



GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

GigaVUE Cloud Suite

Product Version: 6.4

Document Version: 1.0

Last Updated: Tuesday, February 27, 2024

(See Change Notes for document updates.)

Copyright 2024 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
6.4.00	1.0	09/08/2023	The original release of this document with 6.4.00 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 11
 - Virtual Dashboard Widgets 11
- Get Started with Third Party Orchestration** **13**
 - License information 13
 - Volume-Based License 13
 - Base Bundles 14
 - Add-on Packages 14
 - How GigaVUE-FM Tracks Volume-Based License Usage 15
 - Apply License 19
 - Network Firewall Requirement 19
 - Configure Role-Based Access for Third Party Orchestration 21
 - Users 21
 - Add Users 21
 - How to Unlock User Account 24
 - Create Roles 24
 - Create Roles 24
 - Create User Groups 27
 - Create User Groups 28
- Deployment Options for GigaVUE Cloud Suite for Third Party Orchestration** **30**
 - Deploy GigaVUE Fabric Components using Generic Mode 31
 - Without Creating Monitoring Domain 31
 - By Creating Monitoring Domain 32
 - Deploy GigaVUE Fabric Components using Integrated Mode 33

- Deploy GigaVUE Cloud Suite for Third Party Orchestration34**
- Install GigaVUE-FM35
- Prepare UCT-V to Monitor Traffic35
 - Supported Operating Systems for UCT-V36
 - Linux UCT-V Installation36
 - Windows UCT-V Installation41
- Uninstall UCT-V45
 - Uninstall Linux UCT-V45
 - Uninstall Windows UCT-V46
- Upgrade or Reinstall UCT-V46
- Install Custom Certificate46
 - Upload Custom Certificates using GigaVUE-FM47
 - Upload Custom Certificate using Third Party Orchestration47
- Adding Certificate Authority48
- CA List48
- Modes of Deployments48
- Create Monitoring Domain49
- Deploy Fabric Components using Generic Mode51
 - Configure GigaVUE Fabric Components using AWS51
 - Configure GigaVUE Fabric Components using Azure60
 - Configure GigaVUE Fabric Components using GCP71
 - Configure GigaVUE Fabric Components using Nutanix85
 - Configure GigaVUE Fabric Components using OpenStack94
 - Configure GigaVUE V Series Nodes using VMware ESXi102
 - Configure GigaVUE Fabric Components using VMware vCenter104
 - Configure GigaVUE Fabric Components using Third Party Orchestration on NSX-T Federation Environment108
- Deploy Fabric Components using Integrated Mode111
- Configure Monitoring Session111**
- Create a Monitoring Session112
 - Edit Monitoring Session113
 - Enable Prefiltering, Precryption, and Secure Tunnel114
 - Prefiltering115
- Interface Mapping117
- Create Ingress and Egress Tunnel117
- Create Raw Endpoint124
- Create a New Map125
 - Example- Create a New Map using Inclusion and Exclusion Maps129
- Add Applications to Monitoring Session129
- Deploy Monitoring Session130
- View Monitoring Session Statistics132

View Health Status on the Monitoring Session Page	133
Health	133
V Series Node Health	133
Target Source Health	134
Visualize the Network Topology	134
Configure Application Intelligence Solutions on GigaVUE V Series Nodes using Third Party Orchestration	135
Generic Mode	135
Integrated Mode	136
Configure Environment	136
Create Environment	137
Create Credentials	138
Create AWS Credentials	138
Create Azure Credentials	138
Create Connection	139
Connect to AWS	140
Connect to Azure	141
Connect to VMware ESXi	142
Connect to VMware NSX-T	142
Create Source Selectors	144
Create Tunnel Specifications	146
User Defined Application	148
Create Rules under User Defined Application	148
Supported Protocols and Attributes	149
Mindata	153
Supported RegExp Syntax	153
Limitations	154
Configure Application Intelligence Session	154
Prerequisites	155
Create an Application Intelligence Session in Virtual Environment	155
Slicing and Masking in Application Filtering Intelligence	158
Configuring Application Filtering Intelligence with Slicing	158
Configuring Application Filtering Intelligence with Masking	158
Configuring Application Filtering Intelligence with Slicing and Masking	159
Application Metadata Intelligence	159
Create Application Metadata Intelligence Session for Virtual Environment	160
Create NetFlow Session for Virtual Environment	164
NetFlow Dashboard	168
Secure Tunnels	169
Supported Platforms	170

Configure Secure Tunnel for Third Party Orchestration	170
Precrypted Traffic	170
Mirrored Traffic	170
Prerequisites	171
Configure Secure Tunnel from UCT-V to GigaVUE V Series Node	171
Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2	172
Edit SSL Configuration	175
Viewing Status of Secure Tunnel	176
Precription™	176
How Gigamon Precryption Technology Works	177
Why Gigamon Precryption	177
Key Features	178
Key Benefits	178
How Gigamon Precryption Technology Works	178
Precryption Technology on Single Node	179
Precryption Technology on Multi-Node	179
Supported Platforms	180
Prerequisites	181
Note	181
Configure Precryption in UCT-V	182
Monitor Cloud Health	183
Configuration Health Monitoring	183
Traffic Health Monitoring	184
Create Threshold Template	185
Apply Threshold Template	186
Edit Threshold Template	186
Supported Resources and Metrics	187
View Health Status	189
Administer GigaVUE Cloud Suite for Third Party Orchestration	191
Configure Third Party Orchestration Settings	191
Role Based Access Control	192
GigaVUE-FM Version Compatibility Matrix	193
GigaVUE-FM Version Compatibility	194
Additional Sources of Information	195
Documentation	195
How to Download Software and Release Notes from My Gigamon	197
Documentation Feedback	198
Contact Technical Support	199
Contact Sales	199

Premium Support	200
The VUE Community	200
Glossary	201

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

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

Topics:

- [Overview of Third Party Orchestration](#)
- [Get Started with Third Party Orchestration](#)
- [Deploy GigaVUE Cloud Suite for Third Party Orchestration](#)
- [Configure Monitoring Session](#)
- [Configure Application Intelligence Solutions on GigaVUE V Series Nodes using Third Party Orchestration](#)
- [Secure Tunnels](#)
- [Precryption™](#)
- [Monitor Cloud Health](#)
- [Administer GigaVUE Cloud Suite for Third Party Orchestration](#)
- [GigaVUE-FM Version Compatibility Matrix](#)

Overview of Third Party Orchestration

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

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

- GigaVUE® Fabric Manager (GigaVUE-FM)
- UCT-Vs
- UCT-V Controllers

- GigaVUE V Series Proxy
- GigaVUE V Series Nodes

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

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

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

The images of the components are available in the [Gigamon Customer Portal](#) and the images for public clouds are available in the respective market place.

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

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

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

Components for Third Party Orchestration

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

Component	Description
GigaVUE® Fabric Manager (GigaVUE-FM)	GigaVUE-FM is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud. You are responsible for launching GigaVUE-FM from your end on the supported cloud or enterprise platforms.
UCT-V (earlier known as G-vTAP Agent)	UCT-V is an agent that is installed in your Virtual Machine (VM). This agent mirrors the selected traffic from the VMs to the GigaVUE® V Series node. The UCT-V is offered as a Debian (.deb), Redhat Package Manager (.rpm) or windows package. Refer to Install UCT-Vs .
Next generation UCT-V (earlier known as Next Generation G-	Next generation UCT-V is a lightweight solution that acquires traffic from Virtual Machines and in-turn improves the performance of the UCT-V mirroring capability. The solution has a prefiltering capability at the tap level that reduces the traffic flow from the agent to V Series node and in-turn reduces the V Series load. Next generation UCT-V gets activated only on

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

Cloud Overview Page

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

Go to **Traffic > Virtual > Orchestrated Flows > Overview**. The Cloud Homepage appears.

Virtual Dashboard Widgets

This section describes the widgets that can be viewed on the overview page.

- Overview
- V Series Alarms
- Connection Status
- Usage (VBL)
- Summary (Monitoring Session details)
- Traffic Rate
- Aggregate Summary

Overview

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

V Series Alarms

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

Connection Status

The connection status presents a pie chart that helps you to quickly view the connection status of connections configured in the monitoring domain. Each type of connection status is assigned a color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of connected.

Usage

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

Summary

This widget allows you to view the list of all the available monitoring session along with the respective monitoring domain, platform, connection, their health status, V Series Node health status and the deployment status of the connection. You can click on the monitoring session name to view the **Edit Monitoring session** page of the respective monitoring session.

Traffic Rate

The traffic rate widget displays the rate of traffic flowing through the GigaVUE V Series Nodes. Each line in the graph indicates the rate of traffic flow for transmitting, receiving, and their ratio which is specified by the legend.

