down. This allows you to clone the GigaVUE-FM qcow2 image which you have already uploaded.
	• **Disk Placement** - Select **Same Cluster** when there is no shared storage between clusters. Select **Other Cluster** when shared storage exists between clusters. By default, Same Cluster is selected.
	• **Image** - Select the Image uploaded in the Upload Fabric Images section.
	• **Capacity** - Enter the Capacity in GB. Minimum value is 40GB.
	• **Bus Type** - Select the Bus Type as SCSI.
	Click **Save**.
	Add additional disk:
	Click **Attach Disk**. Enter or select the following details:
	• **Type** - Select **Disk** from drop-down menu.
	  • **Operation** - Select **Allocate on Storage Container** from the drop-down.
	  • **Disk Placement** - Select **Same Cluster** when there is no shared storage between clusters. Select **Other Cluster** when shared storage exists between clusters. By default, Same Cluster is selected.
	  • **Storage Container** - Select SelfServiceContainer from the drop down.
	  • **Capacity** - Enter the Capacity in GB. Minimum value is 40GB.
	  • **Bus Type** - Select the Bus Type as SCSI.

Networks	Click **Attach to Subnet**. The **Attach to Subnet** dialog box opens. Enter or select the following details: • **Subnet** - Select the Underlay Subnet from the drop-down menu. • **Network Connection State** - Ensure the status is Connected. • **Assignment Type** - Select the IP assignment type from the drop-down menu. • **IP Address** - Enter the static IP address for VLAN. This field is enabled only if Assign Static IP is selected in the Assignment Type field.
Boot Configuration	Select the boot configuration: UEFI Mode - To enable UEFI boot mode, select the **UEFI Mode** option.
Shield VM Security Settings	Enable the **Secure Boot** check box to use the secure boot mode.

In the **Management** tab, enter or select the following details:

Field	Description
Categories	Search for the category to be assigned to the VM. The policies associated with the category value are assigned to the VM.
Timezone	Select the time zone from the drop-down list.

After the VM is created, it appears in the VM list with the Power State set to **Off**. Once powered on, the VM becomes active.

Access GigaVUE-FM by entering the VM's IP address in a web browser and logging in using the default credentials: username admin and password admin123A!!. You can also access the GigaVUE-FM console from Prism Central, where you are prompted to change the password on first login.

Deployment Guidelines

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

- Set the correct MTU for tunnels: Use 1350 for IPv4 tunnels and 1330 for IPv6. To update the Traffic Acquisition Tunnel MTU:

  1. Select the monitoring domain.
  2. Select the **Edit Monitoring Domain** option.
  3. Enter the **Traffic Acquisition Tunnel MTU** value and select **Save**.

  > **NOTE:** Set the correct MTU before deploying the Monitoring Session. If not, you must undeploy and redeploy the session after updating the MTU.

- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to Configure Tokens.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. For details, refer to Create Monitoring Domain.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- When GigaVUE-FM version is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For details, refer to the *Configure Role-Based Access for Third-Party Orchestration* section in the v6.9 Documentation.

In Nutanix Prism Central, you can configure the following GigaVUE fabric components:

Configure UCT-V Controller in Nutanix

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

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

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

Register UCT-V Controller during Instance Launch

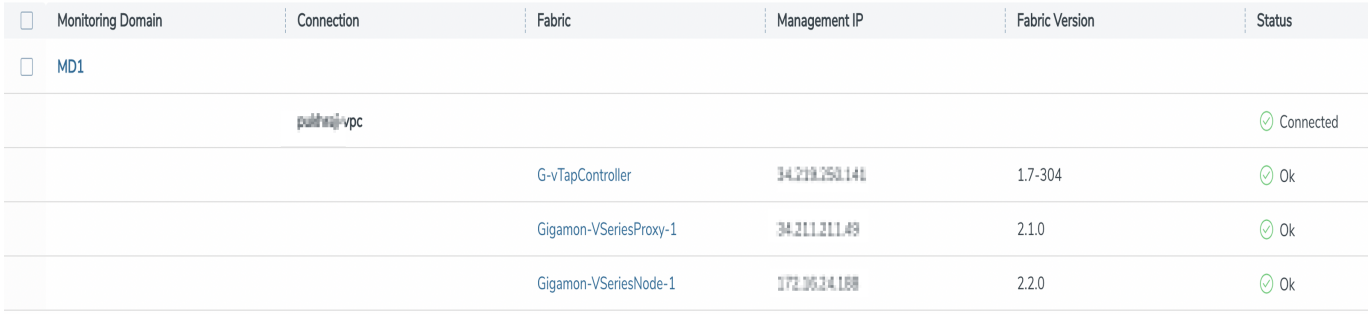
In the Nutanix Prism Central, you can launch the UCT-V Controller instance and register the UCT-V Controller using user data.

Perform the following steps:

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

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteAddress: <IP address of the GigaVUE-FM>
        sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
        remotePort: 443
```

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



Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
MD1					
	pathnaji-vpc				Connected
		G-vTapController	34.219.250.141	1.7-304	Ok
		Gigamon-VSeriesProxy-1	34.211.211.49	2.1.0	Ok
		Gigamon-VSeriesNode-1	172.30.24.188	2.2.0	Ok

Register UCT-V Controller after Instance Launch

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

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

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

3. Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

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

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

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

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

```
network:
  version: 2
  renderer: NetworkManager
```

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   $ sudo netplan apply

6. Restart the UCT-V Controller service.

   $ sudo service uctv-cntlr restart

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

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

Configure UCT-V in Nutanix

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

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

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

Register UCT-V during Instance Launch

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

In Nutanix Prism Central, you can launch the UCT-V instance and register the UCT-V using user data.

Perform the following steps:

1. On the Prism Central, go to the **List** tab and click **Create VM**. The Create VM dialogue box appears. For details, refer to Creating a VM through Prism Central (AHV) topic in the Nutanix documentation.
2. On the **Step 3:Management** tab, in the **Guest Customization** field, select **Cloud-init (Linux)**. Enter the registration data in the text box and deploy the instance. The UCT-V uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
         groupName: <Monitoring Domain Name>
         subGroupName: <Connection Name>
         token: <Token>
         remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
         sourceIP: <IP address of UCT-V> (Optional Field)
```

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

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

Register UCT-V after Instance Launch

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

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

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to Linux UCT-V Installation and 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.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, perform the following steps:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, select **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
    sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
```

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

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

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

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

Configure GigaVUE V Series Nodes and V Series Proxy in Nutanix

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

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

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

- Acquire Traffic using UCT-V
- Acquire Traffic using UCT-V

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

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

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

2. On the **Step 3:Management** tab, in the Guest Customization field, select **Cloud-init (Linux)**. enter the registration data in the text box and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

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

You can register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file.

Perform the following steps:

1. Log in to the GigaVUE V Series Node or Proxy.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
deployments to specify which UCT-V Controller interface to use for communicating with
GigaVUE-FM.)
    remotePort: 443
```

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

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

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

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

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

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

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

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

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

```
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   $ sudo netplan apply

6. Restart the GigaVUE V Series service.

   $ sudo service vseries-node restart

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

Limitations

Nutanix does not support IPv6 for the current release of GigaVUE Cloud Suite.

Acquire Traffic using Customer Orchestrated Source

Important:

If your environment uses GigaVUE-FM with Nutanix Prism Central pc.7.3 and FNS 4.2.0 or 4.2.1, use the GigaVUE-FM orchestrated deployment procedure instead. For more information, refer to Deploy GigaVUE Cloud Suite for Nutanix.

Existing GigaVUE-FM orchestrated Monitoring Domains and Monitoring Sessions are not supported after upgrade and must be deleted before proceeding.

This procedure applies only to Nutanix environments that meet the following minimum software versions. Verify that all components in your environment meet these requirements before you proceed.

Component	Minimum Version
Nutanix Prism Central	pc.7.5
FNS Next Gen	7.5.0
Network Controller	7.0.0
AHV	11.0
AOS	7.5
NCC	5.3.0

After the upgrade is complete, recreate the configuration using Third-Party Orchestration with Customer Orchestrated Source as the traffic acquisition method as described in this procedure.

This topic guides you through deploying Gigamon Cloud Suite for traffic visibility on Nutanix platforms running Prism Central pc.7.5, using Nutanix Flow Network Security Next Generation (FNS-NG) and Service Insertion.

Recommended Instance Type

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

Compute Instances	vCPU	Memory	Disk Space
GigaVUE-FM	4 vCPU	16GB	2 x 40GB
GigaVUE V Series Node	4 vCPU	8GB	10GB
GigaVUE V Series Proxy	1 vCPU	4GB	10GB

Prerequisites

Keep in mind the following when deploying the visibility solution using FNS-NG:

- VLANs must be migrated to Network Controller-Managed VLANs (NC-VLANs). The new Service Insertion applies only to NC-VLANs.
- FNS-NG supports traffic monitoring of only underlay networks. For overlay traffic, use the existing Acquire Traffic using UCT-V .

- GigaVUE-FM can be deployed internally on the Nutanix environment or externally outside the Nutanix platform. As long as connectivity is available between GigaVUE-FM and GigaVUE V Series Node (or Proxy), the solution can be deployed.
- Deploy a medium form factor GigaVUE V Series Node based on the per-cluster traffic load.
- Set the correct MTU for tunnels: Use 1350 for IPv4 tunnels and 1330 for IPv6. Set the correct MTU before deploying the Monitoring Session. If not, you must undeploy and redeploy the session after updating the MTU.

Deployment Planning

This section outlines the workflow for acquiring traffic with Customer Orchestrated Source and deploying GigaVUE Fabric Components. It provides instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Create a VM for GigaVUE-FM- Install and configure GigaVUE-FM as the centralized management platform. Note the GigaVUE-FM IP address
- Configure Role-Based Access for Third Party Orchestration - Create users, roles and the respective user groups in GigaVUE-FM. You can use the user group to create a token for registration data, which helps deploy fabric components in your orchestrator.
- Create a GigaVUE-FM Token- Note the GigaVUE-FM IP address and token, which are required later for GigaVUE V Series registration.
- Create a Monitoring Domain- Create a Monitoring Domain with traffic acquisition set to **Customer Orchestrated Source**. Note the Monitoring Domain name and Connection name, as these values are required for cloud-init configuration during GigaVUE V Series Node deployment.
- Deploy and Register GigaVUE V Series Node- Deploy a VM using the image. Configure three NICs (Management, Data, and Network Function) and provide cloud-init registration parameters, including the GigaVUE-FM IP, token, Monitoring Domain name, and Connection name. Power on the VM to automatically register it with GigaVUE-FM.
- Create Network Function Entity in Prism Central- Create a Network Function entity and associate it with the GigaVUE V Series Node's Network Function NIC. This enables Nutanix to identify the GigaVUE V Series Node as a network service and direct traffic to it.
- (Optional) Assign Categories to Target VMs- Assign categories to target workload VMs.
- Create an Application Security Policy- Configure inbound and outbound rules to forward traffic to the Network Function, enabling traffic redirection to the GigaVUE V Series Node.
- Create a monitoring session in GigaVUE-FM - Create a Monitoring Session that maps the GigaVUE V Series Node's Network Function NIC to a REP (ingress) and defines a tunnel to the monitoring tool (egress).
- Deploy Monitoring Session - Deploy the session to activate traffic processing.

- View Monitoring Session Statistics - Verify the flow. Nutanix Security Policy redirects traffic to the GigaVUE V Series Node through service insertion, the node processes the traffic, and the tunnel forwards it to the monitoring tool.

Create a VM for GigaVUE-FM

You can deploy GigaVUE-FM as a VM within the Nutanix Prism Central environment or externally. Ensure that GigaVUE-FM has network connectivity to the GigaVUE V Series Node management interface.

Refer to Upload Fabric Images to download the image file and upload the same to the Prism Central image library.

To launch the GigaVUE-FM instance from the Prism Central, refer to Create a VM topic in the Nutanix Prism Central documentation.

The following table lists the specific options you must select when creating a VM for GigaVUE-FM.

In the **Configuration** tab, enter the following details:

Field	Description
Name	Enter a name for the VM.
Description	Enter description for the VM. (optional)
Cluster	Select the cluster in which you want to deploy GigaVUE-FM.
Number of VMs	Enter the number of GigaVUE-FM you want to deploy.
VM Properties	• **CPU(s)**—number of vCPUs required. Minimum value is 1 vCPUs. However, the recommended value is 4 vCPUs. • **Cores Per vCPU**—number of cores per vCPU. The recommended value is 2 vCPUs. • **Memory**—memory size of the vCPU(s). Minimum value is 16GB.

In the **Resources** tab, enter or select the following details:

Field	Description

Disks	Click **Attach Disk**. The Attach Disk dialog box opens. Enter or select the following details:
	• **Type** - Select **Disk** from drop-down menu.
	• **Operation** - Select **Clone from Image** from the drop-down. This allows you to clone the GigaVUE-FM qcow2 image which you have already uploaded.
	• **Disk Placement** - Select **Same Cluster** when there is no shared storage between clusters. Select **Other Cluster** when shared storage exists between clusters. By default, Same Cluster is selected.
	• **Image** - Select the Image uploaded in the Upload Fabric Images section.
	• **Capacity** - Enter the Capacity in GB. Minimum value is 40GB.
	• **Bus Type** - Select the Bus Type as SCSI.
	Click **Save**.
	Add additional disk:
	Click **Attach Disk**. Enter or select the following details:
	• **Type** - Select **Disk** from drop-down menu.
	  • **Operation** - Select **Allocate on Storage Container** from the drop-down.
	  • **Disk Placement** - Select **Same Cluster** when there is no shared storage between clusters. Select **Other Cluster** when shared storage exists between clusters. By default, Same Cluster is selected.
	  • **Storage Container** - Select SelfServiceContainer from the drop down.
	  • **Capacity** - Enter the Capacity in GB. Minimum value is 40GB.
	  • **Bus Type** - Select the Bus Type as SCSI.

Networks	Click **Attach to Subnet**. The **Attach to Subnet** dialog box opens. Enter or select the following details: • **Subnet** - Select the Underlay Subnet from the drop-down menu. • **Network Connection State** - Ensure the status is Connected. • **Assignment Type** - Select the IP assignment type from the drop-down menu. • **IP Address** - Enter the static IP address for VLAN. This field is enabled only if Assign Static IP is selected in the Assignment Type field.
Boot Configuration	Select the boot configuration: UEFI Mode - To enable UEFI boot mode, select the **UEFI Mode** option.
Shield VM Security Settings	Enable the **Secure Boot** check box to use the secure boot mode.

In the **Management** tab, enter or select the following details:

Field	Description
Categories	Search for the category to be assigned to the VM. The policies associated with the category value are assigned to the VM.
Timezone	Select the time zone from the drop-down list.

After the VM is created, it appears in the VM list with the Power State set to **Off**. Once powered on, the VM becomes active.

Access GigaVUE-FM by entering the VM's IP address in a web browser and logging in using the default credentials: username admin and password admin123A!!. You can also access the GigaVUE-FM console from Prism Central, where you are prompted to change the password on first login.

Create a GigaVUE-FM Token

GigaVUE-FM allows you to generate a token only if you are an authenticated user and based on your privileges in accessing the GigaVUE-FM. You can create multiple tokens if required.

To create a token in GigaVUE-FM, follow these steps:

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

   NOTE: If you are a user with write access, then you can view a drop- down list under **Tokens**. Select **Current User Tokens** to create a token.
3. Select **New Token**.
4. Enter a name for the new token in the **Name** field.
5. Enter the days until the token is valid in the **Expiry** field.
6. Select the user group for which you are privileged to access GigaVUE-FM from the **User Group** drop-down list.
7. Select **OK** to generate a new token. The generated token appears on the **Tokens** page.
8. Select the token to copy and use it to authenticate the GigaVUE-FM REST APIs.
   a. Go to **Actions** > **Copy Token**.
   b. Paste the copied token in the required fields to complete authentication.

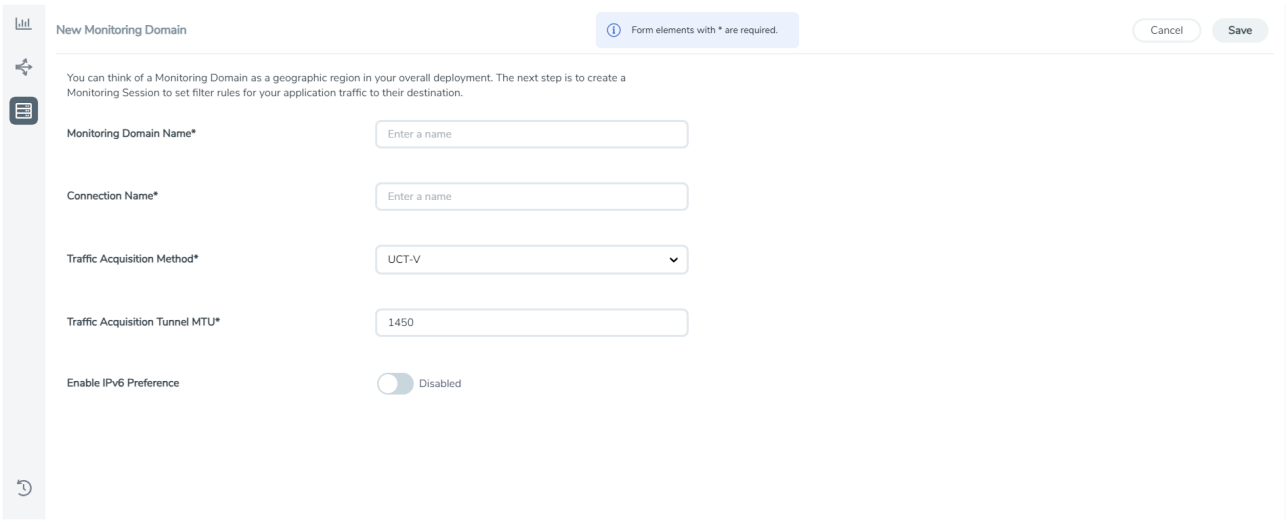
   NOTE: You cannot view the generated token. You can only copy and paste the generated token.

Create a Monitoring Domain

If a default Monitoring Domain was automatically created during a previous Third Party Orchestration registration, edit the existing Monitoring Domain to set the Traffic Acquisition Method to **Customer Orchestrated Source** before creating a Monitoring Session. Else, proceed with the following procedure to create a Monitoring Domain with Traffic Acquisition Method set to **Customer Orchestrated Source**:

To create a monitoring domain in Third Party Orchestration:

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



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

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain. A monitoring domain consists of set of connections.
Connection Alias	An alias used to identify the connection.
Traffic Acquisition Method	Select a tapping method. • **Customer Orchestrated Source**: If you select the Customer Orchestrated Source option, the mirrored, tunneled or the raw traffic from your workloads is directed directly to the GigaVUE V Series Nodes, and you need not configure the UCT-Vs and UCT-V Controllers.
Uniform Traffic Policy (When Traffic Acquisition Method is Customer Orchestrated Source)	**Note**: This step is optional when acquiring traffic using Customer-Orchestrated Source in Nutanix Prism Central FNS-NG. Enable this option if you wish to use the same monitoring session configuration for the GigaVUE V Series Node deployed under this monitoring domain. Enable this check box when using packet mirroring configuration for GCP. **Note**: Once the monitoring session is deployed for the monitoring domain you cannot enable or disable this option.

4. Click **Save**.

Notes:

- Ensure that all V Series Nodes within a single Monitoring Domain are running the same version. Mixing different versions in the same Monitoring Domain may lead to inconsistencies when configuring Monitoring Session traffic elements.
- Similarly, when upgrading a V Series Node, ensure that the GigaVUE-FM version is the same or higher than the V Series Node version.

Deploy and Register GigaVUE V Series Node

Important:

GigaVUE-FM does not support fabric upgrades for GigaVUE V Series nodes. To upgrade a GigaVUE V Series node:

- Power off and delete the existing GigaVUE V Series node from Prism Central.
- Upload and deploy the new GigaVUE V Series node image to Prism Central.

Before deploying the GigaVUE V Series Node, you must decide how it will register with GigaVUE-FM. This choice determines the remotePort and remoteIP values in the cloud-init configuration and cannot be changed after the VM is created.

Register	remotePort	remoteIP
GigaVUE V Series Node	443	IP address of GigaVUE-FM
GigaVUE V Series Proxy	8891	IP address of GigaVUE V Series

Register	remotePort	remoteIP
		node

Refer Upload Fabric Images to download the GigaVUE V Series Node or GigaVUE V Series Proxy image.

Upload the GigaVUE V Series to Prism Central

You are required to make the GigaVUE V Series Node image available in the Prism Central image library for use during VM deployment.

You can upload images to Nutanix Prism Central using one of the following methods:

- Upload an image file directly from your local system.
- Upload from a remote server. Provide the URL of the image hosted on a remote server to import it into Prism Central.

Use the method that best fits your environment and image source.

Deploy and Configure the GigaVUE V Series node VM

You are required to deploy the GigaVUE V Series Node as a VM in Prism Central, configured with the appropriate NICs and cloud-init registration parameters to enable automatic registration with GigaVUE-FM on first boot.

GigaVUE V Series requires three NICs:

- Management NIC — provides connectivity between the GigaVUE V Series Node and GigaVUE-FM.
- Data NIC — used to forward processed traffic to your monitoring tools.
- Network Function NIC — receives redirected traffic from Nutanix Service Insertion. This NIC is essential for the FNS-NG integration.

Refer to Create a VM topic in Nutanix Prism Central documentation.

The following table lists the specific options you must select when creating a VM for GigaVUE V Series.

On the Configuration page, enter the basic VM settings:

Field	Description
Name	Enter a descriptive name (for example, VSN-Cluster1-Node1)
Description	Enter description for the VM. (optional)

Field	Description
Cluster	Select the cluster in which you want to deploy GigaVUE V Series.
Number of VMs	Enter the number of GigaVUE V Series node you want to deploy.
VM Properties	• **CPUs** - Number of vCPUs required. Minimum value is 1 vCPUs. However, the recommended value is 4 vCPUs. • **Cores per CPU** - Enter the number of cores per socket. • **Memory** - Allocate memory based on deployment requirements. However the recommended value is 8GB. Refer to Recommended Instance Type.

On the Resources page and select the following.

Field	Description
Disks	Select **Clone from Image** and select the GigaVUE V Series node image you had uploaded in Deploy and Register GigaVUE V Series Node.
Network	Attach the following NICs: • **Management NIC** - Select the underlay subnet • **Data NIC**: Select the Data subnet • **Network Function NIC**: Select the subnet associated with the NC-VLAN used for service insertion. To add Network Function NICs, click **More Network Options** > **Add Network Function NIC**. The Network Function NIC is identified by its MAC address in Nutanix Prism Central. During Network Function creation, this MAC address is selected and mapped to the NF entity, which enables redirected (tapped) traffic from Security Policies to be sent to this GigaVUE V Series node. **NOTE:** You must set Network Function NIC. Nutanix Service Insertion uses this NIC to redirect workload VM traffic to the GigaVUE V Series Node. If Network Function NIC is configured as a normal NIC, traffic redirection does not occur and the security policy has no effect.

On the Management configuration page, configure cloud-init to enable automatic registration with GigaVUE-FM.

1. In the **Guest Customization** field, select Cloud-init (Linux) and **Configuration Method** as Custom Script.
2. Enter the Registration details replacing the placeholder. The GigaVUE V Series Node uses this user data to generate the config file (/etc/gigamon-cloud.conf) used to register with GigaVUE-FM.