Aggregate Summary

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

Get Started with Third Party Orchestration

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

Refer to the following sections for details:

- [License information](#)
- [Network Firewall Requirement](#)
- [Configure Role-Based Access for Third Party Orchestration](#)

License information

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

Volume-Based License

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

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

Volume-based licenses are available as monthly subscription licenses with a service period of 1 month. Service period is the period of time for which the total usage or overage is tracked. There is a grace period for each license that is encoded in the license file. The license effectively provides data allowance for this additional time after the official end time of the license.

For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales. Refer to [Contact Sales](#).

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUEPlus

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

Bundle Replacement Policy

Refer to the following notes:

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

Add-on Packages

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

Rules for add-on packages:

- Add-on packages can only be added when there is an active base bundle available in GigaVUE-FM.
- The base bundle limits the total volume usage of the add-on package.

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

- If your add-on package has volume allowance less than the base bundle, then your add-on package can only handle volume allocated for add-on package.
- When the life term of an add-on package extends beyond the base bundle, then when the base bundle expires, the volume allowance of the add-on package will be reduced to zero until a new base bundle is added.

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

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

How GigaVUE-FM Tracks Volume-Based License Usage

GigaVUE-FM tracks the license usage for each V series node as follows:


- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only those applications that are licensed at that point (applicable only for ACTIVE licenses, licenses in grace period are not included).
- When a license goes into grace period, you will be notified with an audit log.
- When a license finally expires (and has not been renewed yet), you will be notified by an audit log. Monitoring sessions using the corresponding license will not be undeployed.

For releases prior to 6.4:

- The monitoring sessions using the corresponding license will be undeployed (but not deleted from the database).
- When a license is later renewed or newly imported, any undeployed monitoring sessions are redeployed.

Manage Volume-based Licenses

To manage active Volume-based License:

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

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

Field	Description
SKUs	Unique identifier associated with the license
Bundles	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

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

The expired licenses are displayed in the **VBL Inactive** page, which can be found under the **FM/Cloud** drop-down in the top navigation bar. This page lists the following information about the inactive Volume-based Licenses:

Field	Description
SKUs	Unique identifier associated with the license.
Bundles	Bundle to which the license belongs to.
Ends	License end date
Grace Period	Number of days the license is in grace period
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 VBL Inactive page. To display these fields, click on the column setting configuration option and enable these fields.

Use the following buttons to manage your VBL.


Button	Description
Activate Licenses	Use this button to activate a Volume-based License. Refer to Activate Volume-based Licenses for more information.
Email Volume Usage	Use this button to send the volume usage details to the email recipients.
Filter	Use this button to narrow down the list of active Volume-based Licenses that are displayed on the VBL active page.
Export	Use this button to export the details in the VBL active page to a CSV or XLSX file.
Deactivate	Use this button to deactivate the licenses. You can only deactivate licenses that are in grace period or that have expired.

For more detailed information on dashboards and reports 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 Licensed 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

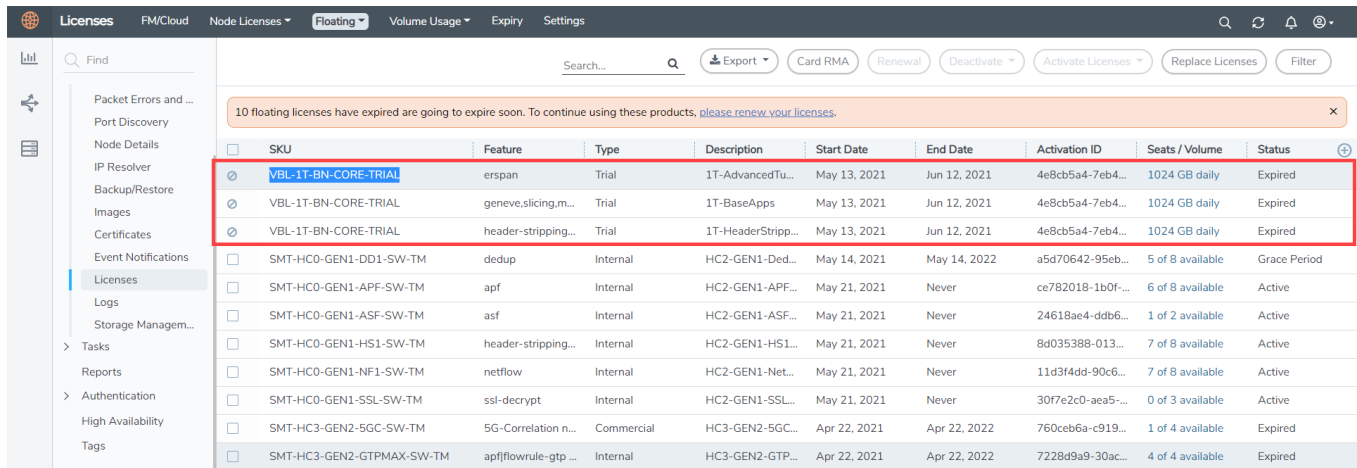
Activate Volume-based Licenses

To activate Volume-based licenses:

1. On the left navigation pane, click .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.
3. Click **Activate Licenses**. The **Activate License** page appears. Perform the following steps:
 - a. Download the fabric inventory file that contains information about GigaVUE-FM. Click **Next**. Refer to the [What is a Fabric Inventory File?](#) section for more details.
 - b. Navigate to the Licensing Portal. Upload the Fabric Inventory file in the portal. Once the fabric inventory file is uploaded, select the required license and click **Activate**. A license key is provided. Record the license key or keys.
 - c. Return to GigaVUE-FM and add the additional licenses.

Default Trial Licenses

After you install GigaVUE-FM, a default free 1TB of CoreVUE trial volume-based license (VBL) is provided one-time for 30 days (from the date of installation).



SKU	Feature	Type	Description	Start Date	End Date	Activation ID	Seats / Volume	Status
VBL-1T-BN-CORE-TRIAL	erspan	Trial	1T-AdvancedTu...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	geneve.slicing,m...	Trial	1T-BaseApps	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	header-stripping...	Trial	1T-HeaderStripp...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
SMT-HC0-GEN1-DD1-SW-TM	dedup	Internal	HC2-GEN1-Ded...	May 14, 2021	May 14, 2022	a5d70642-95eb...	5 of 8 available	Grace Period
SMT-HC0-GEN1-APF-SW-TM	apf	Internal	HC2-GEN1-APF...	May 21, 2021	Never	ce782018-1b0f...	6 of 8 available	Active
SMT-HC0-GEN1-ASF-SW-TM	asf	Internal	HC2-GEN1-ASF...	May 21, 2021	Never	24618ae4-ddb6...	1 of 2 available	Active
SMT-HC0-GEN1-HS1-SW-TM	header-stripping...	Internal	HC2-GEN1-HS1...	May 21, 2021	Never	8d035388-013...	7 of 8 available	Active
SMT-HC0-GEN1-NF1-SW-TM	netflow	Internal	HC2-GEN1-Net...	May 21, 2021	Never	11d3f4dd-90c6...	7 of 8 available	Active
SMT-HC0-GEN1-SSL-SW-TM	ssl-decrypt	Internal	HC2-GEN1-SSL...	May 21, 2021	Never	30f7e2c0-aea5...	0 of 3 available	Active
SMT-HC3-GEN2-5GC-SW-TM	5G-Correlation n...	Commercial	HC3-GEN2-5GC...	Apr 22, 2021	Apr 22, 2022	760ceb6a-c919...	1 of 4 available	Expired
SMT-HC3-GEN2-GTPMAX-SW-TM	apfflowrule-gtp...	Internal	HC3-GEN2-GTP...	Apr 22, 2021	Apr 22, 2022	7228d9a9-30ac...	4 of 4 available	Expired

This license includes the following applications:


- ERSPAN
- Geneve
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flowmap
- Header-stripping
- Add header

NOTE: There is no grace period for the trial license. If you do not have any other Volume-based licenses installed, then after 30 days, on expiry of the trial license, any deployed monitoring sessions will be undeployed from the existing GigaVUE V Series Nodes.

To deactivate the trial VBL refer to [Delete Default Trial Licenses](#) section for details.

Delete Default Trial Licenses

GigaVUE-FM allows you to deactivate the default trial licenses from this page. To deactivate the license:

1. On the left navigation pane, click .
2. Go to **System > Licenses > Floating**. Click **Activated**.
3. Click **Deactivate > Default Trial VBL**.

The VBL trial licenses is deactivated and is no longer listed in the Activated page. However, you can view these deactivated licenses from the Deactivated page.

Apply License

For instructions on how to generate and apply license refer to the *GigaVUE Licensing Guide*.

Network Firewall Requirement

The following table lists the Network Firewall Requirements for GigaVUE V Series Node deployment.

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
Inbound	<ul style="list-style-type: none"> • HTTPS • SSH 	TCP	<ul style="list-style-type: none"> • 443 • 22 	Administrator Subnet	Management connection to GigaVUE-FM
Inbound	Custom TCP Rule	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE V Series Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation UCT-V to send statistics to GigaVUE-FM
Outbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series node
UCT-V Controller					
Inbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with GigaVUE-FM
Inbound (This is the port	Custom TCP Rule	TCP(6)	8891	UCT-V or Subnet IP	Allows UCT-V Controller to communicate registration requests from UCT-V and

Direction	Type	Protocol	Port	CIDR	Purpose
used for Third Party Orchestration)					forward the same to GigaVUE-FM
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
Outbound	Custom TCP Rule	TCP(6)	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate with UCT-Vs
UCT-V					
Inbound	Custom TCP Rule	TCP(6)	9901	UCT-V Controller IP	Allows UCT-Vs to communicate with UCT-V Controller
Outbound (This is the port used for Third Party Orchestration)	Custom TCP Rule	TCP(6)	8891	UCT-V or Subnet IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat
Outbound	<ul style="list-style-type: none"> • UDP • IP 	<ul style="list-style-type: none"> • UDP (VXLAN) • IP Protocol (L2GRE) 	VXLAN (default 4789)	UCT-V or Subnet IP	Allows UCT-Vs to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Outbound	Custom TCP Rule	TCP	11443	UCT-V subnet	Allows UCT-V to securely transfer the traffic to GigaVUE V Series Node
GigaVUE V Series Proxy (optional)					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows V Series Proxy to communicate with V Series node
GigaVUE V Series Node					
Inbound	Custom TCP Rule	TCP	8889	<ul style="list-style-type: none"> • GigaVUE-FM IP • V Series Proxy IP 	Allows V Series Proxy or GigaVUE-FM to communicate with V Series node
Inbound	<ul style="list-style-type: none"> • UDP • IP 	<ul style="list-style-type: none"> • UDP (VXLAN) • IP Protocol (L2GRE) 	<ul style="list-style-type: none"> • VXLAN (default 4789) • L2GRE 	UCT-V or Subnet IP	Allows UCT-Vs to (VXLAN/L2GRE) tunnel traffic to V Series nodes

Direction	Type	Protocol	Port	CIDR	Purpose
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound	Custom UDP Rule	<ul style="list-style-type: none"> • UDP (VXLAN) • IP Protocol (L2GRE) 	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound (optional)	ICMP	ICMP	<ul style="list-style-type: none"> • echo request • echo reply 	Tool IP	Allows V Series node to health check tunnel destination traffic
Bi-directional	Custom TCP Rule	TCP	11443	GigaVUE V Series Node subnet	Allows to securely transfer the traffic in between GigaVUE V Series Nodes.

Configure Role-Based Access for Third Party Orchestration

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

Users

The Users page lets you manage the GigaVUE-FM and GigaVUE-OS FM users. You can also configure user's role and user groups to control the access privileges of the user in GigaVUE-FM.

Add Users

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


IMPORTANT: It is recommended to create users through GigaVUE-FM:

- You cannot view or manage users created in GigaVUE-FM CLI using GigaVUE-FM.
- You cannot view changes made to the users in GigaVUE-FM CLI in GigaVUE-FM.

NOTE: Monitor and operator users are not available in GigaVUE-FM. However, if you upgrade from a previous version in which monitor/operator users have been mapped in map default user, then after upgrade:

- **In AAA:** Users authenticated through the external servers will be assigned the fm_user role.
- **In LDAP:** Remote group based DN entry will not be migrated.

To add users perform the following steps:

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

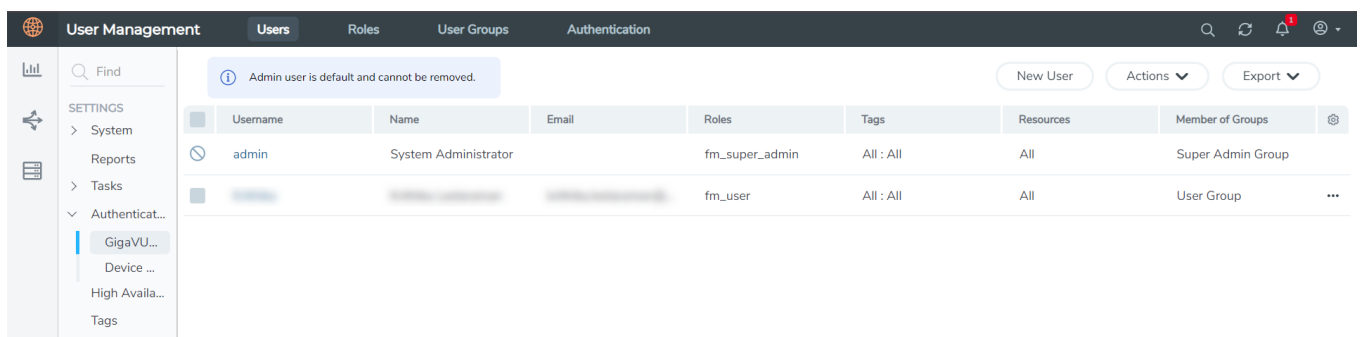


Figure 1 FM Users Page

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

Add User ✕

ⓘ All form elements are required unless indicated as optional. ✕

Name

Username

Password

Confirm password

Email

User Group
 ?

ⓘ Your new password must contain:

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

Cancel Ok

Figure 2 *Create User*

a. In the Add User pop-up box, 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. Refer to the [Change Your Password](#) section.
- **User Group:** User group

NOTE: GigaVUE-FM will prompt for your password.

b. Click **Ok** to save the configuration.

The new user is added to the summary list view.

You can also assign users to roles and user groups that set the access permissions. Refer to the following sections for details:

- [Create Roles](#)
- [Create Groups.](#)

NOTE: If you have logged in as a user with **fm_super_admin** role or a user with either read/write access on FM security Management category, then click on the ellipsis to:

- **Assign User Group:** Assign user group to users.
- **Edit:** Edit the user details.
- **Delete:** Delete a user.
- **Unlock:** Unlock a locked user.

How to Unlock User Account

To unlock a locked user, you must be a user with **fm_super_admin** role or a user with either read/write access on FM security Management category.

To unlock:

1. Select the required user whose account you want to lock.
2. Click on the ellipses and select **Unlock**. You can also click the **Actions** drop-down button and select **Unlock**.
3. A notification message prompts up. Click **Unlock** to unlock the user.

The user account is unlocked. An event is triggered in the Events page, and an email will be sent if Email Notification settings are configured.

The User name and password provided in this section will be used as the User and Password in the registration data.

After adding User, you must configure roles for third party orchestration.

Create Roles

You can associate a role with user. Under the **Select Permissions** tab select **Third Party Orchestration** and provide read/write permissions.

Create Roles

This section describes the steps for creating roles and assigning user(s) to those roles.

GigaVUE-FM has the following default roles:

- **fm_super_admin** — Allows a user to do everything in Fabric Manager, including adding or modifying users and configuring all AAA settings in the RADIUS, TACACS+, and LDAP tabs. Can change password for all users.
- **fm_admin** — Allows a user to do everything in Fabric Manager except add or modify users and change AAA settings. Can only change own password.

- **fm_user** — Allows a user to view everything in Fabric Manager, including AAA settings, but cannot make any changes.

NOTE: If you are a user with read-only access you will be restricted from performing any configurations on the screen. The menus and action buttons in the UI pages will be disabled appropriately.

Starting in software version 5.7, you can create custom user roles in addition to the default user roles in GigaVUE-FM. Access control for the default roles and the custom roles is based on the categories defined in GigaVUE-FM. These categories provide the ability to limit user access to a set of managed inventories such as ports, maps, cluster, forward list and so on.

Refer to the following table for the various categories and the associated resources. Hover your mouse over the resource categories in the Roles page to view the description of the resources in detail.


Category	Associated Resources
All	<p>Manages all resources</p> <ul style="list-style-type: none"> ● A user with fm_super_admin role has both read and write access to all the resource categories. ● A user with fm_user role has only read access to all the resource categories.
Infrastructure Management	<p>Manages resources such as devices, cards, ports and cloud resources. You can add or delete a device in GigaVUE-FM, enable or disable cards, modify port parameters, set leaf-spine topology. The following resources belong to this category:</p> <ul style="list-style-type: none"> ● Physical resources: Chassis, slots, cards ports, port groups, port pairs, cluster config, nodes and so on ● GigaVUE-FM inventory resources: Nodes, node credentials ● Device backup/restore: Device and cluster configuration ● Device license configuration: Device/cluster licensing ● Statistics: Device, port ● Tags: Events, historical trending ● Device security: SystemTime, System EventNotification, SystemLocalUser, System Security Policy Settings, AAA Authentication Settings, Device User Roles, LDAP Servers, RADIUS Servers, TACACS+ Servers ● Device maintenance: Sys Dump, Syslog ● Cloud Infrastructure resources: Cloud Connections, Cloud Proxy Server, Cloud Fabric Deployment, Cloud Configurations, Sys Dump, Syslog, Cloud licenses, Cloud Inventory. <p>NOTE: Cloud APIs are also RBAC enabled.</p>
Traffic Control Management	<p>Manages inline resources, flow maps, GigaSMART applications, second level maps, map chains, map groups. The following</p>