```
#cloud-config
write_files:
  - path: /etc/gigamon-cloud.conf
```

```
owner: root:root
permissions: '0644'
content: |
  Registration:
      groupName: <Monitoring Domain Name in GigaVUE-FM>
      subGroupName: <Connection Name within the Monitoring Domain>
      token: <Token generated in GigaVUE-FM>
      remoteIP: <IP address of the GigaVUE-FM>
      remotePort: 443
```

Important: If you have not added the NICs during the VM creation, you can attach the required NICs by editing the VM configuration before powering on the VM.

Review the configuration on the Review page and create the VM. After the VM is created, power on the GigaVUE V Series node VM. The GigaVUE V Series node automatically registers with GigaVUE-FM using the cloud-init configuration.

You can verify that the deployed node appears in **GigaVUE-FM** under **Third Party Orchestration** > **Monitoring Domain** > GigaVUE V Series Nodes (IP) with the status Healthy.

[Active-Standby] Deploy and Register a Second GigaVUE V Series Node

NOTE: For high availability, we recommend deploying two GigaVUE V Series nodes and registering them to the same Monitoring Domain in GigaVUE-FM.

Active-Standby mode improves availability by using two GigaVUE V Series nodes. One node is active and processes traffic, while the other is standby and takes over if the active node becomes unavailable. During failover, the standby node automatically becomes active, ensuring continuous traffic monitoring.

Requirements

- Two GigaVUE V Series nodes
- Both nodes powered on at all times
- Both nodes registered with GigaVUE-FM
- A single Network Function (NF) entity that includes both nodes

Deploy a second GigaVUE V Series node by referring to Deploy and Register GigaVUE V Series NodeRegister both nodes with GigaVUE-FM.

After deploying and registering the GigaVUE V Series node, create the Network Function (NF) entity and Security Policy in Nutanix Prism Central to define how traffic is redirected to the node.

Create Network Function Entity in Prism Central

You must create a Network Function (NF) entity in Prism Central. A Security Policy redirects traffic only to a Network Function entity, not directly to a VM or NIC. Without this entity, the GigaVUE V Series node does not receive traffic, even if it is deployed and registered with GigaVUE-FM.

Refer to Create Network Function Entity topic in the Nutanix Prism Central.

The following table lists the specific options you must select while creating a Network Function Entity:

Field	Description
Name	Enter a name for the network function (for example, Gigamon-Monitoring).
Traffic Forwarding Mode	Select **vTAP** (Virtual TAP). vTAP copies traffic from the target VM and sends it to the GigaVUE V Series node without interrupting the original traffic flow.
Assign VM NICs	Select your GigaVUE V Series Node VM. In the drop-down, confirm that the MAC address of the Network Function NIC is listed. If no MAC address appears, verify that the Network Function NIC was correctly added during VM creation in Deploy and Register GigaVUE V Series Node.

The network function entity is now created and linked to the GigaVUE V Series node.

NOTE: Each NF entity supports a maximum of two GigaVUE V Series nodes as an Active-Standby pair. If your deployment includes additional GigaVUE V Series nodes, create separate NF entities and corresponding Security Policies for each node pair, and map the appropriate target VM categories to distribute traffic across nodes.

(Optional) Assign Categories to Target VMs

Security policies in Prism Central are applied to categories, which are logical groupings of VMs. Assign categories (tags) to identify the workloads whose traffic you want to monitor.

Refer to the following topics in the Nutanix Prism Central documentation:

1. Create a Category
2. Assign Category to an Entity

Assign the required category key-value pair to the VM so it can be identified and used in Create an Application Security Policy.

You can also assign the required category during VM creation by selecting the appropriate key-value pair in the **Categories** field on the Management configuration page. Search for the key-value pair you created, select it, and then complete the remaining VM configuration to ensure the VM is correctly classified from the start.

Create an Application Security Policy

Nutanix Prism Central offers a visualization-based approach to configuring security policies and monitoring the traffic to which a given policy applies. A Security Policy can redirect traffic to only one NF entity, which maps to the Network Function NIC of a specific GigaVUE V Series node.

> **NOTE:** If you have deployed more than one GigaVUE V Series node, create a separate NF entity and a dedicated Security Policy for each node in Nutanix Prism Central.
>
> To distribute traffic across multiple nodes, define distinct target VM categories and create a corresponding Security Policy for each node, ensuring that each policy maps its assigned VMs to the appropriateGigaVUE V Series node.

Refer to Creating an Application Policy with Service Insertion.

The following table lists the specific options you must select when you are creating a security policy.

On the Define Policy page, enter the following details:

Field	Description
Name	Enter a name for the policy (for example, security-policy-vsn).
Policy Type	Select Application: Secure Entities. For service insertion, where traffic is forwarded to a network function such as a GigaVUE V Series node, select Application:Secure Entities.

On the Secure Application page, enter the following details:

Field/Pane	Description
Scope	Set the scope to VLANs only. Service Insertion is supported only on NC-VLANs.
Inbound	Add traffic sources by choosing whether to capture all traffic or limit it to a specific source. If you choose to limit it to a specific source, in the **Entity Type** field, select VM or Subnet. These are the only entity types supported for service insertion.
Outbound	Add traffic sources by choosing whether to capture all traffic or limit it to a specific destination. If you choose to limit it to a specific destination, in the **Entity Type** field, select VM or Subnet. These are the only entity types

Field/Pane	Description
	supported for service insertion.
Secured Entities	Identifies the entities whose traffic is monitored. Select VM as the entity type and choose the category key-value pair assigned to the target VMs to define the traffic scope. When creating the rules or security policy, the selected secured entity and configured condition are applied together.

After defining the traffic sources and secured entity:

1. Create separate inbound and outbound rules, where the configured traffic condition and the selected secured entity are applied together.
2. During rule creation, open the inbound rule configuration using the (+) symbol which appears once you click on the Inbound/Outbound pane. Click **Enable forwarding to a Network Function**, then select the network function entity created in Create Network Function Entity in Prism Central so that the traffic is redirected for inspection.
3. Configure outbound rules in the same way to ensure both traffic directions are monitored.
4. Finally, **Apply and Enforce** the policy to activate traffic redirection. The policy must be in the Enforced state for traffic redirection to take effect. A policy that is saved but not enforced does not redirect traffic.

What to do next:

Create a Monitoring Session (Third Party Orchestration) in GigaVUE-FM to define the traffic processing pipeline from the GigaVUE V Series's Network Function NIC to the monitoring tool.

Configure GigaVUE Fabric Components using OpenStack

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

Recommended Instance Type

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

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

Deployment Best Practices

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

- Set the correct MTU for tunnels: Use 1450 for IPv4 tunnels and 1430 for IPv6. To update the Traffic Acquisition Tunnel MTU:

  1. Select the monitoring domain.
  2. Select the **Edit Monitoring Domain** option.
  3. Enter the **Traffic Acquisition Tunnel MTU** value and select **Save**.

  > **NOTE:** Set the correct MTU before deploying the Monitoring Session. If not, you must undeploy and redeploy the session after updating the MTU.

- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. For details, refer to Create Monitoring Domain.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in OpenStack.
- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to Configure Tokens.
- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For details, refer to the *Configure Role-Based Access for Third-Party Orchestration* section in the 6.9 Documentation.

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

Configure UCT-V Controller in OpenStack

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

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

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

Register UCT-V Controller during Instance Launch

In your OpenStack dashboard, you can launch the UCT-V Controller and register UCT-V Controller using Customization Script.

perform the following steps:

1. On the Instance page of OpenStack dashboard, select **Launch instance**. The Launch Instance wizard appears. For detailed information, refer to Launch and Manage Instances topic in OpenStack Documentation.
2. On the **Configuration** tab, enter the Customization Script as text in the following format and deploy the instance. The UCT-V Controller uses this registration data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteAddress: <IP address of the GigaVUE-FM>
        sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
        remotePort: 443
```

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

Register UCT-V Controller after Instance Launch

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

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

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

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
deployments to specify which UCT-V Controller interface to use for communicating with
GigaVUE-FM.)
    remotePort: 443
```

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

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

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

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

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

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.

5. Apply the configuration.

```
$ sudo netplan apply
```

6. Restart the UCT-V Controller service.

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

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

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

Configure UCT-V in OpenStack

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

To register UCT-V using a configuration file:

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

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

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, perform the following steps:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, click **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
    sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
```

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

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

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

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

Configure GigaVUE V Series Nodes and V Series Proxy in OpenStack

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if the user

does not wish to reveal the IP addresses of the nodes, then you can register your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

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

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

Register V Series Nodes or V Series Proxy during Instance Launch

To register V Series nodes or proxy using the Customization Script in OpenStack GUI:

1. On the Instance page of OpenStack dashboard, select **Launch instance**. The Launch Instance wizard appears. For detailed information, refer to Launch and Manage Instances topic in OpenStack Documentation.
2. On the **Configuration** tab, enter the Customization Script as text in the following format and deploy the instance. The V Series nodes or V Series proxy uses this customization script to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

Register V Series Node or V Series Proxy after Instance Launch

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

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

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

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

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

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

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

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

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

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

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

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

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   $ sudo netplan apply

6. Restart the GigaVUE V Series service.

   $ sudo service vseries-node restart

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

Configure GigaVUE Fabric Components using VMware ESXi

This topic provides instructions on how to deploy the fabric components for VMware ESXi.

NOTE: When registering GigaVUE V Series Nodes in GigaVUE-FM, make sure that the connection name under each Monitoring Domain is unique. When GigaVUE-FM version is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a Username and Password instead of using tokens in the registration data. For more details, refer to the Configure Role-Based Access for Third-Party Orchestration section in the 6.9 Documentation.

Recommended Instance Type

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

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

You can deploy the GigaVUE V Series Node using the following deployment modes based on your requirement.

- Single uplink for Management, Data and Tool connectivity.
- Single uplink for Management and Tool connectivity, and another uplink for Data connectivity.
- (Recommended) Separate uplinks (three) for Management, Data, and Tool connectivity.

Prerequisites

The following prerequisites are required for deployment of the GigaVUE V Series Node in VMware ESXi.

- **Configuring port groups:** Create a Management Port Group for connectivity with GigaVUE-FM, a Data Port Group to receive data from the H Series node, and a Tool Port Group for connectivity with the tools.
- **Configuring virtual switch:** Create unique virtual switches for each port group. Refer to VMware Documentation for more information.
- Download the OVA files from the Gigamon Community portal and extract it to get the OVF and VMDK files.

Deploy and Register GigaVUE V SeriesNode

To deploy and register:

1. Log into the VMware ESXi web interface.

2. Right-click the ESXi Host, Cluster, or data center on which you want to deploy the GigaVUE V Series Node and then select **Create/Register VM**. The **New Virtual Machine** wizard appears.
3. In the **Select Creation Type** page, select Deploy a virtual machine from an OVF and OVA file option.
4. Click **Next**. The **Select OVF and VMDK files** page appears.
5. In the **Select OVF and VMDK files** page, enter a unique name for the virtual machine and upload the .ovf and .vmdk files from your local machine.
6. Click **Next** and the **Select storage** page appears.
7. Select a datastore where the virtual machine's files will be stored.
8. Click **Next**. The **Deployment Options** page appears.
9. In the **Deployment Options** page, select the management port, data port, and tool port as referenced in the prerequisites.
    a. Select the **Deployment Type** from the list:
        - Do Not Use DHCP – Select this option if you want to use static IP addresses for the management, data, and tool ports.
        - Management, Data and Tool Port DHCP – Select this option if you want to use dynamic IP addresses for the management, data, and tool ports.
        - Management Port DHCP – Select this option if you want to use dynamic IP address only for the management port.
        - Tool Port DHCP - Select this option if you want to use dynamic IP address only for the tool port.
        - Data Port DHCP – Select this option if you want to use dynamic IP address only for the data port.
    b. Select Thin/Thick in the **Disk Provisioning** field.
    c. Unselect the **Power on automatically** checkbox. This is selected by default. It is recommended to disable the Power on automatically option and review all configuration before switching on the virtual machine.
10. Click **Next**. The **Additional Settings** page appears.
11. Do the following configuration in the **Additional Settings** page.
    a. In the **System** section, enter the hostname of the V Series node instance in the **Hostname** field and create a new admin password for the V Series node instance in the **Administrative Login Password** field.

    This credential will be used for V series SSH access. The default username is gigamon. If the deployment fails, you can login to V Series SSH/Console and check the logs for troubleshooting.

b. In the **Network Connectivity** section, enter the required fields based on the selected network configuration.

> **NOTE:** Ensure to unselect the **Management Port DHCP** checkbox if you want to use static IP address for the management port. If you select the Management Port DHCP checkbox, dynamic IP address will be configured for the management port even if you have selected Do Not Use DHCP option in the Configuration page.

c. Enter the required value in the **Management Port MTU size in bytes** field. The default value is 1500B.

d. Enter the DNS server address in the **Nameserver** field to resolve the domain name of the tool destination URL.

e. In the **Optional Parameters** section, enter the Monitoring Domain name in the **GroupName** field and connection name in the **SubGroupName** field. The Monitoring Domain and connection name corresponds to the domain name and connection that you created during the Configure GigaVUE Fabric Components using VMware ESXi configuration.

f. Enter the token created in GigaVUE-FM in the **JWT Token used for registration** field. Refer to Configure GigaVUE Fabric Components using VMware ESXi.

g. Enter the GigaVUE-FM IP address and remote port in the **RemoteIP** and **RemotePort** fields respectively. In case of any error, you should re-deploy the V Series.

h. In the **Custom node properties** field enter app_mode=linux_apps (mandatory).

12. Click **Next** and the **Ready to complete** page appears.
13. Review all the entered information and modify the configuration if required.
14. Click **Finish**. When the operation completes, you have successfully deployed a GigaVUE V Series Node.

Verify GigaVUE V Series Node Registration

During the initial bring up, the V Series reboots multiple times for initialization. After few minutes, you can check the status of the deployment in GigaVUE-FM. If the status is failed, you can check the logs to perform troubleshooting.

To check the logs:

1. Log in to V Series Node via console or SSH to management IP address.
2. Enter the below path in the terminal to check the registration details.

```
tail -f /var/log/vseries-node-reg.log
```

OVF Package Files

Form Factor	Supported Ports	File Name	Comments
Small (2vCPU, 4GB Memory, and 8GB Disk space)	Mgmt Port, Tool Port, and 8 Network Ports	vseries-node-file1.ovf	Use these files when deploying GigaVUE V Series Node via VMware vCenter.
Medium (4vCPU, 8GB Memory, and 8GB Disk space)	Mgmt Port , Data Port, and Tool Port	vseries-node-file2.ovf	
Large (8vCPU, 16GB Memory, and 8GB Disk space)	Mgmt Port, Tool Port, and 8 Network Ports	vseries-node-file3.ovf	
Small (2vCPU, 4GB Memory, and 8GB Disk space)	Mgmt Port , Data Port, and Tool Port	vseries-node-file4.ovf	Use these when deploying GigaVUE V Series Node via VMware NSX-T Manager.
Medium (4vCPU, 8GB Memory, and 8GB Disk space)	Mgmt Port , Data Port, and Tool Port	vseries-node-file5.ovf	
Large (8vCPU, 16GB Memory, and 8GB Disk space)	Mgmt Port, Tool Port, and 2 Network Ports	vseries-node-file6.ovf	
Small (2vCPU, 4GB Memory, and 8GB Disk space)		vseries-node-file7.ovf	Use these files when deploying GigaVUE V Series Node via VMware ESXi without vCenter.
Medium (4vCPU, 8GB Memory, and 8GB Disk space)	Mgmt Port, Tool Port, and 8 Network Ports	vseries-node-file8.ovf	
Large (8vCPU, 16GB Memory, and 8GB Disk space)	Mgmt Port , Data Port, and Tool Port	vseries-node-file9.ovf	
Larger (8vCPU, 16GB Memory, and 80GB Disk space)	Mgmt Port, Tool Port, and 8 Network Ports	vseries-node-file12.ovf	Use these files when deploying GigaVUE V Series Node via VMware vCenter and if you wish to configure AMX application.
Larger (8vCPU, 16GB Memory, and 80GB Disk space)	Mgmt Port , Data Port, and Tool Port	vseries-node-file15.ovf	Use these files when deploying GigaVUE V Series Node via VMware ESXi without vCenter and if you wish to configure AMX application. **NOTE:** This file supports form factor with higher range of CPU, memory and disk space.
	Mgmt Port , Data Port, and Tool Port	vseries-node-file16.ovf	minipc - Virtual Small Form Factor

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

The static IP addresses are assigned to the GigaVUE V Series node in the following scenarios:

• When you have assigned or selected DHCP for the port groups during deployment and want to change it to static IP address after deployment.

• When you have assigned static IP address for the port groups during deployment and want to update the assigned static IP address.

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

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

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

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

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
```

```
routes:
  - to: 10.114.48.1/32
    scope: link
  - to: default
    via: 10.114.48.1
```

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

   $ sudo netplan apply

6. Restart the GigaVUE V Series service.

   $ sudo service vseries-node restart

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

Register UCT-V Controller

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

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

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

1. Log in to the UCT-V Controller.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data.
   Refer to Configure Tokens for token creation details.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
deployments to specify which UCT-V Controller interface to use for communicating with
GigaVUE-FM.)
```

```
    remotePort: 443
```

3. When using Static IP configuration or multiple interfaces with Static IP configuration, create a new .yaml file in **/etc/netplan/** directory.
4. Update the file and save it.
5. 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.

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

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

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

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

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
```

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

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

   ```
   $ sudo netplan apply
   ```

6. Restart the UCT-V Controller service.

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

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

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

Register UCT-V

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

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to Linux UCT-V Installation and 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.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, perform the following steps:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, select **View**.
     c. In the **View** tab, enable the **File name extensions** checkbox.

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

4. Restart the UCT-V service.

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

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

Verification and Troubleshooting

After applying the configuration, the should register with GigaVUE-FM.

After successful registration the sends heartbeat messages to every 30 seconds.

If one heartbeat is missing- Status: Unhealthy.

If five consecutive heartbeats fail- attempts to reach

If that fails unregisters the and removes from.

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

Perform the following steps when you deploy V Series Node in VMware ESXi host with SR-IOV Adapter:

1. On the VM page in the VMware ESXi host environment, select **Edit**.
   The **Edit Settings** page appears.

2. In the **Virtual Hardware** tab, edit the following fields:
   - CPU: 8
   - Memory: 16GB
   - Hard disk 1: 80GB
   - Network adapter 1: VM Network (Connected)
   - Network adapter 2: Port Group (Connected)
   - Network adapter 3: Port Group (Connected)
   - Video card: 4MB

   NOTE: Make sure to select **Reserve all guest memory** for VM Memory.

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

a. **Port-Group Mapping:**

- ens160: Mapped with VMNetwork
- ens192 and ens224: Correctly mapped with the Port Groups that the user creates

Sample Netplan Configs:

- ens160 with 192.168.10.X
- ens192 with 192.168.20.X

```
Example netplan config:

gigamon@vseries:/etc/netplan$ more 60-netcfg.yaml
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens160:
      dhcp4: no
      dhcp6: no
      addresses:
        - 10.115.203.139/21
        - 2001:db8:1::10/64
      routes:
        - to: default
          via: 10.115.200.1
        - to: default
          via: 2001:db8:1::1
    ens192:
      dhcp4: no
      dhcp6: yes
      addresses:
        - 192.150.10.25/24
      routes:
        - to: 192.150.10.0/24
          scope: link