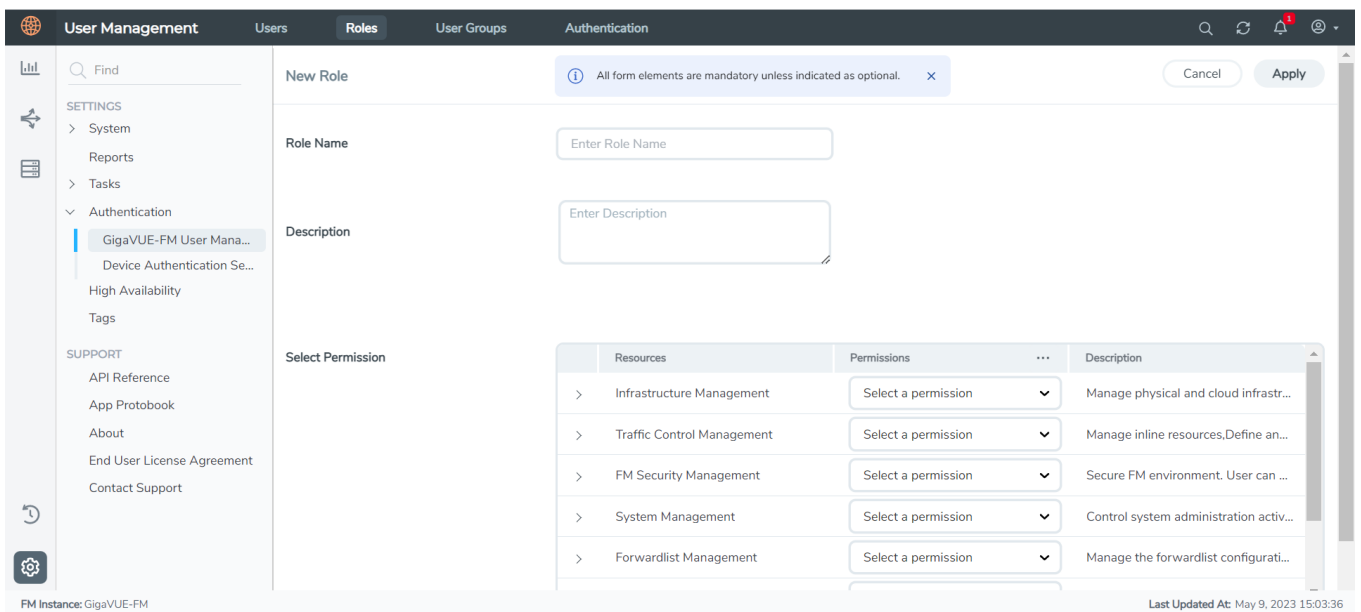
Category	Associated Resources
	<p>resources belong to this category:</p> <ul style="list-style-type: none"> ● Infrastructure resources: IP interfaces, circuit tunnels, tunnel endpoints, tunnel load balancing endpoints, ARP entries ● Intent Based Orchestration resources: Policies, rules ● GigaSMART resources: GigaSMART, GSgroups, vPorts, Netflow exporters ● Map resources: Fabric, fabric resources, flow maps, maps, map chains, map groups, map templates ● Application intelligence resources: Application visibility, Metadata, application filter resources ● Tag: Flow manipulation - Netflow operations, Statistics - device port ● Active visibility ● Inline resources: Inline networks, Inline network groups, Inline tools, Inline tool groups, Inline serial tools, Inline heartbeat profile ● Cloud operation resources: Monitoring session, stats, map library, tunnel library, tools library, inclusion/exclusion maps. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: Cloud APIs are also RBAC enabled.</p> </div>
FM Security Management	Ensures secure GigaVUE-FM environment. Users in this category can manage user and roles, AAA services and other security operations.
System Management	<p>Controls system administration activities of GigaVUE-FM. User in this category are allowed to perform operations such as backup/restore of GigaVUE-FM and devices, and upgrade of GigaVUE-FM. The following GigaVUE-FM resources belong to this category:</p> <ul style="list-style-type: none"> ● Backup/restore ● Archive server ● License ● Storage management ● Image repo config ● Notification target/email
Forward list/CUPS Management	<p>Manages the forward list configuration. The following resources belong to this category:</p> <ul style="list-style-type: none"> ● GTP forward list ● SIP forward list
Third Party Orchestration	Used to deploy fabric components using external orchestrator.
Device Certificate Management	Manages device certificates.
Other Resource Management	Manages virtual and cloud resources

You can associate the custom user roles either to a single category or to a combination of categories based on which the users will have access to the resources. For example, you can create a 'Physical Devices Technician' role such that the user associated with this role can only access the resources that are part of the **Physical Device Infrastructure Management**.

NOTE: A user with **fm_admin** role has both read and write access to all of the categories, but has read only access to the FM Security Management category.

To create a role

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



The screenshot shows the 'New Role' configuration page in the GigaVUE-FM User Management interface. The page has a dark header with 'User Management' and tabs for 'Users', 'Roles', 'User Groups', and 'Authentication'. A left sidebar contains navigation options like 'System', 'Reports', 'Tasks', 'Authentication', and 'SUPPORT'. The main content area is titled 'New Role' and includes a warning message: 'All form elements are mandatory unless indicated as optional.' There are 'Cancel' and 'Apply' buttons at the top right. The form contains three main sections: 'Role Name' with an input field 'Enter Role Name', 'Description' with a text area 'Enter Description', and 'Select Permission' which is a table.

Resources	Permissions	Description
> Infrastructure Management	Select a permission	Manage physical and cloud infrastr...
> Traffic Control Management	Select a permission	Manage inline resources.Define an...
> FM Security Management	Select a permission	Secure FM environment. User can ...
> System Management	Select a permission	Control system administration activ...
> Forwardlist Management	Select a permission	Manage the forwardlist configurati...

At the bottom left, it says 'FM Instance: GigaVUE-FM' and at the bottom right, 'Last Updated At: May 9, 2023 15:03:36'.

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:** In the **Select Permission** table, select the required permission for the various resource categories.
4. Click **Apply** to save the configuration.

Create User Groups

You can use the user group option to associate the users with Roles and Tags. A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more user groups.

Create User Groups

Starting in software version 5.8.00, you can use the user group option to associate the users with Roles and Tags. A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more user groups.

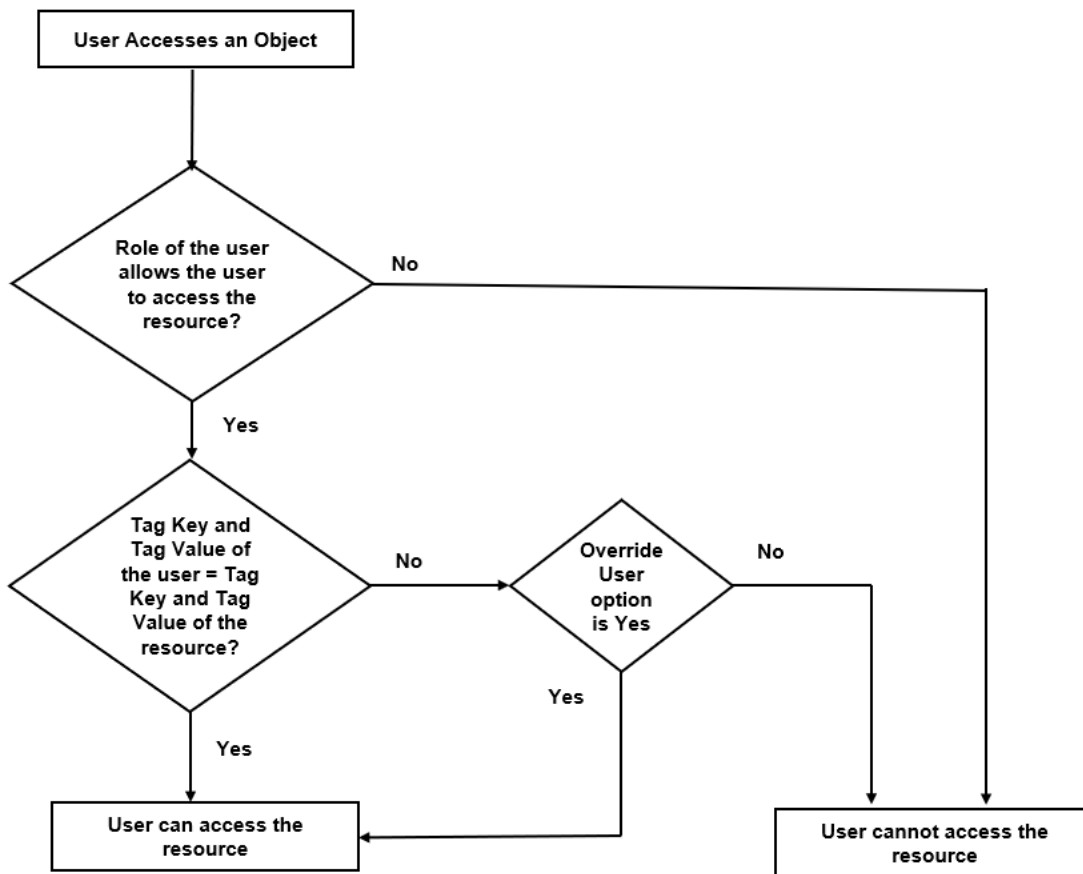
The following user groups are available by default in GigaVUE-FM. You will not be able to edit or change these groups in the system.