   ens224:
      dhcp4: no
      dhcp6: yes
      addresses:
        - 10.210.16.210/20
      routes:
        - to: 10.210.16.0/24
          scope: link
```

3. Power off VM and remove Network Adapter 2 and Network Adapter 3. Now, without saving, add two new Network Adapters and change the **Adapter Type** to **SR-IOV passthrough**.
   Once added, the user-created Port-Group mappings for ens192 and ens224 get swapped.
4. In **Edit Settings**, swap the adapters to correct the configuration mismatch with Netplan configs.

5. Save the configuration and deploy the VM.
   Now, ens192 and ens224 are mapped with the correct Port Group Mappings.
6. Use the following command to manually configure /etc/gigamon-cloud.conf with registration configurations to register V Series Node with GigaVUE-FM.
   ```
   gigamon@vsn-5gc-new:~$ cat /etc/gigamon-cloud.conf
   ```
7. Under the additional settings page, provide the user data as shown below:
   - GroupName: <Monitoring domain name>
   - SubGroupName: < Connection name>
   - token: <Token>
   - remoteIP: <IP address of the GigaVUE-FM>
   - remotePort: 443

   Refer to Configure Tokens for token creation details.

Configure GigaVUE Fabric Components using VMware vCenter

This topic provides instructions on how to deploy the fabric components using VMware vCenter.

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

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

Recommended Instance Type

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

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

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

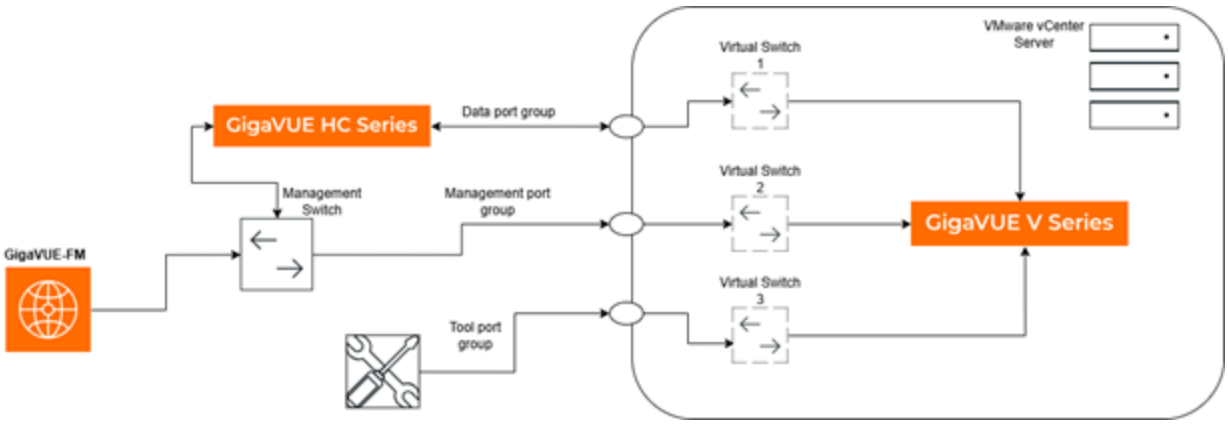
Fabric Component Registration for Deployments

The following table displays the fabric components registration required for various deployments.

Application	Deployment	GigaVUE V Series Registration	UCT-V Registration	UCT-V Controller Registration
Linux	AMX, 5G Cloud, GV-HTTP2, 5G-SBI, Sbipoe	Required	NA	NA
GigaSMART	AMI, AFI, Slicing, App Viz, Dedup, Header Stripping, Load Balancing, Masking	Required	Required	Required

GigaVUE V Series Node Deployment and Registration

The following architecture diagram explains the deployment of GigaVUE V Series Node in VMware vCenter and registration of the V Series Node with GigaVUE-FM.



The architecture includes a HC Series device that is connected to the VMware vCenter server through a data port. The VMware vCenter server has virtual switches and V Series node that communicate with the HC Series device, GigaVUE-FM and tools through the Management, Data, and Tool port groups. Each port group is mapped to a unique virtual switch to ensure smooth transmission of data, management, and tool traffic. The V Series node is deployed with the Linux or GigaSMART applications. The Data port group carries monitored traffic from the H Series to the V Series, and the Tool port group connects the V Series to the external tools.

Deployment Mode

The GigaVUE Cloud Suite fabric components support the following deployment modes:

- Single uplink for Management, Data and Tool connectivity
- Single uplink for Management and Tool connectivity, and another uplink for Data connectivity
- Separate uplinks (three) for Management, Data, and Tool connectivity

Prerequisites

The following prerequisites are required for deployment of the GigaVUE V Series Node in VMware vCenter.

- **Configuring port groups:** Create a Management Port Group for connectivity with GigaVUE-FM, a Data Port Group to receive data from the H Series node, and a Tool Port Group for connectivity with the tools. Refer to VMware Documentation for more information.
- **Configuring virtual switch:** Create unique virtual switches for each port group. Refer to VMware Documentation for more information.
- **Configuring monitoring domain:** Create a monitoring domain in the GigaVUE-FM UI. The Connection name must be unique across the monitoring domains. Refer to Create Monitoring Domain topic for more information.
- **Configuring token:** Create a token for registration of V Series Node with GigaVUE-FM. Refer to Configure Tokens topic for more information.
- Download the OVA files from the Gigamon Community portal and extract it to get the OVF and VMDK files.

Deploy and Register GigaVUE V SeriesNode

Do the following steps:

1. Log into the VMware vCenter web interface.
2. Right-click the vCenter Host, Cluster, or data center on which you want to deploy the GigaVUE V Series Node and then select Deploy OVF Template. The **Deploy OVF Template** wizard appears.
3. In the **Select an OVF template** page, choose one of the following options:
   a. URL – Enter the URL of the .ovf file.

   > **NOTE:** Refer to the OVF Package Files for selecting the required OVF file.

   b. Local file – Click the Upload Files button and navigate to .ovf and .vmdk files that are available on your local machine, and then select the files.
   c. Refer to the OVF Package Files table for the OVF package files.
4. Click **Next**. **Select a name and folder** page appears.

5. Enter a unique name for the virtual machine in the **Virtual machine name** field, and then select a location and host to which you want to deploy the GigaVUE FM instance.
6. Click **Next**. **Select a compute resource** page appears.
7. Select a destination compute host for the OVF deployment.
8. Click **Next**. The **Review details** page appears.
9. Verify the OVF template details, and then select Next. The **Configuration** page appears.
10. Select a deployment configuration from the following:
    a. Do Not Use DHCP – Select this option if you want to use static IP addresses for the management, data, and tool ports
    b. Management, Data and Tool Port DHCP – Select this option if you want to use dynamic IP addresses for the management, data, and tool ports
    c. Management Port DHCP – Select this option if you want to use dynamic IP address only for the management port
    d. Tool Port DHCP - Select this option if you want to use dynamic IP address only for the tool port
    e. Data Port DHCP – Select this option if you want to use dynamic IP address only for the data port
11. . Click **Next** and the **Select storage** page appears.
12. . From the **Select virtual disk format** list, select **Thick Provisioning** as the format for the virtual disks and provisioning.
13. . Select a datastore where the virtual machine's files will be stored.

    NOTE: Note: It is recommended to use datastore that has Solid-State Drive (SSD) drive type for AMX deployments to get a better performance.

14. . Click **Next**. The **Select networks** page appears.
15. . Select the port groups configured for Management Port, Tool Port and Data Port.
16. . Click **Next**. The **Customize template** page appears. The Customize template page has three sections namely: System, Network Connectivity, Optional Parameters.
17. . Do the following configuration in the Customize template page.
    a. In the **System** section, enter the hostname of the V Series node instance in the **Hostname** field and create a new admin password for the V Series node instance in the **Administrative Login Password** field.

> **NOTE:** This credential will be used for V series SSH access. The default username is gigamon. If the status is failed you can login to V Series SSH/Console and check the logs for troubleshooting

b. In the **Network Connectivity** section, enter the required fields based on the selected network configuration.

> **NOTE:** Ensure to unselect the Management Port DHCP checkbox if you want to use static IP address for the management port. If you select the Management Port DHCP checkbox, dynamic IP address will be configured for the management port even if you have selected Do Not Use DHCP option in the Configuration page.

> **NOTE:** If you do not enter value for the Management Port MTU size in bytes, the default value of 1500B is considered.

c. Enter the DNS server address in the **Nameserver** field to resolve the domain name of the tool destination URL.

d. In the **Optional Parameters** section, enter the monitoring domain name in the **GroupName** field and connection name in the **SubGroupName** field.

> **NOTE:** The monitoring domain and connection name corresponds to the domain name and connection referenced in the prerequisites section.

e. Enter the token created in GigaVUE FM UI in the **JWT Token used for registration** field.

f. Enter the GigaVUE FM IP address and remote port in the **RemoteIP** and **RemotePort** fields respectively.

g. In the **Custom node properties** field enter one of the following:

- app_mode=linux_apps
- app_mode=gs_apps

> **NOTE:** Refer to Fabric Component Registration for Deployments table.

18. Click **Next** and the **Ready to complete** page appears.
19. Review all the entered information and then click **Finish**. When the operation completes, you have successfully deployed a GigaVUE V Series node.

> **NOTE:** You can modify the CPU, Memory and Disk if required to handle higher traffic load, before powering on the VM.

Verification and Troubleshooting

During the initial bringup, the V Series reboots multiple times. After a wait time of 5 minutes, you can check the status of the deployment. If the status is failed, you can check the logs to perform troubleshooting.

OVF Package Files

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

Form Factor	Supported Ports	File Name	Comments
Larger (8vCPU, 16GB Memory, and 80GB Disk space)	Mgmt Port, Tool Port, and 8 Network Ports	vseries-node-file12.ovf	Use these files when deploying GigaVUE V Series Node via VMware vCenter and if you wish to configure AMX application.
Larger (8vCPU, 16GB Memory, and 80GB Disk space)	Mgmt Port , Data Port, and Tool Port	vseries-node-file15.ovf	Use these files when deploying GigaVUE V Series Node via VMware ESXi without vCenter and if you wish to configure AMX application. **NOTE:** This file supports form factor with higher range of CPU, memory and disk space.
	Mgmt Port , Data Port, and Tool Port	vseries-node-file16.ovf	minipc - Virtual Small Form Factor

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

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

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

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

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

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

```
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   $ sudo netplan apply

6. Restart the GigaVUE V Series service.

   $ sudo service vseries-node restart

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

Register UCT-V Controller

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

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

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

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

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
deployments to specify which UCT-V Controller interface to use for communicating with
GigaVUE-FM.)
    remotePort: 443
```

3. When using Static IP configuration or multiple interfaces with Static IP configuration, create a new .yaml file in **/etc/netplan/** directory.
4. Update the file and save it.
5. 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.

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

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

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

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

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

```
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   $ sudo netplan apply

6. Restart the UCT-V Controller service.

   $ sudo service uctv-cntlr restart

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

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

Register UCT-V

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

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to Linux UCT-V Installation and 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.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, perform the following steps:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, select **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

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

4. Restart the UCT-V service.

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

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

Verification and Troubleshooting

After applying the configuration, the should register with GigaVUE-FM.

After successful registration the sends heartbeat messages to every 30 seconds.

If one heartbeat is missing- Status: Unhealthy.

If five consecutive heartbeats fail- attempts to reach

If that fails unregisters the and removes from .

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

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

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

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

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

Prerequisites:

- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to Configure Tokens .

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

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

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

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

Register UCT-V Controller

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

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

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

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

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

3. Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

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

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

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

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

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   $ sudo netplan apply

6. Restart the UCT-V Controller service.

   $ sudo service uctv-cntlr restart

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

Register UCT-V

IMPORTANT: You must enable the basic authentication for launching UCT-V Controller version 6.9 and below.

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 happens through another Controller that is active.

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

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer toLinux 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.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, perform the following steps:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, select **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the UCT-V Controller 1>, <IP address of the UCT-V
Controller 2>
    sourceIP: <IP address of UCT-V> (Optional Field)
```

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

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

4. Restart the UCT-V service.

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

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

Register GigaVUE V Series Node

IMPORTANT: You must enable the basic authentication for launching GigaVUE V Series Nodes version 6.9 and below.

For instructions on how to deploy GigaVUE V Series Node on the VMware ESXi host, refer to Configure GigaVUE Fabric Components using VMware ESXi topic.

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

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

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

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

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

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

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

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
```

```
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

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

   ```
   $ sudo netplan apply
   ```

6. Restart the GigaVUE V Series service.

   ```
   $ sudo service vseries-node restart
   ```

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

Deploy and Register GigaVUE V Series Nodes on KVM Hypervisor

This section provides information on how to deploy and register GigaVUE V Series Node on a KVM hypervisor, specifically for deploying Application Metadata Exporter (AMX) application on GigaVUE-FM Hardware Appliance.

NOTE: As of now, AMX is the only validated and tested application for this deployment scenario. GigaVUE-FM manages the deployment of the AMX application on the V Series Node.

Refer to the following:

- Deploy GigaVUE V Series Node on KVM hypervisor
- Register GigaVUE V Series Nodes using a Configuration file

Deploy GigaVUE V Series Node on KVM hypervisor

Prerequisites:

1. From Gigamon Customer Portal, download the recent GigaVUE V Series Node image, and move qcow2 file to a desired location.
2. Install and enable Cockpit services on the KVM hypervisor.

3. Perform the following steps to enable Cockpit View on the KVM hypervisor:
   a. Update the system package list

```
sudo apt update
```

   b. Install Cockpit and Cockpit-Machines

```
sudo apt install -y cockpit cockpit-machines
```

   c. Enable and start the Cockpit service

```
sudo systemctl enable --now cockpit.socket
```

   After executing the commands, you can access KVM using port 9090 in your browser: http://<your-server-IP>:9090

Points to Note:

- When you deploy the fabric components using third party orchestration, you cannot delete the Monitoring Domain without unregistering the registered fabric components.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both of these interfaces when deploying the GigaVUE V Series Node in KVM.
- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For more details, refer to Configure Role-Based Access for Third Party Orchestration.
- On the **User Management** page, token configuration happens. For details, refer to Configure Tokens.
- For better performance, we recommend to enable SR-IOV.

Create a Virtual machine KVM Hypervisor

To create a VM in KVM hypervisor for deploying the GigaVUE V Series Node, follow the below instructions:

Parameters	Instructions	Mandatory field
Connection	Select **System**.	Yes
Installation Type	Select **Cloud base image** from the drop-down list.	Yes

Parameters	Instructions	Mandatory field
Installation Source	Select the location of the qcow2 image.	Yes
Operating System	Select the latest Ubuntu version.	
Storage	Select **Create new qcow2 volume**.	

Select **Create and edit** to edit the Virtual Machine. Edit the VM as mentioned in the following table.

Parameters	Instructions	Mandatory field
CPU		
vCPU Maximum	Enter the maximum number of vCPU's required (ex: 10).	Yes
vCPU Count	Enter the number of CPUs to allocate (ex: 8).	Yes
Network Interfaces Add additional interfaces for Data and Tool		

NOTE: The CPU values mentioned in the above table are sample entries and can be customized as required.

Select **Install** and then **Run** to deploy the V Series Node. After successfully creating the VM (GigaVUE V Series Node) in KVM, register the GigaVUE V Series Node with GigaVUE-FM using configuration file. For details, refer to Deploy and Register GigaVUE V Series Nodes on KVM Hypervisor.

Register GigaVUE V Series Nodes using a Configuration file

To register GigaVUE V Series Node using a configuration file:

1. Log in to the GigaVUE V Series Node using the default user name **gigamon** and the default password Gigamon123!.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node using the following details:

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

3. Restart the GigaVUE V Series Node service.

```
$ sudo service vseries-node restart
```

Deploy Fabric Components using Integrated Mode

In integrated mode, using GigaVUE-FM, you create a monitoring domain in your respective GigaVUE Cloud Suite. Then, use your own orchestration system just deploy GigaVUE V Series nodes.

GigaVUE-FM displays the deployed Nodes under the monitoring domain you created in your respective GigaVUE Cloud Suite. In this case, ensure that the monitoring domain and the connection name given in GigaVUE-FM matches the groupName and subGroupName in the user data provided in your orchestration system.

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

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

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

Configure Secure Communication between Fabric Components in FMHA

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

Follow these steps:

1. Access the active GigaVUE-FM via CLI.
2. Archive the stepCA directory using the following commands:
   ```
   sudo su
   cd /var/lib
   tar -cvf /home/admin/stepca.tar stepca
   ```
3. Set the permissions of the tar file using the following commands:
   ```
   chmod 666 /home/admin/stepca.tar
   ```

4. Copy the tar file to all standby instances in the **/home/admin/ directory** using scp:
   ```
   scp /home/admin/stepca.tar <standby-node>:/home/admin/
   ```
5. Download the **runstepca_fmha** script from the Community Portal.
6. Log in to the standby instance using CLI.
7. Copy the script in the standby instance in the **/home/admin directory** and execute it using the following command:
   ```
   sh /home/admin/runstepca_fmha
   ```

Configure Secure Tunnel for Third Party Orchestration

You can configure the Secure tunnels on:

- Precrypted Traffic
- Mirrored Traffic

Precrypted Traffic

Secure tunnels help protect sensitive precrypted traffic by framing packets in PCAPng format and transmitting them through a TLS socket. When you enable secure tunnel for both precrypted and mirrored traffic, the system creates two separate TLS sessions.

Recommendation: Always enable secure tunnels for precrypted traffic to ensure secure data transmission.

For more information about PCAPng, refer to PCAPng Application.

Mirrored Traffic

You can also 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 for Third Party Orchestration in UCT-V
- Configure Secure Tunnel for Third Party Orchestration

Prerequisites

- While creating Secure Tunnel, you must provide the following details:
  - SSH key pair

    - CA Certificate chain
- Port 11443 is enabled in security group settings. For details, refer to Network Firewall Requirement.

Notes

- Protocol versions IPv4 and IPv6 are supported.
- If you wish to use IPv6 tunnels, your GigaVUE-FM and the fabric components version must run vesion 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 is transmitted over IPv4, regardless of IPv6 preference.
- After configuring secure tunnels, if a Monitoring Domain contains only one GigaVUE V Series Node and that GigaVUE V Series Node reboots or restarts, then you must manually add the SSL Key pairs to the Monitoring Domain again. For details, refer to Edit SSL Configuration.

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

S. No	Task	Refer to
1.	Upload a CA Certificate chain in a single file	You must upload a CA Certificate chain to UCT-V Controller to establish a connection with the GigaVUE V Series Node. To upload the CA Certificate chain using GigaVUE-FM, follow the steps given below: 1. Go to **Inventory > Resources > Security > CA List**. 2. Select **New** to add a new Authority. The **Add Custom Authority** page appears. 3. Enter or select the following information. • Alias - Alias name of the CA. • File Upload - Choose the certificate from the desired location. 4. Select **Save**. **NOTE:** Ensure that the Intermediate CA Certificate(s) are included in the CA certificate chain file in the correct signing order, followed by the Root CA Certificate at the end. For more information, refer to the section Adding Certificate Authority
2.	Upload a SSL Key Pair	You must add a SSL key pair to GigaVUE V Series Node. To add SSL Key Pair, follow the steps in the section SSL Decrypt.
3.	Select the SSL Key Pair and CA Certificate chain, after deploying the fabric components.	You must select the added SSL Key Pair and CA Certificate chain in GigaVUE V Series Node after creating a Monitoring Domain configuring the fabric components in GigaVUE-FM. Refer to Edit SSL Configuration for more detailed information on how to select the added SSL Key Pair and CA Certificate chain in GigaVUE V Series Node.
4	Enable the secure tunnel	You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE V Series Node. To enable the secure tunnel feature follow these steps: **1.** In the Edit Monitoring Session page, click **Options**. The **Monitoring Session Options** page appears. **2.** Enable the **Secure Tunnel** button. You can enable secure tunnel for both mirrored and precrypted traffic.

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	Refer to
1.	Upload a CA Certificate chain in a single file	You must upload a CA Certificate chain to UCT-V Controller to establish a connection with the GigaVUE V Series Node. To upload the CA Certificate chain using GigaVUE-FM, follow the steps given below: 1. Go to **Inventory > Resources > Security > CA List**. 2. Select **New** to add a new Authority. The **Add Custom Authority** page appears. 3. Enter or select the following information. • Alias - Alias name of the CA. • File Upload - Choose the certificate from the desired location. 4. Select **Save**. **NOTE:** Ensure that the Intermediate CA Certificate(s) are included in the CA certificate chain file in the correct signing order, followed by the Root CA Certificate at the end. For more information, refer to the section Adding Certificate Authority
2.	Upload an SSL Key Pair	You must add an SSL key pair to GigaVUE V Series node. To add an SSL Key Pair, follow the steps in the section Upload SSL Keys.
3	Select the SSL Key Pair and CA Certificate chain, after deploying the fabric components.	You must select the added SSL Key Pair and CA Certificate chain in GigaVUE V Series Node after creating a Monitoring Domain configuring the fabric components in GigaVUE-FM. Refer to Edit SSL Configuration for more detailed information on how to select the added SSL Key Pair and CA Certificate chain in GigaVUE V Series Node.
4	Create a secure tunnel between UCT-V and the first GigaVUE V	You should enable the secure tunnel feature to establish a connection between the UCT-V and the first GigaVUE V Series

S. No	Task	Refer to
	Series Node	Node. To enable the secure tunnel feature follow these steps: **1.** In the Edit Monitoring Session page, click **Options**. The **Monitoring Session Options** page appears. **2.** Enable the **Secure Tunnel** button. You can enable secure tunnel for both mirrored and precrypted traffic.
5	Create an Egress tunnel from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session.	You must create a tunnel for traffic to flow out from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session. Refer to Create Ingress and Egress Tunnels for more detailed information on how to create tunnels. To create the egress tunnel, follow these steps: **1.** After creating a new Monitoring Session, or click **Actions** > **Edit** on an existing Monitoring Session, the GigaVUE-FM canvas appears. **2.** In the canvas, select **New** > **New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add** Tunnel Spec quick view appears. **3.** On the New Tunnel quick view, enter or select the required information as described in the following table: • Alias - The name of the tunnel endpoint. • Description - The description of the tunnel endpoint. • Type - Select TLS-PCAPNG for creating egress secure tunnel • Traffic Direction - Choose **Out** (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: o MTU- The default value is 1500. o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64. o DSCP - Enter the Differentiated Services Code Point (DSCP) value. o Flow Label - Enter the Flow Label value. o Source L4 Port- Enter the Souce L4 Port value o Destination L4 Port - Enter the Destination L4 Port value. o Flow Label o Cipher- Only SHA 256 is supported. o TLS Version - Select TLS Version1.3. o Selective Acknowledgments - Choose **Enable** to turn on the TCP selective acknowledgments. o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.

S. No	Task	Refer to
		o Delay Acknowledgments - Choose **Enable** to turn on delayed acknowledgments. • IP Version - The version of the Internet Protocol. IPv4 and IPv6 are supported. • Remote Tunnel IP - Enter the interface IP address of the second GigaVUE V Series Node (Destination IP). **4.** Select **Save**.
6	Select the added SSL Key Pair after deploying the fabric components in the second GigaVUE V Series Node	You must select the added SSL Key Pair in the second GigaVUE V Series Node. Select the second GigaVUE V Series Node and follow the steps given in Edit SSL Configuration.
7	Create an ingress tunnel in the second GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session for the second GigaVUE V Series Node.	You must create a ingress tunnel for traffic to flow in from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session. Refer to Create a Monitoring Session to know about Monitoring Session. To create the ingress tunnel, follow these steps: **1.** After creating a new Monitoring Session, or click **Actions** > **Edit** on an existing Monitoring Session, the GigaVUE-FM canvas appears. **2.** In the canvas, select **New** > **New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add** Tunnel Spec quick view appears. **3.** On the New Tunnel quick view, enter or select the required information as described in the following table: • Alias - The name of the tunnel endpoint. • Description - The description of the tunnel endpoint. • Type - Select TLS-PCAPNG for creating egress secure tunnel. • Traffic Direction - Choose **In** (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6. • IP Version - The version of the Internet Protocol. IPv4 and IPv6 are supported. • Remote Tunnel IP - Enter the interface IP address of the first GigaVUE V Series Node (Destination IP). **4.** Select **Save**.

Viewing Status of Secure Tunnel

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

To verify the status of secure tunnel,

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

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

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

Create Prefiltering Policy Template

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

To create a prefiltering policy template,

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

2. Select **New**.

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

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

5. Select one of the following options:

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

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

6. Select one of the following options:

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

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

7. Select a priority value from 1-8.

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

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

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

- L3
- L4

9. Select one of the following options **Filter Name**:

- ip4Src
- ip4Dst
- ip6Src
- ip6Dst
- Proto: Applies toboth ipv4 and ipv6.

10. Select one of the following options for **Filter Relation**:

- Not Equal to
- Equal to

11. In the **Value** field, enter the source or destination port.

12. Select **Save**.

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

To enable prefiltering, refer to Monitoring Session Options.

Create Precryption Template for UCT-V

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

Rules and Notes:

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

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

- Create Precryption Template for Filtering based on Applications
- 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 you apply Precryption in the Monitoring Session Options page.

To create,

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

   The **Precryption Policies** page appear

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

3. Select **Add**.

   The New Precryption Template page appears.

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

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

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

Create Precryption Template for Filtering based on L3-L4 details

To create,

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

3. Perform the following steps:

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

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

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

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

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

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

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

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

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

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

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

- L3:
- L4

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

For L3, perform the following:

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

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

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

- Not Equal to
- Equal to

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

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

For L4, perform the following:

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

- Source Port
- Destination Port

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

- Not Equal to
- Equal to

iii. Enter the source or destination port value.

4. Select **Save**.

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

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

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

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

Configure Monitoring Session

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

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

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

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

Create a Monitoring Session (Third Party Orchestration)

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

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

Target Instance

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

You can create multiple Monitoring Sessions within one Monitoring Domain.

To create a new Monitoring Session:

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

Monitoring Session Page (Third Party Orchestration)

The table outlines core tabs in the Monitoring Session interface, each enabling targeted configuration, traffic analysis, and infrastructure visibility to support efficient session management.

Tab	Description
Overview	You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can also view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can filter the statistics based on the elements associated with the Monitoring Session. For more information, refer to View Monitoring Session Statistics.
Sources	Displays the sources and target details monitored by the Monitoring Session. You can view and edit the connection details of the Monitoring Session. You can view the deployment status, number of targets, and targets source health. In the **Selection Status** section, you can view the VM status. The status indicates whether the VM is supported, not supported, selected, or not selected. When you hover over the status, a tooltip displays the reason for that status. **NOTE:** In the case of OVS Mirroring, the Sources tab also displays the Hypervisor details along with the Instances.
Traffic Processing	You can view, add, and configure applications, tunnel endpoints, raw endpoints, and maps. You can view the statistical data for individual applications and also apply threshold template, enable user defined applications, and enable or disable distributed De-duplication. Refer to Configure Monitoring Session Options for more detailed information.
V Series Nodes	You can view the V Series nodes associated with the Monitoring Session. In the split view, you can view details such as name of the V Series Node, health status, deployment status, Host VPC, version, and Management IP. You can also change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping section for details.
Topology	Displays the fabric and monitored instances based on the connections configured in your network. You can select a specific connection to explore its associated subnets and instances in the topology view, offering a clear visualization of the monitored network elements. Refer to Visualize the Network Topology (Third Party Orchestration).

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

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

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

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

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