User Group	Tag Key and Tag Value	Permission
Super Admin Group	Tag Key = All Tag Value = All	Group with privileges of fm_super_adminrole.
Admin Group	Tag Key= All Tag Value = All	Group with privileges of fm_admin role.
View only user	Tag Key = All Tag Value = All	Group with privileges of fm_user role.


By creating groups and associating to tags and roles, you can control the users of the following:

- The category of resources which the user can access, such as the clusters, ports, maps and so on. This is defined using the **Roles** option. Refer to the Roles section for more details.
- The physical and logical resources that the user can access, such as the ports in a cluster that belong to a specific department in a location. This is defined using the **Tags** option.

Refer to the following flow chart to see how access control operation occurs when the user accesses a resource:



To create a user group:

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

The screenshot shows the 'New User Group' configuration wizard in the 'Assign Roles' step. The wizard progress bar indicates steps: 1. Group Info, 2. Assign Roles (current), 3. Assign Tags, and 4. Assign Users. Below the progress bar is a table of roles:

Roles	Description	Resources
<input type="checkbox"/> fm_super_admin	Allows a user to do everything in GigaVUE-FM, including add...	All
<input checked="" type="checkbox"/> fm_admin	Allows a user to do everything in GigaVUE-FM except adding...	Infrastructure Management+ 6 more
<input type="checkbox"/> fm_user	Allows a user to view everything in GigaVUE-FM, including A...	All

At the bottom of the table, there is a pagination control: 'Go to page: 1 of 1' and '3 roles total'.

3. In the **Group Info** tab, enter the following details:
 - **Group Name**
 - **Description**
4. In the **Assign Roles** tab, select the required role.
5. In the **Assign Tags** tab, select the required tag key and tag value.
6. In the **Assign Users** tab, select the required users. Click **Apply** to save the configuration. Click **Skip and Apply** to skip this step and proceed without adding users.

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

Click on the ellipses to perform the following operations:

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

Deployment Options for GigaVUE Cloud Suite for Third Party Orchestration

This section provides a detailed information on the multiple ways in which GigaVUE Cloud Suite for Third Party Orchestration can be configured to provide visibility for physical and virtual traffic. There are five different ways in which GigaVUE Cloud Suite for Third Party

Orchestration can be configured based on the traffic acquisition method and the method in which you want to deploy fabric components. For more detailed information and the work flow refer the following topics:

- [Deploy GigaVUE Fabric Components using Generic Mode](#)
 - [Without Creating Monitoring Domain](#)
 - [By Creating Monitoring Domain](#)
- [Deploy GigaVUE Fabric Components using Integrated Mode](#)

Deploy GigaVUE Fabric Components using Generic Mode

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

Without Creating Monitoring Domain

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

Traffic Acquisition Method as UCT-V

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

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Install UCT-V Agents	Prepare UCT-V to Monitor Traffic
3	Configure GigaVUE Fabric Components	Deploy Fabric Components using Generic Mode
4	Create Monitoring session	Configure Monitoring Session
5	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
6	Deploy Monitoring Session	Deploy Monitoring Session
7	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as Customer Orchestrated Source

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

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

By Creating Monitoring Domain

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

Traffic Acquisition Method as UCT-V

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

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Install UCT-V Agents	Prepare UCT-V to Monitor Traffic
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	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as Customer Orchestrated Source

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

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Create a Monitoring Domain	Create Monitoring Domain
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

Deploy GigaVUE Fabric Components using Integrated Mode

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

Step No	Task	Refer the following topics
1	Install GigaVUE-FM	Install GigaVUE-FM
2	Install UCT-V Agents	Prepare UCT-V to Monitor Traffic
3	Create a Monitoring Domain NOTE: Ensure that the Use FM to Launch Fabric toggle button is disabled.	Refer to the <i>Create Monitoring Domain</i> section in the respective cloud guide.
4	Configure GigaVUE Fabric Components	Deploy Fabric Components using

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

Deploy GigaVUE Cloud Suite for Third Party Orchestration

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

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

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

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

- [Install GigaVUE-FM](#)
- [Prepare UCT-V to Monitor Traffic](#)
- [Uninstall UCT-V](#)
- [Upgrade or Reinstall UCT-V](#)
- [Install Custom Certificate](#)

- [Adding Certificate Authority](#)
- [Modes of Deployments](#)
- [Create Monitoring Domain](#)
- [Deploy Fabric Components using Generic Mode](#)
- [Deploy Fabric Components using Integrated Mode](#)

Install GigaVUE-FM

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

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

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

Prepare UCT-V to Monitor Traffic

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

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

A UCT-V consists of a source interface and a destination interface. The network packets collected from the source interface are sent to the destination interface. From the destination interface, the packets traverse through the L2GRE/VXLAN tunnel interface to the GigaVUE V Series node.

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

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

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-V¹ is v6.4.00

Supported Operating Systems for G-vTAP Agents are v1.8-3, v1.8-4, v1.8-5, v1.8-7, v6.1.00, v6.2.00, v6.3.00

Operating System	Supported Versions
Ubuntu/Debian	Versions 18-04 and above are supported.
CentOS/RHEL/Fedora	Versions 7.5 and above.
Amazon Linux	Versions 1 and 2 (For version 2, package iproute-tc must be installed first)
Windows Server	Versions 2012 through 2022
Windows Client	Versions 10 and 11
RHEL	Versions 8.8 and above.

GigaVUE-FM version 6.4 supports UCT-V version 6.4 as well as (n-2) versions. It is always recommended to use the latest version of UCT-V with GigaVUE-FM, for better compatibility.

Linux UCT-V Installation

Refer to the following sections for the Linux agent installation:

- [Single ENI Configuration](#)
- [Dual ENI Configuration](#)
- [Install UCT-Vs](#)

Single ENI Configuration

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

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

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

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

Dual ENI Configuration

A UCT-V lets you configure two ENIs. One ENI can be configured as the source interface and another ENI can be configured as the destination interface.

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

Install UCT-Vs

You must have sudo/root access to edit the UCT-V configuration file.

For dual or multiple ENI configuration, you may need to modify the network configuration files to make sure that the extra NIC/ENI will initialize at boot time.

NOTE: Before installing UCT-V.**deb** or **.rpm** packages on your Linux VMs, you must install packages like Python3 and Python modules (netifaces, urllib3, and requests). Package iproute-tc is also required on RHEL and CentOS VMs.

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

Refer to the following topics for details:

- [Install UCT-V from Ubuntu/Debian Package](#)
- [Install UCT-V from RPM package](#)
- [Install UCT-V from Red Hat Enterprise Linux and CentOS with Selinux Enabled](#)

Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

1. Download the UCT-V **6.4.00** Debian (.deb) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue_uctv_6.4.00_amd64.deb
$ sudo dpkg -i gigamon-gigavue_uctv_6.4.00_amd64.deb
```

- Once the UCT-V package is installed, modify the file `/etc/uctv/uctv.conf` to configure and register the source and destination interfaces. The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

NOTE: 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. When you have an active, successful monitoring session deployed, modifying the UCT-V config file results in traffic loss until 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
```

- Save the file.
- To enable the third-party orchestration, a configuration file `/etc/gigamon-cloud.conf` needs to be created with the following contents:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of the UCT-V Controller 1>,
            <IP address of the UCT-V Controller 2>
  remotePort: 8891
```

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

- Reboot the instance.

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

```
$ sudo /etc/init.d/uctv status
UCT-V is running
```

Install UCT-V from RPM package

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

1. Run the following command:

```
sudo yum install iproute-tc -y
sudo yum install python3 -y
sudo yum install gcc -y
sudo yum install python3-pip -y
sudo pip3 install urllib3
sudo pip3 install requests
sudo yum install python-devel -y
sudo pip3 install netifaces
```
2. Download the UCT-V 6.4.00 RPM (.rpm) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
3. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue_uctv_6.4.00_x86_64.rpm
$ sudo rpm -i gigamon-gigavue_uctv_6.4.00_x86_64.rpm
```

- 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: Any changes to the UCT-V agent 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. When you have an active, successful monitoring session deployed, modifying the UCT-V config file results in traffic loss until 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
```

- Save the file.
- To enable the third-party orchestration, a configuration file `/etc/gigamon-cloud.conf` needs to be created with the following contents:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of the UCT-V Controller 1>,
            <IP address of the UCT-V Controller 2>
  remotePort: 8891
```

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

- Reboot the instance.