Monitoring Session Options (Third Party Orchestration)

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

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

Access the TRAFFIC PROCESSING tab

To navigate to **TRAFFIC PROCESSING** tab, follow these steps:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. On the left pane with the Monitoring Sessions list view, select a Monitoring Session.
3. Select the **TRAFFIC PROCESSING** tab.

Apply Threshold Template

You can apply the Threshold configuration to a Monitoring Session before deployment.

To apply a threshold,

1. In the **TRAFFIC PROCESSING** page, select **Options > Thresholds**.
2. Select an existing threshold template from the **Select Template** drop-down list. You can create a template using **New Threshold Template** option and apply it.
3. Select **Apply.**

For more information, refer to the Traffic Health Monitoring section.

The template is added to the Monitoring Session.

Notes:

- Undeploying the Monitoring Session does not remove the applied Thresholds.
- You can also view the details related to the applied thresholds, such as traffic element, metrics, type, trigger values, and time intervals, in the threshold window.

Select **Clear Thresholds** to clear the applied thresholds across the selected Monitoring Session.

Enable User-Defined Applications

To enable a defined application,

1. In the Monitoring Session **TRAFFIC PROCESSING** page, select **Options > User Defined Applications**.
2. Enable the **User-defined Applications** toggle button.
3. From the **Actions** drop-down, add one of the existing applications or create a User-Defined Application.

For more information, refer to User Defined Application.

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. For more information, refer to Distributed De-duplication.

To enable,

1. In the TRAFFIC PROCESSING page, select **Options > Distributed De-duplication**.

2. Enable the toggle.

Notes:

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

Create Ingress and Egress Tunnel (Third Party Orchestration)

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

Create a new tunnel endpoint

To create,

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

   The GigaVUE-FM Monitoring Session canvas page appears.
2. On the left pane of the canvas, select the icon to view the traffic processing elements.
3. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace.

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

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

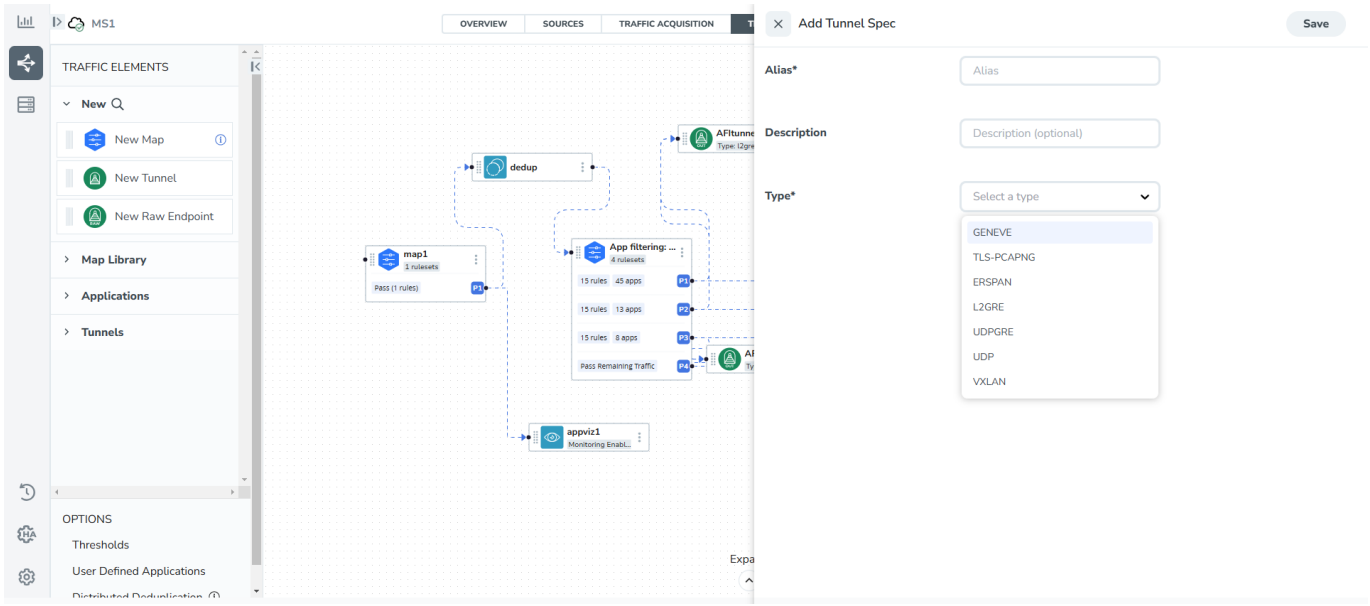


Table 1: Details - Add Tunnel Specifications

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

Field	Description	
	Source L4 Port	The port used to establish the connection to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port used to establish the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose **Out** (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node to the destination endpoint.	
	Remote Tunnel IP/FQDN	For egress tunnels, specify the destination endpoint by using an IPv4 address, IPv6 address, or fully qualified domain name (FQDN). FQDN support applies only to VXLAN and L2GRE egress tunnels. By using an FQDN, you can keep the same tunnel configuration even when the destination IP address changes. If the FQDN resolves to both IPv4 and IPv6 addresses, the system selects the address based on the preferred IP stack configured for the monitoring domain.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Multi Tunnel	Enable the multi-tunnel flag to create multiple tunnels for flow distribution to the 5G-Cloud application. Refer to 5G-Cloud Ericson SCP Support. **Applicable Platforms**: OpenStack, Third Party Orchestration, VMware ESXi **Notes:** ▪ You can configure either a single-tep or multi-tep setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session. ▪ When you enable Multi-Tunnel on a VXLAN tunnel and set the number of tunnels, GigaVUE-FM automatically creates the

Field	Description	
		additional VXLAN tunnel endpoints. Any later changes to the original VXLAN tunnel, such as disabling Multi-Tunnel or modifying Domain Tagging do not update these auto created endpoints. They continue to retain the configuration that existed at the time they were created. To apply updated settings, you must delete the VXLAN TEP and the associated LB application, then recreate the LB and VXLAN TEP with the new configuration, and re-establish the link between them.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping. **NOTE:** This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to PCAPng Application for details.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It routes the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		

Field	Description	
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **Note**: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to the Secure Tunnels.		
In	Choose **In** (decapsulation) to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
Out	Choose **Out** (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint.	
	Remote Tunnel IP/FQDN	For egress tunnels, specify the destination endpoint by using an IPv4 address, IPv6 address, or fully qualified domain name (FQDN). FQDN support applies only to VXLAN and L2GRE egress tunnels. By using an FQDN, you can keep the same tunnel configuration even when the destination IP address changes. If the FQDN resolves to both IPv4 and IPv6 addresses, the system selects the address based on the preferred IP stack configured for the monitoring domain.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping. **NOTE:** This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to PCAPng

Field	Description	
		Application for details.
ERSPAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	**IP Version**	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **Note**: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to Secure Tunnels section.		
In	**IP Version**	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments for a delay.

Field	Description	
Out	**IP Version**	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that helps network devices identify the higher or lower priority to handle traffic. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable the receipt of acknowledgments.
	Sync Retries	Enter the number of times you can try the sync. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable the receipt of acknowledgments when there is a delay.
UDP:		
Out	**L4 Destination IP Address**	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. For details, refer to Application Metadata Exporter.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.

Managing Tunnel Endpoints

Apply a threshold template to Tunnel End Points

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

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

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

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

Delete Tunnel Endpoints

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

Create Raw Endpoint (Third Party Orchestration)

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

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

To add Raw Endpoint to the Monitoring Session,

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

3. Enter the Alias and Description details for the Raw End Point and click **Save**.
4. Perform the following steps to deploy the Monitoring Session after adding the Raw Endpoint:
   a. On the **TRAFFIC PROCESSING** page, select **Actions>Deploy**. The **Deploy Monitoring Session** dialog box appears.
   b. Select the desired V Series Nodes to deploy the Monitoring Session.
   c. Select the interfaces for each of the REPs and the TEPs deployed in the Monitoring Session from the drop-down menu for the selected individual V Series Nodes.
   d. Select **Deploy**.
5. Select **Export** to download all or selected V Series Nodes in CSV and XLSX formats.

Create a New Map (Third Party Orchestration)

Terms to know before creating a map:

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

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps** Below are the filter rule types that work in ATS: • mac Source • mac Destination • ipv4 Source • ipv4 Destination • ipv6 Source • ipv6 Destination • VM Name Destination • VM Name Source • VM Tag Destination • VM Tag Source The traffic direction is as follows: • For any rule type as Source - the traffic direction is egress. • For Destination rule type - the traffic direction is ingress. • For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. **Note**: • If no ATS rule filters listed above are used, all VMs and vNICS are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC. • Use the **GigamonNode** Tag to exclude any Gigamon devices from the target. • When using VM Name filter for selecting the Virtual Machines using Inclusion and Exclusion Maps, wild- cards in VM names are not supported. You must use the prefix of the Virtual Machine name.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

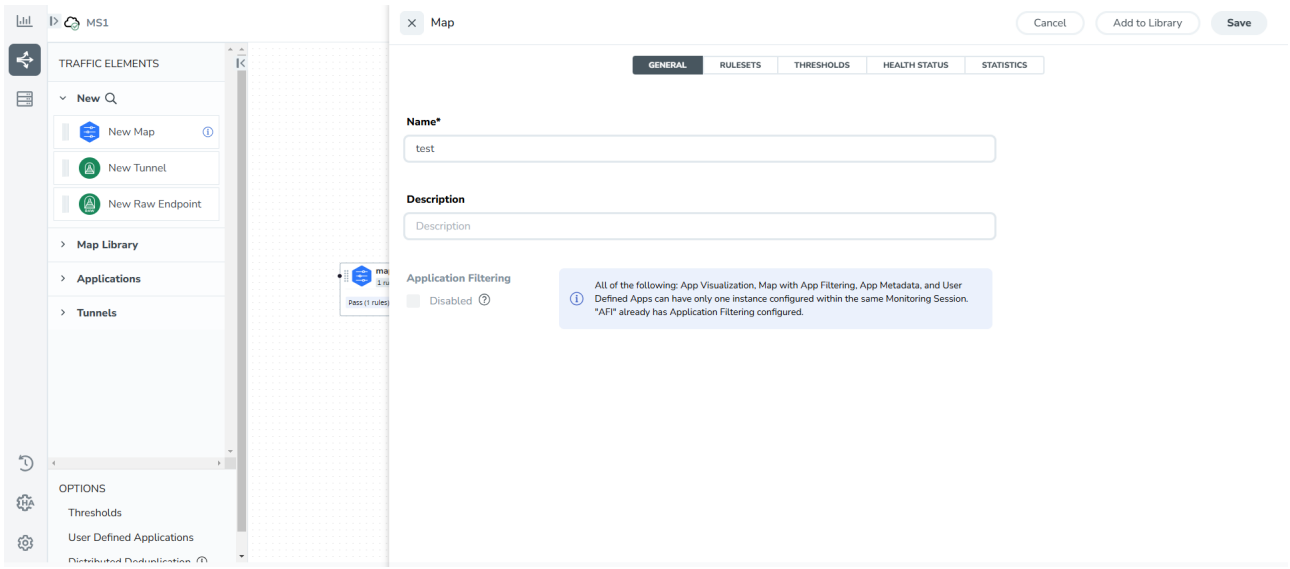
Rules and Notes:

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

- If a packet is fragmented then all the fragments are destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. For details, refer to "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide*.

To create a new map:

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



2. On the new Map quick view, select the **General** tab and enter the required information as described below.
   a. Enter the **Name** and **Description** of the new map.
   b. Enable the **Application Filtering** option if you wish to use Application Filtering Intelligence.
   Enabling this option allows you to filter traffic based on Application name or family. Refer to Application Filtering Intelligence.

> **NOTE:** Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:
> - Traffic Map—Only Pass rules for ATS
> - Inclusion Map—Only Pass rules for ATS
> - Exclusion Map—Only Drop rules for ATS

3. Select the **Rule Sets** tab.
   a. **To create a new rule set:**
      i. Select **Actions > New Ruleset**.
      ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
      iii. Enter the Application Endpoint in the Application EndPoint ID field.
      iv. Select a required condition from the drop-down list.
      v. Select the rule to **Pass** or **Drop** through the map.
   b. **To create a new rule:**
      i. Select **Actions > New Rule**.
      ii. Select a required condition from the drop-down list. Click ... and select **Add Condition** to add more conditions.
      iii. Select the rule to **Pass** or **Drop** through the map.
4. Select **Save**.

Through the map, you can drop or pass packets based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. For details, refer to Example- Create a New Map using Inclusion and Exclusion Maps .

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

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

Example- Create a New Map using Inclusion and Exclusion Maps

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

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

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

Map Library

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

To add a map,

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

   The GigaVUE-FMCanvas page appears.

2. From the page, select the desired map and save it as a template.

3. Select **Details**.

   The Application quick view appears.

4. Select **Add to Library** and perform one of the following:

   - From the **Select Group** list, select an existing group.

- Select **New Group** to create a new one.

5. In the **Description** field, add details, and select **Save**.

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

Reusing a map

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

Add Applications to Monitoring Session

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

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

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

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

- Application Metadata Intelligence
- Application Filtering Intelligence

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

Interface Mapping

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

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

To perform interface mapping,

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.

   The **Monitoring Sessions** landing page appears.

2. Navigate to the **V SERIES NODES** tab and select **Interface Mapping**.

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

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

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

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

5. Select **Deploy**.

   NOTE: The updated mappings take effect when deployed.

Deploy Monitoring Session

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

To deploy the Monitoring Session,

1. **Add components to the canvas**
   Drag and drop the following items to the canvas as required:

   - **Ingress tunnel** (as a source): From the **New** section.
   - **Maps:** From the **Map Library** section.
   - **Inclusion and Exclusion maps:** From the Map Library to their respective section at the bottom of the workspace.
   - GigaSMART **apps:** From the **Applications** section.
   - **Egress tunnels:** From the **Tunnels** section.

2. **Connect components**
   Perform the following steps after placing the required items in the canvas.

   a. Hover your mouse on the map

   b. Select the dotted lines

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

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

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

   The monitored instances and the subnets are visible in orange.

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

4. **Deploy the Monitoring Session**

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

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

Important:

Bulk Deploy: Select one or more monitoring sessions, and then choose Deploy from the available actions to deploy them simultaneously.

When deploying multiple monitoring sessions, GigaVUE-FM checks for sessions with undeployed changes. If any are found, GigaVUE-FM displays a warning message before proceeding the action. Bulk Deploy uses the previously deployed configuration for those sessions by default. Your latest changes are not applied.

To include the latest changes in a **Bulk Deploy** action:

1. Deploy the monitoring session with undeployed changes individually. From the **Actions** menu, select **Deploy**.
2. After the deployment completes, run **Bulk Deploy** again.

If you run **Bulk Deploy** without deploying the individual monitoring session first, GigaVUE-FM continues to use the previously deployed configuration.

View the Deployment Report

You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab.

- When you select the **Status** link, the Deployment Report is displayed.
- When the deployment is incorrect, the Status column displays one of the following errors:
  - **Success:** Not deployed on one or more instances due to V Series Node failure.
  - **Failure:** Not deployed on all V Series Nodes or Instances.

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

The Monitoring Session Deployment includes two key configuration:

- Interface Mapping
- Tool Exclusion

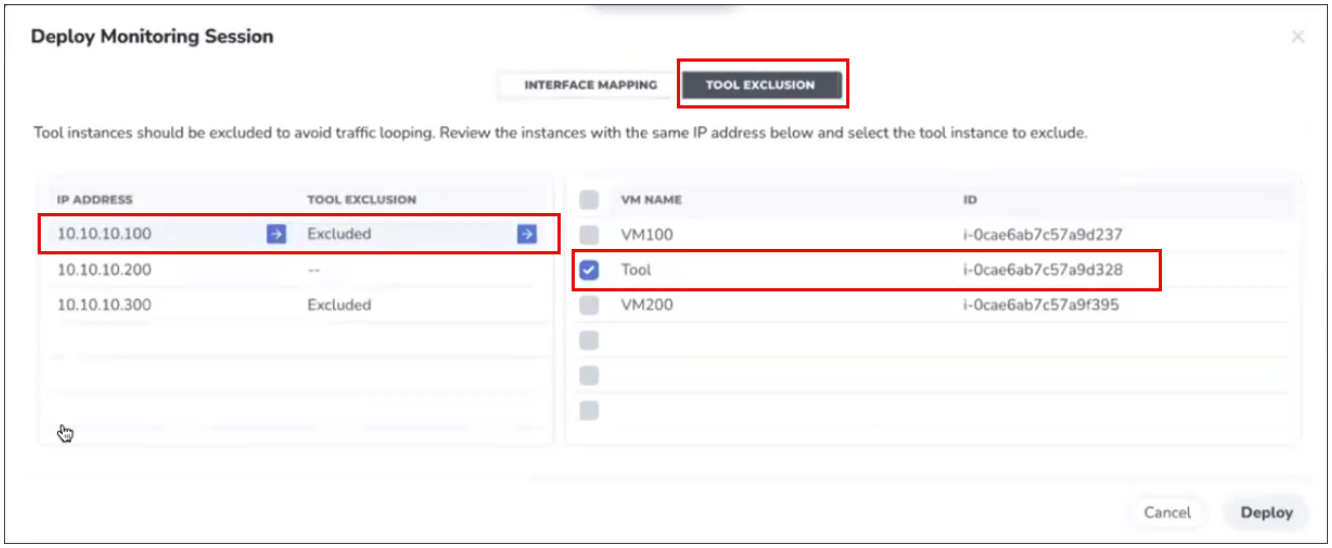
Interface Mapping

It allows to associate specific network interfaces (from monitored instances) with monitoring tools. This ensures that traffic from selected sources is accurately mirrored and routed for analysis. You can:

- Select interfaces from available instances.
- Map each interface to one or more monitoring tools.
- Apply filters or conditions to refine traffic selection.

Tool Exclusion

It excludes specific monitoring tools from receiving mirrored traffic during a monitoring session. This option is available only when the Traffic Acquisition method is set to **VPC Traffic Mirroring**.



- Review the list of available monitoring tools.
- Select the tools to exclude from traffic flow.
- Confirm the exclusion before deploying the session.

View Monitoring Session Statistics

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

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

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

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

Visualize the Network Topology (Third Party Orchestration)

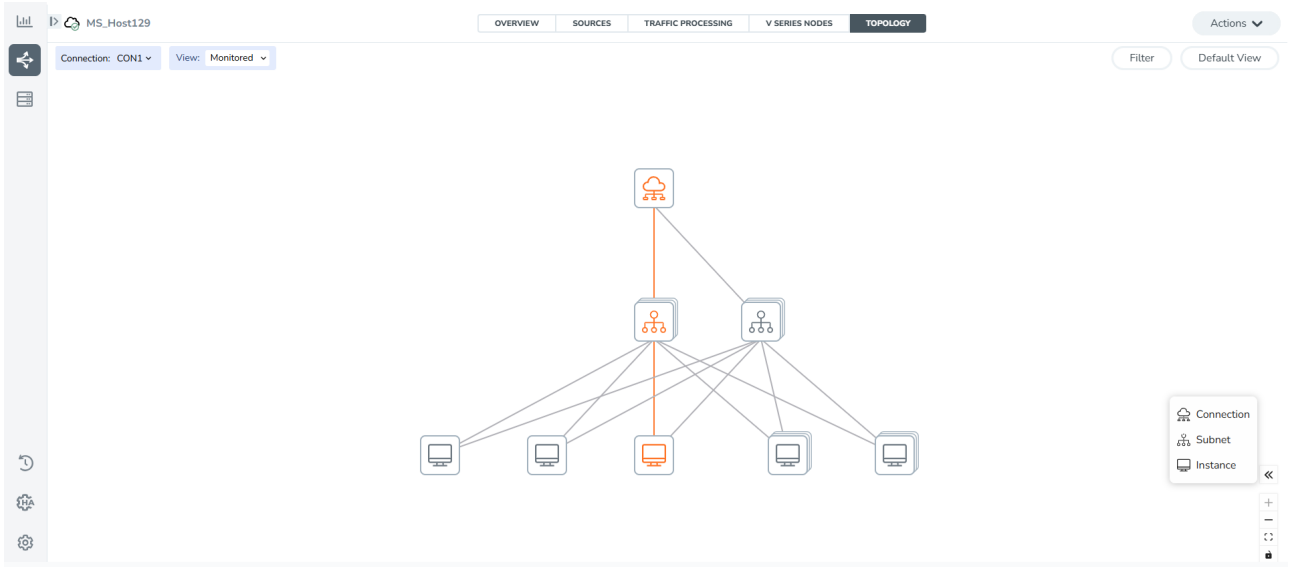
You can have multiple connections in GigaVUE-FM. Each connection can have multiple Monitoring Sessions configured within it. The Topology tab provides a visual representation of the monitored elements within a selected connection and Monitoring Session.

To view the topology in GigaVUE-FM:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Create a Monitoring Session or select an existing Monitoring Session,
3. Open the **TOPOLOGY** tab.
4. From the **Connection** list on the Topology page, select a connection.

   The topology view of the monitored subnets and instances in the selected session is displayed.

5. From **View,** select one of the following instance types:
   - Fabric