Check the status with the following command:

```
$ sudo service uctv status
```


UCT-V is running

Install UCT-V from Red Hat Enterprise Linux and CentOS with Selinux Enabled

1. Launch the RHEL/CentOS agent AML image.
2. Download the following packages from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
 - gigamon-gigavue_uctv_6.4.00_x86_64.rpm
3. Copy the downloaded UCT-V package files and strongSwan TAR file to UCT-V.
4. Install UCT-V package:

```
sudo rpm -ivh gigamon-gigavue_uctv_6.4.00_x86_64.rpm
```
5. Edit uctv.conf file to configure the required interface as source/destination for mirror:

NOTE: 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. When you have an active, successful monitoring session deployed, modifying the UCT-V config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst  
# sudo /etc/init.d/uctv restart
```

6. Reboot the instance.

Windows UCT-V Installation

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

VXLAN is the only supported tunnel type for Windows UCT-V.

Windows UCT-V Installation Using MSI Package

To install the Windows UCT-V using the MSI file:

1. Download the Windows UCT-V 6.4.00 MSI package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Install the downloaded MSI package as **Administrator** and the UCT-V service starts automatically.

- Once the UCT-V package is installed, modify the file **C:\ProgramData\Uct-v\uctv.conf** to configure and register the source and destination interfaces.

NOTE: 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. When you have an active, successful monitoring session deployed, modifying the UCT-V config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.



Following are the rules to modify the UCT-V configuration file:

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

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

```
192.168.1.0/24 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.

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

- Save the file.

5. To enable the third-party orchestration, a configuration file **C:\ProgramData\uctv\gigamon-cloud.conf** needs to be created with the following contents:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of UCT-V Controller 1, IP address of UCT-V
Controller 2>
  remotePort: 8891
```

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

6. To restart the Windows UCT-V, perform one of the following actions:
 - Restart the VM.
 - Run 'sc stop uctv' and 'sc start uctv' from the command prompt.
 - Restart the UCT-V from the Windows Task Manager.

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

Windows UCT-V Installation Using ZIP Package

To install the Windows UCT-V using the ZIP package:

1. Download the Windows UCT-V **6.4.00** ZIP package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Extract the contents of the .zip file into a convenient location.
3. Run 'install.bat' as an **Administrator** and the UCT-V service starts automatically.

- Once the UCT-V package is installed, modify the file **C:\ProgramData\Uct-v\uctv.conf** to configure and register the source and destination interfaces.

NOTE: 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. When you have an active, successful monitoring session deployed, modifying the UCT-V config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.



Following are the rules to modify the UCT-V configuration file:

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

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

```
192.168.1.0/24 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.

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

- Save the file.

6. To enable the third-party orchestration, a configuration file **C:\ProgramData\uctv\gigamon-cloud.conf** needs to be created with the following contents:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of UCT-V Controller 1, IP address of UCT-V
Controller 2>
  remotePort: 8891
```

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

7. To restart the Windows UCT-V, perform one of the following actions:
- Restart the VM.
 - Run 'sc stop uctv' and 'sc start uctv' from the command prompt.
 - Restart the UCT-V from the Windows Task Manager.

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

NOTE: You must edit the Windows Firewall settings to grant access to the uctv process. To do this, access the Windows Firewall settings and find “uctvd” in the list of apps and features. Select it to grant access. Be sure to select both Private and Public check boxes. If “uctvd” does not appear in the list, click **Add another app...** Browse your program files for the uctv application (uctvd.exe) and then click **Add**.

(**Disclaimer:** These are general guidelines for changing Windows Firewall settings. See Microsoft Windows help for official instructions on Windows functionality.)

Uninstall UCT-V

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

Uninstall Linux UCT-V

The following steps provide instructions on how to uninstall Linux UCT-V

Stop the UCT-V service using the following commands:

For Ubuntu/Debian Package:

```
sudo service uctv stop
```

For RPM package or Red Hat Enterprise Linux and CentOS with Selinux Enabled:

```
sudo systemctl stop uctv
```

Uninstall the UCT-V using the following:

For Ubuntu/Debian Package:

```
sudo dpkg -r uctv
```

For RPM package:

```
sudo rpm -e uctv
```

For Red Hat Enterprise Linux and CentOS with Selinux Enabled:

```
sudo rpm -e uctv
```

Uninstall Windows UCT-V

To uninstall Windows UCT-V:

1. On your windows, go to **Task Manager > Services**. Search for **uctv**.
2. Right click **uctv** and select **Stop**.
3. Go to **Control Panel** search for uctv and uninstall.

Upgrade or Reinstall UCT-V

To upgrade UCT-V, delete the existing UCT-V and installing the new version of UCT-V.

NOTE: Before deleting the UCT-V, take a back up copy of **/etc/uctv/uctv.conf** configuration file. Follow this step to avoid reconfiguring the source and destination interfaces.

Refer to [Uninstall UCT-V](#) for more detailed information on how to uninstall UCT-V.

Refer to the following topics for more detailed information on how to install new UCT-V:

- [Linux UCT-V Installation](#)
- [Windows UCT-V Installation](#)

Install Custom Certificate

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

You can upload the custom certificate in two ways:

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

Upload Custom Certificates using GigaVUE-FM

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

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

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

4. Click **Save**.

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

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

Upload Custom Certificate using Third Party Orchestration

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

For integrated mode:

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

For generic mode:

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

Adding Certificate Authority

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

CA List

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

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

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

Field	Action
Alias	Alias name of the CA.
File Upload	Choose the certificate from the desired location.

4. Click **Save**.

Modes of Deployments

There are two ways in which GigaVUE V Series Nodes can be deployed using the third party orchestration. They are:

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

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

Create Monitoring Domain

To create a monitoring domain in Third Party Orchestration:

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

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

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain. A monitoring domain consists of set of connections.
Connection Alias	An alias used to identify the connection.
Traffic Acquisition Method	Select a tapping method. The available options are: <ul style="list-style-type: none"> ● 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 the V Series Node deployed under this monitoring domain. Enable this check box when using packet mirroring configuration for GCP. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: Once the monitoring session is deployed for the monitoring domain you cannot enable or disable this option.</p> </div>
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: AWS - 8950 Azure - 1450 OpenStack - 1450 Nutanix - 1250 The MTU must be 50 bytes less than the native MTU of the respective platform.

4. Click **Save**.

Deploy Fabric Components using Generic Mode

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

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

- [Configure GigaVUE Fabric Components using AWS](#)
- [Configure GigaVUE Fabric Components using Azure](#)
- [Configure GigaVUE Fabric Components using GCP](#)
- [Configure GigaVUE Fabric Components using Nutanix](#)
- [Configure GigaVUE Fabric Components using OpenStack](#)
- [Configure GigaVUE V Series Nodes using VMware ESXi](#)
- [Configure GigaVUE Fabric Components using Third Party Orchestration on NSX-T Federation Environment](#)

Configure GigaVUE Fabric Components using AWS

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

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

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 8590. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- When deploying the fabric components using generic mode, the connection name must be used as the subGroupName in the registration data.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to [Create Monitoring Domain](#) for more detailed information on how to create monitoring domain under third party orchestration.

- Only **UCT-V** or **Customer Orchestrated Source** can be used as the traffic acquisition method when using generic mode.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- You can also upload custom certificates to GigaVUE V Series Nodes, , GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform when deploying the fabric components. Refer to [Install Custom Certificate](#) for more detailed information.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in AWS. Refer to [Launch an instance using the Launch Instance Wizard](#) topic in Amazon EC2 Documentation for more detailed information on how to add network interfaces when launching an instance.

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

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

Configure UCT-V Controller in AWS

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

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

- [Register UCT-V Controller during Instance Launch](#)
- [Register UCT-V Controller after Instance Launch](#)

Register UCT-V Controller during Instance Launch

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

1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to [Launch an instance using the Launch Instance Wizard](#) topic in Amazon EC2 Documentation.

2. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The UCT-V Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM. You can also install custom certificates to UCT-V Controller, refer to the below table for details:

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



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

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

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

Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
MD1					
	pubtrng-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, follow the steps given below:

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

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

- Restart the UCT-V Controller service.

```
$ sudo service uctv-ctrl 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 node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller and if that fails as well then GigaVUE-FM unregisters the UCT-V Controller and it will be removed from GigaVUE-FM.

Configure UCT-V in 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.

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

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

- [Register UCT-V during Instance Launch](#)
- [Register UCT-V after Instance Launch](#)

Register UCT-V during Instance Launch

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

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

1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to [Launch an instance using the Launch Instance Wizard](#) topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The UCT-V uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      user: <Username>
      password: <Password>
      remoteIP: <IP address of the UCT-V Controller 1>, <IP address of the UCT-V
Controller 2>
      remotePort: 8891
```

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

Register UCT-V after Instance Launch

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

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

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



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

Registration:

```

groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <IP address of the UCT-V Controller 1>, <IP address of the UCT-V Controller 2>
remotePort: 8891

```



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

4. Restart the UCT-V service.
 - Linux platform:


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

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

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if 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 AWS EC2, use any one of the following methods.

- [Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch](#)
- [Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch](#)

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

1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to [Launch an instance using the Launch Instance Wizard](#) topic in Amazon EC2 Documentation.

- On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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



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

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>
user: <Username>
password: <Password>
remoteIP: <IP address of the GigaVUE-FM> or <IP address of the proxy>
remotePort: 443
```



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

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 node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series proxy and if that fails as well then GigaVUE-FM unregisters the GigaVUE V Series proxy and it will be removed from GigaVUE-FM.

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

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

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure there is no existing user in GigaVUE-FM, with the username **orchestration**.

It is recommended to change the password in the Users page, once the upgrade is complete. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for detailed steps on how to change password in the user page.

Configure GigaVUE Fabric Components using Azure

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

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

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1450. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.

- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to [Create Monitoring Domain](#) for more detailed information on how to create monitoring domain under third party orchestration.
- You can also upload custom certificates to GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform when deploying the fabric components. Refer to [Install Custom Certificate](#) for more detailed information.

Prerequisites

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

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

- [Create GigaVUE V Series Node with Management and Data NIC Attached using CLI](#)
- [Create GigaVUE V Series Node with Management and Data NIC Attached using Azure GUI](#)

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

Create management NIC:

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

Create data NIC with Accelerated Networking enabled:

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

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

```
az vm create --resource-group <Resource group> --size <Standard_D4s_v4/Standard_D8S_V4> --name <GigaVUE V Series Node> --admin-username gigamon --generate-ssh-keys --image gigamon-inc:gigamon-gigavue-cloud-suite:vseries-node:6.4 --plan-name vseries-node --plan-product gigamon-gigavue-cloud-suite --plan-publisher gigamon-inc --nics <Management NIC and Data NIC>
```

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

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

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

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

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

Configure UCT-V Controller in Azure

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

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

- [Register UCT-V Controller during Virtual Machine Launch](#)
- [Register UCT-V Controller after Virtual Machine Launch](#)

Register UCT-V Controller during Virtual Machine Launch

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

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

- 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.

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



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

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

Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
MD1					
	pubtraj/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 Virtual Machine Launch

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

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

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



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

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 node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller and if that fails as well then GigaVUE-FM unregisters the UCT-V Controller and it will be removed from GigaVUE-FM.

Configure UCT-V in Azure

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

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

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

- [Register UCT-V during Virtual Machine Launch](#)
- [Register UCT-V after Virtual Machine Launch](#)

Register UCT-V during Virtual Machine Launch

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

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

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

2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The UCT-V uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      user: <Username>
      password: <Password>
      remoteIP: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
      remotePort: 8891
```



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

Register UCT-V after Virtual Machine Launch

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

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

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

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



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

Registration:

```

groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V Controller 2>
remotePort: 8891

```

4. Restart the UCT-V service.
 - Linux platform:


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

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

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

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

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

- [Register GigaVUE V Series Node and GigaVUE V Series Proxy during Virtual Machine Launch](#)
- [Register GigaVUE V Series Proxy after Virtual Machine Launch](#)

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

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

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

- 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.

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



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

Register GigaVUE V Series Proxy after Virtual Machine Launch

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

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

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



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

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 node 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 Azure, it does not send any unregistration request and GigaVUE-FM will unregister the V Series Node soon after.

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

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure there is no existing user in GigaVUE-FM, with the username **orchestration**.

It is recommended to change the password in the Users page, once the upgrade is complete. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for detailed steps on how to change password in the user page.

Refer to the following Gigamon Validated Designs for more detailed information.

- [Deploying GigaVUE Cloud Suite for Azure using Third Party Orchestration](#)
- [Deploying GigaVUE Cloud Suite for Azure using Customer 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	<ul style="list-style-type: none"> • c2-standard-4 for 2 interfaces • c2-standard-8 for 3 interfaces
GigaVUE V Series Proxy	e2-micro
UCT-V Controller	e2-micro

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

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1450. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** value and click Save.
- For successful registration of fabric components, firewall rules must be configured to open ports 443 and 8891. Refer to [Use VPC firewall rules](#) topic in GCP documentation for more detailed information on how to configure firewall rules.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to [Create Monitoring Domain](#) for more detailed information on how to create monitoring domain under third party orchestration.
- User and Password provided in the registration data must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.
- When launching an instance, if you wish to access the instance using a private key, you will have add the key to the ssh key. The default password is gigamon.
- You can also upload custom certificates to GigaVUE V Series Nodes, , GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform when deploying the fabric components. Refer to [Install Custom Certificate](#) for more detailed information.

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

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

Configure UCT-V Controller in GCP

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

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

- [Register UCT-V Controller during Instance Launch](#)
- [Register UCT-V Controller after Instance Launch](#)

Register UCT-V Controller during Instance Launch

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

1. On the VM instances page of Google Cloud Platform, click **Create instances** . For detailed information, refer to [Create and Start instance](#) topic in GCP Documentation.

- 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.

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



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

Register UCT-V Controller after Instance Launch

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

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

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

3. Restart the UCT-V Controller service.


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

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

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 node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller and if that fails as well then GigaVUE-FM unregisters the UCT-V Controller and it will be removed from GigaVUE-FM.

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					
	pubtraj/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

Configure UCT-V in GCP

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

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

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

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

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

- [Register UCT-V during Instance Launch](#)
- [Register UCT-V after Instance Launch](#)

Register UCT-V during Instance Launch

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

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

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

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

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      user: <Username>
      password: <Password>
      remoteIP: <IP address of the UCT-V Controller 1>, <IP address of the UCT-V
Controller 2>
      remotePort: 8891
```



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

Register UCT-V after Instance Launch

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

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

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



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

Registration:

```

groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <IP address of the UCT-V Controller 1>, <IP address of the UCT-V Controller 2>
remotePort: 8891

```

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

4. Restart the UCT-V service.
 - Linux platform:


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

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

Configure GigaVUE V Series Nodes and V Series Proxy in GCP

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

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

- [Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch](#)
- [Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch](#)

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

1. On the VM instances page of Google Cloud Platform, click **Create instances** . For detailed information, refer to [Create and Start instance](#) topic in GCP Documentation.

- 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.

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



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

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

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

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

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



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

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 node 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 GCP, it does not send any unregistration request and GigaVUE-FM will unregister the V Series Node soon after.

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

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure there is no existing user in GigaVUE-FM, with the username **orchestration**.

It is recommended to change the password in the Users page, once the upgrade is complete. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for detailed steps on how to change password in the user page.

Refer to [Pervasive Visibility in GCP and GKE using Gigamon Cloud Suite \(6.1\)](#) for more detailed on how to acquire traffic from GCP GKE cluster.

Configure Packet Mirroring for GCP

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

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

Refer to the following topics for detailed information.

- [Configure Packet Mirroring in GCP](#)
- [Deploy GigaVUE V Series Solution with Packet Mirroring](#)

Prerequisites:

- When using packet mirroring, a minimum of 3 NICs must be configured and the Machine Type must be c2-standard-8 (8 vCPU, 32 GB memory).
- Create an instance template in GCP, refer to [Create instance templates](#) topic in Google Cloud Platform for more details.
- Create Instance Group in GCP with autoscaling in Managed Instance Group. Refer [Create a MIG with autoscaling enabled](#) topic in Google Cloud Documentation for more details.
- 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.
- Load Balancer forwards raw traffic. Therefore when configuring the monitoring session the Raw End Point must be used as the first component which receives traffic.
- Three NICs must be configured 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 (Fabric Manager)
- 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

To configure packet mirroring in GCP, refer to [Use Packet Mirroring](#) topic in Google Cloud Documentation for step-by-step instructions. After configuring the packet mirroring in GCP you must deploy the GigaVUE V Series solution in GigaVUE-FM.

Deploy GigaVUE V Series Solution with Packet Mirroring

To deploy GigaVUE V Series solution with packet mirroring in GigaVUE-FM:

Edit the monitoring domain and update the following details:

1. In the **Monitoring Domain Configuration** page, select **Customer Orchestrated Source** as the Traffic Acquisition method.
2. Enable the **Uniform Traffic Policy** check box. When enabling this option, same monitoring session configuration will be applied to all V Series Nodes.
3. Click **Save** to save the configuration.

Create a monitoring session with the following instructions:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select **Third Party Orchestration**. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page. Refer to [Create a Monitoring Session](#) for more detailed information on how to create a monitoring session.

3. In the **Edit Monitoring Session** page. Add Raw End point as the first component and Tunnel End Point as the final component.
4. Then add your application to the monitoring session. Connect your components.
5. To deploy the monitoring session after adding the Raw End Point click the **Deploy** button in the edit monitoring session page.
6. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the interface for REP and TEP from the drop-down menu.