   - Monitored



6. (Optional) Hover over the subnet or VM group icons to view details such as the subnet ID, subnet range, and the total number of subnets and instances.
7. Select the subnet or VM group icons to explore the subnets or instances within the group.

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

- Use the **Filter** button to filter the instances based on the VM name, VM IP, OS Type, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitored instances.
- Apply Navigation controls, such as:
  - Use the arrows at the bottom-right corner to move the topology page up, down, left, or right.
  - Use **+** or **-** icons to zoom in and zoom out of the topology view.
  - Select the **Fit View** icon to fit the topology diagram according to the width of the page.

Configure Precryption in UCT-V

GigaVUE-FM allows you to turn on or off the Precryption feature for a monitoring session.

To enable or disable the Precryption feature in UCT-V, refer to Create monitoring session.

Rules and Notes

- To avoid packet fragmentation, change the option precryption-path-mtu in the UCT-V configuration file (**/etc/uctv/uctv.conf**) within the range 1400-9000 based on the platform path MTU.
- Protocol version IPv4 and IPv6 are supported.
- Using IPv6 tunnels requires GigaVUE-FM and the fabric components version 6.6.00 or above.

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

1. On the left pane in GigaVUE-FM, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
   The **Monitoring Sessions** page appears.
2. Select **New** to open the **Create a New Monitoring Session** page.
3. Enter the appropriate information for the monitoring session:
   a. In the **Alias** field, enter the name of the monitoring session.
   b. In the **Monitoring Domain** field, enter the name of the monitoring domain that you want to select.
   c. In the **Connection** field, enter the desired connection(s) to include as part of the monitoring domain. You can select the connections required for the monitoring domain.
4. Select **Next**. The **Edit Monitoring Session** page appears with the new canvas.
5. Select **Options** button. The Monitoring Session options appear.
6. Select the **Precryption** tab.
7. Enable **Precryption**.
8. Select **Save**. The **Edit Monitoring Session** page appears. You can proceed to create map, tunnels, and add applications.

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

Validate Precryption connection

To validate the Precryption connection, follow these steps:

- Navigate to the **Monitoring Session** dashboard and check the Precryption option. The **yes** status indicates an active state.
- Select **Status** to view the rules configured.

Limitations

During precryption, the agent generates a TCP message and captures the payload in clear text. It probes the SSL connect and accept APIs to extract Layer 3 and Layer 4 (L3/L4) details from the packet. When the agent receives the SSL data on a specific interface, it sets the default gateway's MAC address as the destination MAC address for the TCP packet. If the gateway is misconfigured, the agent sets the destination MAC address to all zeros.

Migrate Application Intelligence Session to Monitoring Session

Starting from Software version 6.5.00, you must configure the Application Intelligence solution from Monitoring Session Page. After upgrading to 6.5.00, you cannot create a new Application Intelligence Session or edit an existing Application Intelligence Session for a virtual environment from the **Application Intelligence** page.

The following actions are available only when using the existing Application Intelligence Session:

- View Details
- Delete
- Forced Delete

We recommend to migrate the existing sessions to Monitoring Session for full functionality. GigaVUE-FM seamlessly migrates all your virtual Application Intelligence sessions and their connections. If migration fails, all sessions return to their original states.

Points to Note:

- You must have write access for the **Traffic Control Management** Resource in GigaVUE-FM to perform this migration. For details, refer to Create Roles section In GigaVUE Administration Guide
- The migration does not proceed:
  - If any of the existing Application Intelligence Session is in PENDING or SUSPENDED. Resolve the issue and start the migration process.
  - If any of the existing Application Intelligence Session is in FAILED state due to incorrect configuration. Resolve the issue and start the migration process.
  - If an existing Monitoring Session has the same name as the Application Intelligence Session. Change the existing Monitoring Session name to continue with the migration process.

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

Migrate your existing Application Intelligence **Session to Monitoring Session Page**

Follow these steps:

1. In the left navigation pane, select **Traffic > Solutions >Application Intelligence**. You cannot create a new Application Intelligence Session from this page.When you have an existing virtual Application Intelligence Session in the above page, the **Migrate Virtual Application Intelligence** dialog box appears.
2. Review the message and select **Migrate.**The **Confirm Migration** dialog box appears with the list of Application Intelligence Session that you need to migrate.
3. Review the list and select **Migrate**. GigaVUE-FM verifies the requirements and then migrates the Application Intelligence Sessions to the Monitoring Session Page.
4. Select **Go to Monitoring Session Page.**

You can view that all the virtual Application Intelligence Sessions in the Application Intelligence page are migrated to the Monitoring Session Page.

Post Migration Notes for Application Intelligence

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

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

Cloud Platform	Instance Size	Maximum Number of Flows

   - Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k..
   - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.

   j. Select **Deploy**. For details on how to deploy, refer to Application Intelligence section in the GigaVUE V Series Applications Guide.

2. **Temporary Loss of Statistics with Version Mismatch**

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

3. **Configuration Changes Post-Migration**

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

Monitor Cloud Health

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

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

Configuration Health Monitoring

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

It supports specific fabric components and features on the respective cloud platforms.

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

Refer to the View Health Status section to view the configuration health status.

Traffic Health Monitoring

GigaVUE-FM monitors the traffic health of the entire Monitoring Session and each individual GigaVUE V Series Node in that session. It checks for issues like packet drops or traffic overflows.

When it detects a problem, GigaVUE-FM updates the health status of the related Monitoring Session. It monitors traffic health in near real-time.

The GigaVUE V Series Node tracks traffic levels. If traffic goes above or below the configured threshold, it alerts GigaVUE-FM. Then, GigaVUE-FM then uses this data to calculate traffic health.

If you deploy GigaVUE-FM and GigaVUE V Series Nodes in different cloud platforms, you must add the GigaVUE-FM public IP address as the Target Address in the Data Notification Interface on the Event Notifications page.

For details, refer to the section in the *GigaVUE Administration Guide* .

This feature supports GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

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

For instructions on creating and applying threshold templates across a Monitoring Session or an application, and viewing the traffic health status, refer to the following topics:

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

Consideration to configure a threshold template

- By default, Threshold Template is not configured to any Monitoring Session. If you wish to monitor the traffic health status, then create and apply threshold template to the Monitoring Session.
- Editing or redeploying the Monitoring Session reapplies all the threshold policies associated with that Monitoring Session.
- Deleting the Monitoring Session clears all the threshold policies associated with that Monitoring Session.
- Threshold configuration is applied before deploying a Monitoring Session and remains even if the session is undeployed.
- After applying threshold template to a particular application, you need not deploy the Monitoring Session again.

Supported Resources and Metrics

The following table lists the resources and the respective metrics supported for traffic health monitoring. Refer to Create Threshold Templates and Apply Threshold Template sections for details on Threshold types and Threshold events.

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

TunnelEncapsulation	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
LoadBalancing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SSLDecryption	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Application Metadata	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
AMX	1. Tx Packets 2. Rx Packets 3. Packets Dropped 4. Ingestor - Rx packets 5. Ingestor - Packets Dropped 6. Ingestor - Rx Octets 7. Ingestor - Octets Dropped 8. Ingestor - Records Dropped 9. Workload - Records Dropped 10. Workload - Req Auth Errors 11. Workload - Req Timedout Errors 12. Workload - Req Errors 13. Exporter - Avg File Size 14. Exporter - File Uploads 15. Exporter - File Uploads Errors 16. Enrichment - One Minute Percent	1. Difference 2. Derivative	1. Over 2. Under

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

Create Threshold Templates

To create threshold templates:

1. Go to **Inventory > Resouces > Threshold Templates**.

   The **Threshold Templates** page appears.

2. Select **Create** to open the New Threshold Template page.

3. Enter the appropriate information for the threshold template as described in the following table:

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

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

Apply Threshold Template

You can apply your threshold template across the entire Monitoring Session and also to a particular application.

Apply Threshold Template to Monitoring Session

To apply the threshold template across a Monitoring Session, follow these steps:

1. On the left pane in GigaVUE-FM, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. In the **TRAFFIC PROCESSING** tab, select **Options>Thresholds** menu.
3. From the **Select Template** drop-down list, select the template you wish to apply across the Monitoring Session.
4. Select **Apply**.

NOTE: You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

Apply Threshold Template to Applications

Applying threshold template across Monitoring Session does not overwrite the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it overwrites the existing threshold value for that particular application.

To apply the threshold template to a particular application in the Monitoring Session, follow these steps:

1. On the **Monitoring Session** page, select **TRAFFIC PROCESSING** tab. The Monitoring Session canvas page appears.
2. Select on the application for which you wish to apply or change a threshold template and select **Details**. The **Application** quick view opens.
3. Select the **Thresholds** tab.
4. Select the template you wish to apply from the Threshold Template drop-down menu or enter the threshold values manually.
5. Select **Save**.

Clear Thresholds

You can clear the thresholds across the entire Monitoring Session and also to a particular application.

Clear Thresholds for Applications

To clear the thresholds of a particular application in the Monitoring Session, follow these steps:

1. On the **Monitoring Session** page, select the **TRAFFIC PROCESSING** tab. The Monitoring Session canvas page appears.
2. Select the application for which you wish to clear the thresholds and click **Details**. The **Application** quick view opens.
3. Select the **Thresholds** tab.
4. Select **Clear All** and then select **Save**.

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a Monitoring Session, follow these steps:

1. On the left navigation pane in GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Select the Monitoring Session and navigate to **TRAFFIC PROCESSING > Options > Thresholds**,
3. Select **Clear Thresholds**.
4. On the **Clear Threshold** pop-up appears, select **Ok**.

NOTE: Clearing thresholds at Monitoring Session level does not clear the thresholds that were applied specifically at the application level. To clear thresholds for a particular application, refer to Clear Thresholds for Applications

View Health Status

You can view the health status of the Monitoring Session on the Monitoring Session details page. The health status of the Monitoring Session is healthy only if both the configuration health and traffic health are healthy.

View Health Status of an Application

To view the health status of an application across an entire Monitoring Session,

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
2. Select a Monitoring Session and navigate to the **TRAFFIC PROCESSING** tab.
3. Select the application for which you wish to see the health status and select **Details**. The quick view page appears.
4. Select the **HEALTH STATUS** tab.

This displays the application's **Configuration Health**, **Traffic Health**, and the **Operational Health**, along with the thresholds applied to each.

NOTE: The secure tunnel status is refreshed every 5 minutes, and the GigaVUE-FM does not display UCT-V secure tunnel status that is older than 7 minutes. If the secure tunnel in the UCT-V is removed, it takes up to 7 minutes to reset the status on the GigaVUE-FM.

View Operational Health Status of an Application

When you configure the Application Metadata Exporter to use **Kubernetes** as the workload platform, the V Series Node transmits failure and error events to GigaVUE-FM, which processes them and updates the node's health status on the Monitoring Session page. When interacting with Kubernetes workloads, the system may encounter errors while retrieving resources such as pods, services, nodes, or endpoints. Refer to Errors for additional error details.

Operational events for Exporter:

Refer below for message format and messages that indicate common issues that can occur during the operations:

Format: <Server Type>_<Message>

Server Types: CLOUD EXPORT, KAFKA

Message	Description
UPLOAD_MAX_TRIES_EXCEED	Upload retries exceeded the maximum limit **Example**: CLOUDEXPORTER_UPLOAD_MAX_TRIES_EXCEED
REACHABILITY_FROM_AMX_TO_TOOLS	AMX failed to reach the tool (Cloud Exporter server or Kafka server) **Example**: CLOUDEXPORTER_REACHABILITY_FROM_AMX_TO_TOOLS
NO_IP_ADDRESS	No IP address was configured on the interface **Example**: CLOUDEXPORTER_NO_IP_ADDRESS
EXPORTER_UPLOAD_ERROR	Upload to the exporter failed **Example**: CLOUDEXPORTER_EXPORTER_UPLOAD_ERROR
EXPORTER_ERR_EVENT_CONTEXT_DEADLINE_EXCEEDED	The exporter health-monitor probe or upload to the tool timed out. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_CONTEXT_DEADLINE_EXCEEDED KAFKA_EXPORTER_ERR_EVENT_CONTEXT_DEADLINE_EXCEEDED
EXPORTER_ERR_EVENT_CONTEXT_CANCELED	The exporter health-monitor probe or upload was canceled before completion, typically due to shutdown or reconfiguration. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_CONTEXT_CANCELED KAFKA_EXPORTER_ERR_EVENT_CONTEXT_CANCELED

Message	Description
EXPORTER_ERR_EVENT_DNS_LOOKUP_FAIL	The hostname of the configured Kafka broker or Cloud Exporter endpoint could not be resolved due to a DNS failure. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_DNS_LOOKUP_FAIL KAFKA_EXPORTER_ERR_EVENT_DNS_LOOKUP_FAIL
EXPORTER_ERR_EVENT_NETWORK_UNREACHABLE	The exporter probe failed at the network layer, for example, due to no route to the host or an unreachable network. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_NETWORK_UNREACHABLE KAFKA_EXPORTER_ERR_EVENT_NETWORK_UNREACHABLE
EXPORTER_ERR_EVENT_TRASPORT_LAYER_ERR	The exporter probe failed at the transport layer, such as connection refusal, TCP reset, or TLS handshake failure. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_TRASPORT_LAYER_ERR KAFKA_EXPORTER_ERR_EVENT_TRASPORT_LAYER_ERR

Operational events for Enrichment:

Refer below for message format and messages that indicate common issues that can occur during the operations:

Format: <Operation Type>_<Message>

Operation Types: GETSERVICES, GETPODS, GETNODES, GETENDPOINTSLICES, WATCHALL

Message	Description
K8S_AUTHORIZATION_FAILURE	The request was denied due to insufficient permissions **Example**: GETPODS_K8S_AUTHORIZATION_FAILURE
K8S_AUTHENTICATION_FAILURE	Authentication failed. Verify your credentials **Example**: GETPODS_K8S_AUTHENTICAION_FAILURE
K8S_UNHANDLED_ERROR	An unspecified error occurred. Check the error description **Example**: GETPODS_K8S_UNHANDLED_ERROR

View Health Status for Individual GigaVUE V Series Nodes

You can also view the health status of an individual GigaVUE V Series Node. To view the configuration health status and traffic health status of the V Series Nodes:

1. On the Monitoring Session page, select the required Monitoring Session from the list view.
2. In the **Overview** tab, view the health status of the required GigaVUE V Series Node from the chart options.

View Application Health Status for Individual V Series Nodes

To view the application configuration and traffic health status of the GigaVUE V Series Nodes:

1. On the Monitoring Session page, select the required Monitoring Session from the list view.
2. On the Overview tab, select the GigaVUE V Series Node from the All V Series Nodes drop-down menu.

   The list view displays the list of applications for the selected GigaVUE V Series Node and the health status of each application.

Administer GigaVUE Cloud Suite for Third Party Orchestration

You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for AWS:

- Configure Third Party Orchestration Settings
- Role Based Access Control

Configure Certificate Settings

To configure certificate settings:

1. Go to **Inventory > VIRTUAL**.
2. Select your cloud platform.
3. Select **Settings > Certificate Settings**.
   The **Certificate Settings** page appears.
4. From the **Algorithm** drop-down list, select the algorithm that determines the cryptographic security of the certificate.

   NOTE: If selecting RSA 8192, the certificate generation may take longer due to the increased key size.
5. In the **Validity** field, enter the total validity period of the certificate.

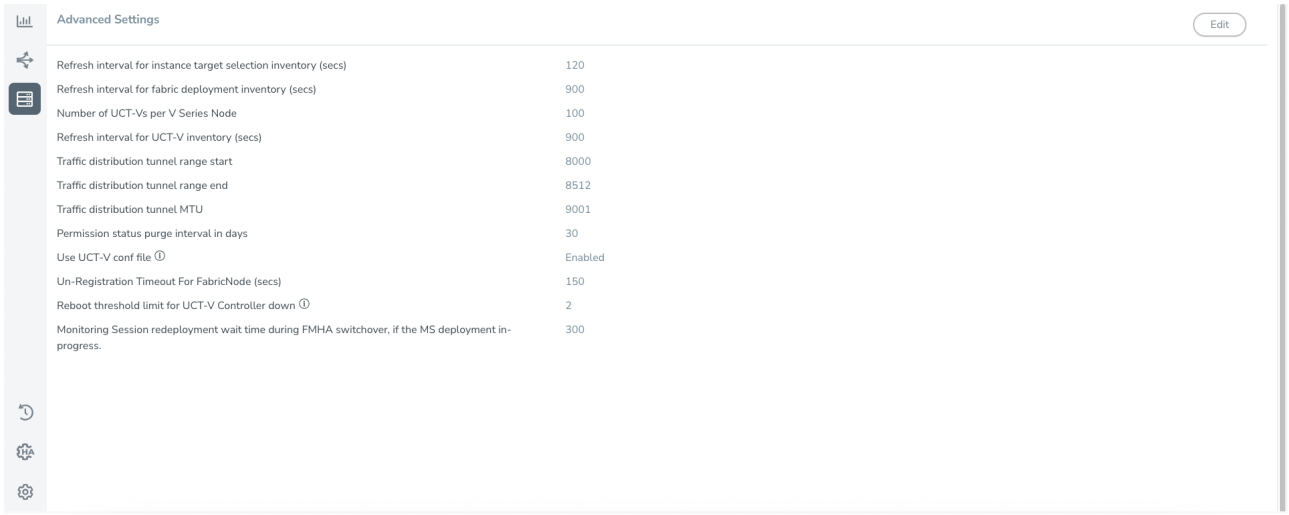
6. In the **Auto Renewal** field, enter the number of days before expiration of the auto-renewal process should begin.
7. Select **Save**.

Configure Third Party Orchestration Settings

This topic allows you to set the maximum number of connections, adjust refresh intervals for instance and non-instance inventory, and define the maximum batch size for monitoring session updates.

To configure these settings,

1. In GigaVUE-FM, go to **Inventory > VIRTUAL > Third-Party Orchestration**.
2. Select **Settings**.
3. In the **Settings** page, select the **Advanced** tab and update the required values.



Settings	Description
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of the instances.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for deploying the fabric components
Number of UCT-Vs per V Series Node	Specifies the maximum number of UCT-Vs that you can assign to the GigaVUE V Series Node. **Points to Note:** • At the time of GigaVUE V Series Node deployment, GigaVUE-FM maps the UCT-Vs equally to all the available GigaVUE V Series Node. For example, there are 10 UCT-Vs, two GigaVUE V Series Nodes, and 10 f

Settings	Description
	UCT-Vs per V Series Node. Even though the first GigaVUE V Series Node can accommodate all the ten UCT-Vs, it is shared equally between the two GigaVUE V Series Node to balance the traffic load. • When a new GigaVUE V Series Node is added to the deployment, GigaVUE-FM does not re-balance the UCT-Vs to the new GigaVUE V Series Node unless the number of UCT-Vs mapped to the GigaVUE V Series Node is greater than the Number of UCT-Vs per V Series Node.
Refresh interval for UCT-V inventory (secs)	Specifies the frequency for discovering the UCT-Vs available. **Note**: When you upgrade to version 6.5 or above, GigaVUE-FM resets the UCT-V Refresh Interval field to its default. To retain your custom value, you must manually reconfigure it.
Traffic distribution tunnel range start	Specifies the start range value of the tunnel ID.
Traffic distribution tunnel range end	Specifies the closing range value of the tunnel ID.
Traffic distribution tunnel MTU	Specifies the MTU value for the traffic distribution tunnel.
Use UCT-V conf file	Enable this option to allow interface mirroring to follow the configuration defined in the file. Disable it to mirror traffic from all physical interfaces. **Note**: • When changing the UCT-V conf file option from **enabled to disabled**, ensure to undeploy the Monitoring Session and delete the Monitoring Domain. Once changed, you should create a new Monitoring Domain and configure the Monitoring Session. • When changing the UCT-V conf file option from **disabled to enabled**, do the following: 1. Edit the uctv.conf file a. **Windows**: C:\ProgramData\Uctv\uctv.conf b. **Linux**: /etc/uctv/uctv.conf 2. Delete the skipConf file from the backup folder a. **Windows**: C:\ProgramData\Uctv\bak\skipConf b. **Linux**: /var/lib/uctv/bak/skipConf 3. Restart the UCT-V a. **Windows**: Restart from the Task Manager b. **Linux**: sudo service uctv restart
Reboot threshold limit for UCT-V Controller down	Specifies the number of times GigaVUE-FM tries to reach UCT-V Controllerr. When the UCT-V Controller moves to down state. GigaVUE-FM retries every 60 seconds.

Role Based Access Control

The Role Based Access Control (RBAC) feature controls the access privileges of users and restricts users from either modifying or viewing unauthorized data. Access privileges in GigaVUE Cloud Suite works on the same principles of access privileges in GigaVUE-FM in which the access rights of a user depends on the following:

- **User role:** A user role defines permission for users to perform any task or operation
- **User group**: A user group consists of a set of roles and set of tags associated with that group. You can associate a new user with one or more groups.

To access the resources and to perform a specific operation in GigaVUE Cloud Suite, a user needs **fm_super_admin** role or write access to the following resource category depending on the task to perform:

Resource Category	Cloud Configuration Task
Physical Device Infrastructure Management: This includes the following cloud infrastructure resources: • Cloud Connections • Cloud Proxy Server (for AWS and Azure) • Cloud Fabric Deployment • Cloud Configurations • Sys Dump • Syslog • Cloud licenses • Cloud Inventory	• Configure GigaVUE Cloud Components • Create Monitoring Domain and Launch Visibility Fabric • Configure Proxy Server (applicable only to AWS and Azure)
Traffic Control Management: This includes the following traffic control resources: • Monitoring session • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps	• Create, Clone, and Deploy Monitoring Session • Add Applications to Monitoring Session • Create Maps • View Statistics • Create Tunnel End Points
Third Party Orchestration: This includes the following resource: • Cloud Orchestration	Deploy the fabric components using Third Party Orchestration. Refer toConfigure Role-Based Access for Third Party Orchestration for more details on how to create users, roles, and user groups for Third Party Orchestration.

NOTE: Cloud APIs are also RBAC enabled.

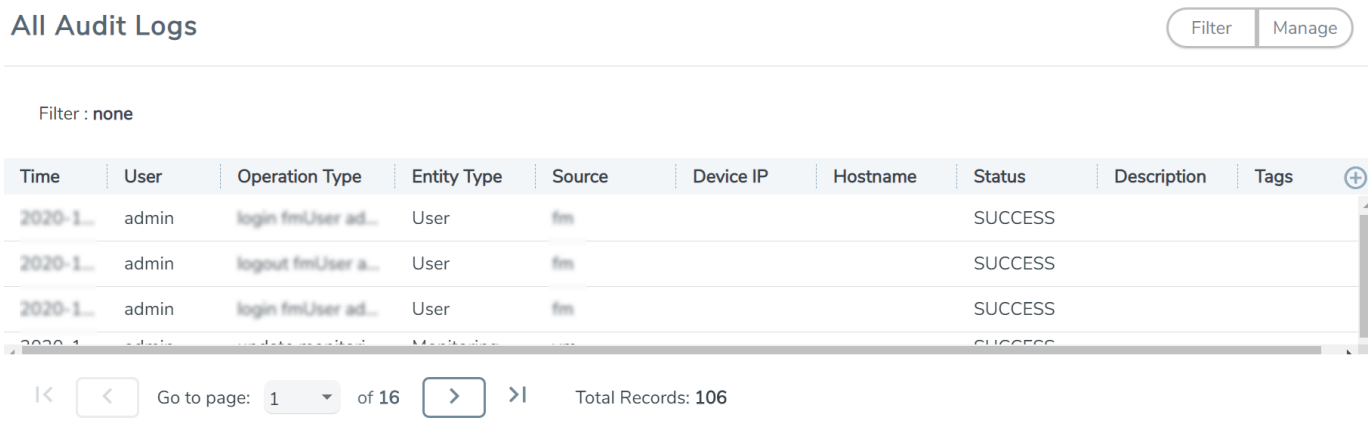
For detailed information about Roles, Tags, User Groups, refer to the *GigaVUE Administration Guide*.

About Audit Logs

Audit logs track the changes and activities that occur in the virtual nodes due to user actions. You can filter the logs to view specific information.

Access Audit Logs

Navigate to **Dashboard > SYSTEM > Audit Logs**. The **All Audit Logs** page appears.



Parameters

The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that the system logs. For example, ▪ Log in and Log out based on users. ▪ Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details about the usage either in GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	For failed status provides a brief update on the reason..

NOTE: Verify if the GigaVUE-FM time is set correctly to ensure accuracy of the captured trending data.

Filtering the audit logs

You can filter to view specific type of logs based on the following criteria:

- **When**: Displays logs that occurred within a specified time range.
- **Who**: Displays logs related to a particular user or users.
- **What**: Displays logs for one or more operations, such as Create, Read, and Update.
- **Where**: Displays logs for GigaVUE-FM or devices.
- **Result**: Displays logs for success or failure.

To filter the audit logs,

1. Select **Filter**.

   A quick view for Audit Log Filters displays.

2. Specify one or all of the following:

   - **Start Date** and **End Date** to display logs within a specific time range.
   - **Who** limits the scope of what displays on the Audit Logs page to a specific user or users.
   - **What** narrows the logs to the types of operation that the log is related to. You can select multiple operations. Select **All Operations** to apply all operation types as part of the filter criteria.
   - **Where** narrows the logs to particular of system that the log is related to. Select **All Systems** apply both GigaVUE-FM and device to the filter criteria. **Result** narrows the logs related to failures or successes. Select **All Results** to apply both success and failure to the filter criteria.

3. Select **OK** to apply the selected filters to the **Audit Logs** page.

Debuggability and Troubleshooting

Use the following information to help diagnose and resolve GigaVUE V Series Nodes issues.

Sysdumps

A sysdump is a log and system data package generated when a GigaVUE V Series Node experiences a crash (such as kernel, application, or hardware failure). These files are essential for debugging.

You cannot download sysdump files if the associated fabric component is deleted or unreachable.

Sysdumps—Rules and Notes

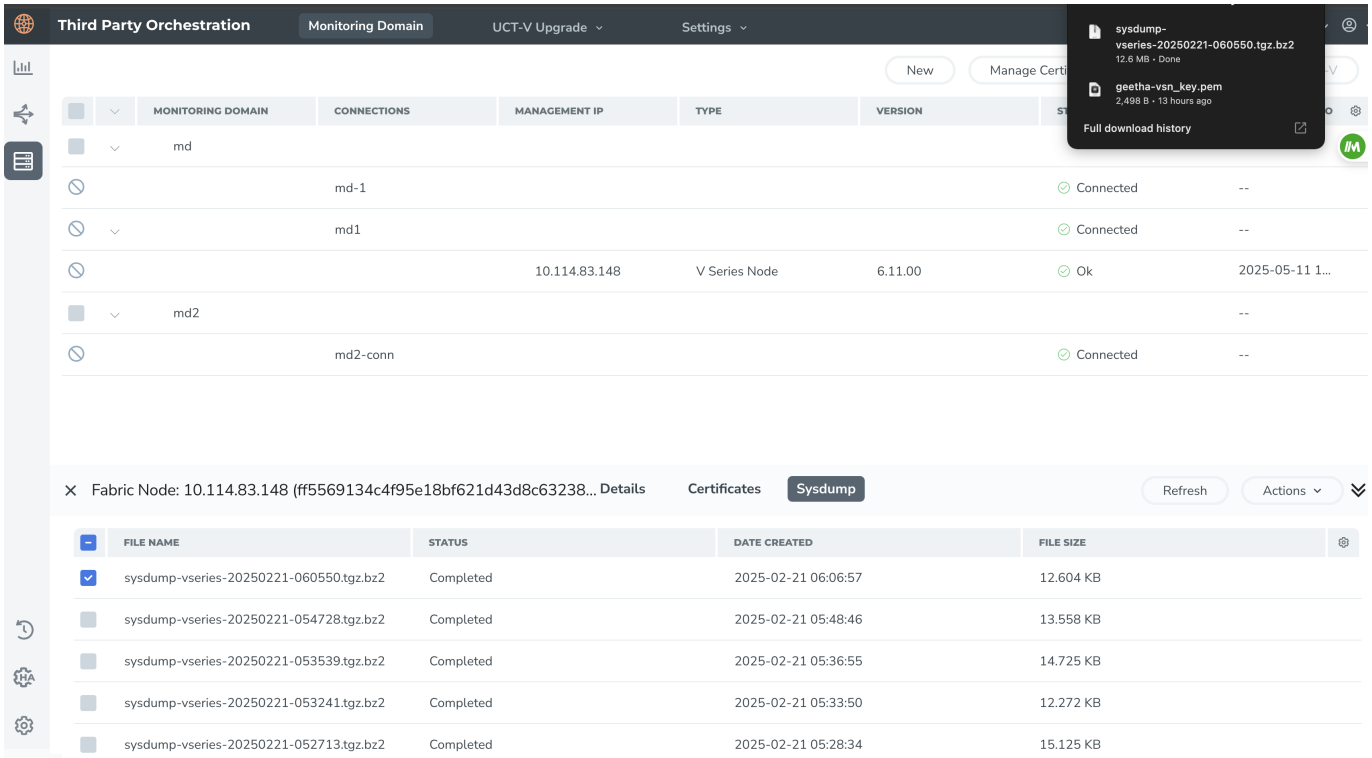
Consider the following points before you generate sysdumps:

- You can generate only one sysdump file at a time for a GigaVUE V Series Node.
- You cannot generate a sysdump file when generation of another sysdump file is in progress.
- The limit of sysdump files available per GigaVUE V Series Node is six. When you generate a seventh sysdump file, the file overwrites the first sysdump file.
- You can download only one sysdump file per GigaVUE V Series Node at a time.
- You can delete sysdump files in bulk for a GigaVUE V Series Node.
- To ensure efficient usage, the system limits the number of simultaneous sysdump generation requests to 10 GigaVUE V Series Nodes.
- GigaVUE V Series Node sysdumps are not stored in Fabric Manager but generated and stored on the GigaVUE V Series Node itself.

Generate a Sysdump File

To generate a sysdumps file:

1. Select the required node, and use one of the following options to generate a sysdump file:
   - Select **Actions > Generate Sysdump**.
   - In the lower pane, go to **Sysdump**, and select **Actions > Generate Sysdump**.
2. View the latest status, click **Refresh**.



Other Actions

- To download a sysdump file, select the file in the lower pane, and then click **Actions > Download**.
- To delete a sysdump file,
    1. Select the file in the lower pane.
    2. Select the desired sysdump file.
    3. Select **Actions > Delete**.
- To bulk delete, select all the sysdump files, and then select **Actions > Delete All.**

FAQs - Secure Communication between GigaVUE Fabric Components (Third Party Orchestration)

This section addresses frequently asked questions about Secure Communication between GigaVUE Fabric Components and GigaVUE-FM. Refer to Secure Communication between GigaVUE Fabric Components section for more details.

1. **Is there a change in the upgrade process for GigaVUE-FM and GigaVUE V Series Node?**

   No. The upgrade process remains unchanged across all supported upgrade paths. You can upgrade your nodes without any additional steps. The upgrade results in the automatic deployment of the appropriate certificates based on the node versions

GigaVUE-FM	GigaVUE V Series Nodes	Custom Certificates Selected (Y/N)	Actual Node Certificate
6.10	6.10	Y	GigaVUE-FM PKI Signed Certificate
6.10	6.9 or earlier	Y	Custom Certificate
6.10	6.9 or earlier	N	Self-Signed Certificate

2. **What is the new authentication type used between GigaVUE-FM and the GigaVUE Fabric Components? Is backward compatibility supported?**

   Backward compatibility is supported, ensuring that fabric components running on version 6.9 or earlier remain compatible with GigaVUE-FM 6.10. The following authentication types are supported across different versions:

GigaVUE-FM	GigaVUE Fabric Components	Authentication
6.10	6.10	Tokens + mTLS Authentication (Secure Communication)
6.10	6.9 or earlier	User Name and Password

3. **What are the new ports that must be added to the security groups?**

   The following table lists the port numbers that must be opened for the respective fabric components:

Component	Port
GigaVUE-FM	9600
GigaVUE V Series Node	80, 8892
GigaVUE V Series Proxy	8300, 80, 8892
UCT-V Controller	8300, 80
UCT-V	8301, 8892, 9902 For more details, refer to Network Firewall Requirement.

4. **Is the registration process different for deploying the fabric components using Third-Party Orchestration?**

   Yes. Beginning with version 6.10, you must use tokens in the gigamon-cloud.conf file instead of the username and password. To generate the token in GigaVUE-FM, go to **Settings > Authentication > User Management > Token**. For more details, refer to Configure Tokens.

   Example Registration Data for UCT-V:

   ```
   #cloud-config
    write_files:
    - path: /etc/gigamon-cloud.conf
      owner: root:root
      permissions: '0644'
      content: |
        Registration:
           groupName: <Monitoring Domain Name>
           subGroupName: <Connection Name>
           token: <Token>
           remoteIP: <IP address of the UCT-V Controller 1, <IP address of the UCT-V Controller
   2>
           sourceIP: <IP address of UCT-V> (Optional Field)
   ```

5. **Are there any changes to the UCT-V manual installation and upgrade process?**

   Starting from version 6.10, you must add tokens during manual installation and upgrades.

   - Create a configuration file named gigamon-cloud.conf with the token and place it in the /tmp directory during UCT-V installation
   - After installing UCT-V, you can add the configuration file in the /etc directory.

   Important! Without this token, UCT-V cannot register with GigaVUE-FM.

6. **Can I use my PKI infrastructure to issue certificates for the Fabric Components?**

   Direct integration of your PKI with GigaVUE-FM is not supported. However, you can provide your Intermediate Certificate Authority (CA) to sign the node certificate.

7. **What happens to the existing custom certificates introduced in the 6.3 release?**

   The custom certificate feature is not supported for the fabric components with version 6.10 or higher, even if a custom certificate is selected in the Monitoring Domain. However, this feature remains available for older versions.

   - When upgrading from version 6.9 or earlier with custom certificates upgrades to version 6.10, the system automatically generates and deploys certificates signed by GigaVUE-FM.
   - If deploying version 6.9 or earlier components from a 6.10 GigaVUE-FM, custom certificates are still applied.

8. **How to issue certificates after upgrading the fabric components to 6.10?**

   When the upgrade process begins, GigaVUE-FM transmits the certificate specifications to the new fabric components using the launch script. The fabric components utilize these specifications to generate their own certificates.

9. **Is secure communication supported in FMHA deployment?**

   Yes, it is supported. However, you must follow a few manual steps before upgrading the fabric components to 6.10. For details, refer to Configure Secure Communication between Fabric Components in FMHA.

   NOTE: This step is essential if you are using cloud deployments in FMHA mode and would like to deploy or upgrade the fabric components to version 6.10 or later.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The VÜE Community

Documentation

©This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view What's New to access quick links to topics for each of the new features in this Release; view Documentation Downloads to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.14 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide

GigaVUE Cloud Suite 6.14 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA400E Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide
GigaVUE Inline Solutions Guide(**NEW**) (previously included in the **GigaVUE Fabric Management Guide**)
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)

GigaVUE Cloud Suite 6.14 Hardware and Software Guides
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud TAP - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices Sanitization guidelines for GigaVUE Fabric Management Guide and GigavUE-OS devices.
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **Note**: Release Notes are not included in the online documentation. **Note**: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to My Gigamon. Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to My Gigamon.
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to: documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	

For Online Topics	**Online doc link**	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*
For PDF Topics	**Document Title**	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	**Describe the issue**	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? **Be as specific as possible.**	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings** **> Support > Contact Support** in GigaVUE-FM.

You can also refer to https://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The VÜE Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)