Configure GigaVUE Fabric Components using Nutanix

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

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

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1300. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- User and Password provided in the registration data must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to [Create Monitoring Domain](#) for more detailed information on how to create monitoring domain under third party orchestration.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- You can also upload custom certificates to GigaVUE V Series Nodes, , GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform when deploying the fabric components. Refer to [Install Custom Certificate](#) for more detailed information.

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

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

Configure UCT-V Controller in Nutanix

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

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

- [Register UCT-V Controller during Instance Launch](#)
- [Register UCT-V Controller after Instance Launch](#)

Register UCT-V Controller during Instance Launch

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

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

- 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.

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

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					
	pubtrajvpc				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>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of the GigaVUE-FM>
  remotePort: 443
```

3. Restart the UCT-V Controller service.

```
$ sudo service uctv-ctrl 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 node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller and if that fails as well then GigaVUE-FM unregisters the UCT-V Controller and it will be removed from GigaVUE-FM.

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

Configure UCT-V in Nutanix

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

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

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

- [Register UCT-V during Instance Launch](#)
- [Register UCT-V after Instance Launch](#)

Register UCT-V during Instance Launch

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

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

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

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      user: <Username>
      password: <Password>
      remoteIP: <IP address of the UCT-V Controller 1>, <IP address of the UCT-V
Controller 2>
      remotePort: 8891
```

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.

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of the UCT -V Controller 1>,<IP address of the UCT -V Controller
2>
  remotePort: 8891
```

4. Restart the UCT-V service.
 - Linux platform:


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

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

Configure GigaVUE V Series Nodes and V Series Proxy in Nutanix

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

NOTE: Before deploying 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 information on Nutanix APIs, refer to Nutanix support site.

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

- [Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch](#)
- [Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch](#)

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

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

- 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.

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



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

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

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

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

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



- 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>.

- 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 node 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.

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

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure there is no existing user in GigaVUE-FM, with the username **orchestration**.

It is recommended to change the password in the Users page, once the upgrade is complete. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for detailed steps on how to change password in the user page.

Limitations

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

Configure GigaVUE Fabric Components using OpenStack

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

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

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1450. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to [Create Monitoring Domain](#) for more detailed information on how to create monitoring domain under third party orchestration.
- User and Password provided in the registration data must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in OpenStack.

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

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

Configure UCT-V Controller in OpenStack

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

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

- [Register UCT-V Controller during Instance Launch](#)
- [Register UCT-V Controller after Instance Launch](#)

Register UCT-V Controller during Instance Launch

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

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

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

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

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

Register UCT-V Controller after Instance Launch

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

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

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

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

3. Restart the UCT-V Controller service.


```
$ sudo service uctv-cntl 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 node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller and if that fails as well then GigaVUE-FM unregisters the UCT-V Controller and it will be removed from GigaVUE-FM.

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

Configure UCT-V in OpenStack

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

To register UCT-V using a configuration file:

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

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



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

Registration:

```

groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <IP address of the UCT-V Controller 1>, <IP address of the UCT-V Controller 2>
remotePort: 8891

```



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

4. Restart the UCT-V service.

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

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

Configure GigaVUE V Series Nodes and V Series Proxy in OpenStack

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

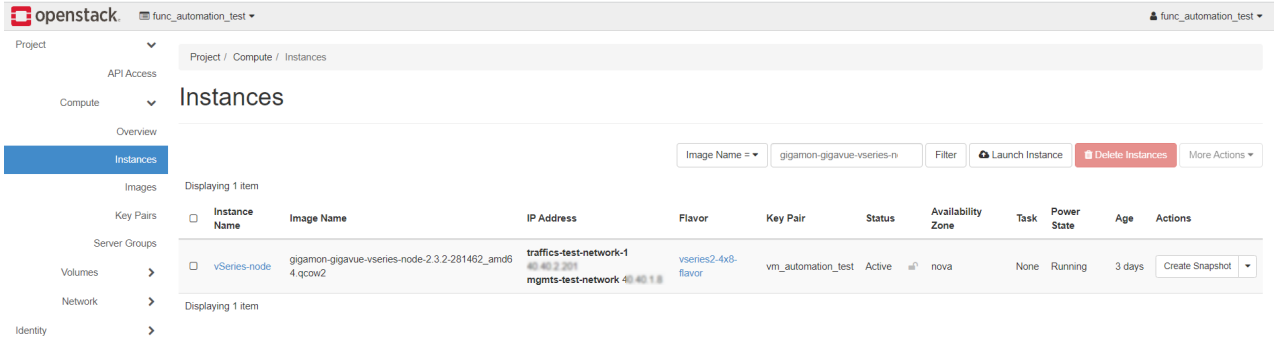
To register GigaVUE V Series Node and GigaVUE V Series Proxy in OpenStack, use any one of the following methods:

- [Register V Series Nodes or V Series Proxy during Instance Launch](#)
- [Register V Series Node or V Series Proxy after Instance Launch](#)

Register V Series Nodes or V Series Proxy during Instance Launch

To register V Series nodes or proxy using the Customization Script in OpenStack GUI:

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



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

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



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

Register V Series Node or V Series Proxy after Instance Launch

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

1. Log in to the 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>
  user: <Username>
  password: <Password>
  remoteIP: <IP address of the GigaVUE-FM> or <IP address of the Proxy>
  remotePort: 443
```



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

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

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

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

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

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure there is no existing user in GigaVUE-FM, with the username **orchestration**.

It is recommended to change the password in the Users page, once the upgrade is complete. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for detailed steps on how to change password in the user page.

Configure GigaVUE V Series Nodes using VMware ESXi

This section describes how to deploy GigaVUE V Series Nodes under Third Party Orchestration Monitoring Domain using VMware ESXi Host.

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

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

4. The **Select OVF and VMDK files** page appears. Provide a name for the Virtual machine. Upload either OVF and VMDK files or OVA files. Click Next.
5. Then, the **Select Storage** page appears, select the storage type and data store. Click Next.
6. Under the **Deployment Options**, provide the necessary details given below.
 - a. Select the network port group associated with the host, network ports and tunneling port details from the **Network Mappings** drop-down.
 - b. Select Thick/Thin from the **Disk provisioning** field.
 - c. Select **Management Port DHCP** from the **Deployment type** drop-down.
 - d. (optional) Enable the **Power on automatically** check-box to power on the Virtual Machine automatically.
7. Under the additional settings page, provide the user data as shown in the figure.

Enter the following values in the additional settings:

- Hostname: <Host Name>
- Administration Password: <Your Password>
- GroupName: <Monitoring domain name>
- SubGroupName: < Connection name>
- User: <Username>
- Password: <Password>
- remoteIP: <IP address of the GigaVUE-FM>
- remotePort: 443

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

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

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

Monitoring Domain	Connections	Name	Management IP	Type	Version	Status
MD1	Connection1					Connected
		10.115.182.94	10.115.182.94	V Series Node	2.6.0	Ok
MD2	Connection2					Connected
		10.115.182.23	10.115.182.23	V Series Node	2.6.0	Ok

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

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure there is no existing user in GigaVUE-FM, with the username **orchestration**.

It is recommended to change the password in the Users page, once the upgrade is complete. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for detailed steps on how to change password in the user page.

Configure GigaVUE Fabric Components using VMware vCenter

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

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

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

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

Register UCT-V Controller

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

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

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

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

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

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 node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller and if that fails as well then GigaVUE-FM unregisters the UCT-V Controller and it will be removed from GigaVUE-FM.

Register UCT-V

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

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

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



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

Registration:

```

groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <IP address of the UCT-V Controller 1>, <IP address of the UCT-V Controller 2>
remotePort: 8891

```



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

4. Restart the UCT-V service.

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

- Linux platform:


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

Register GigaVUE V Series Node

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

1. To register GigaVUE V Series Node after launching a Virtual Machine using a configuration file, follow the steps given below:
2. Log in to the GigaVUE V Series Node.

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

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

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

4. 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**
5. Review the setting selection in the **Ready to Complete page**, then click Finish.

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

Monitoring Domain	Connections	Name	Management IP	Type	Version	Status	
MD1	Connection1		10.115.182.94	10.115.182.94	V Series Node	2.6.0	Connected Ok
	Connection2		10.115.182.23	10.115.182.23	V Series Node	2.6.0	Connected Ok

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

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure there is no existing user in GigaVUE-FM, with the username **orchestration**.

It is recommended to change the password in the Users page, once the upgrade is complete. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for detailed steps on how to change password in the user page.

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

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

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

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

Prerequisites:

- Create service segments in VMware NSX-T Manager and attach it to UCT-V and GigaVUE V Series Nodes. Refer to Create a Service Segment topic in GigaVUE Cloud Suite Deployment Guide - VMware for more detailed information on how to create service segments in VMware NSX-T.
- User and Password provided in the registration data must be configured in the **User Management** page. Refer to [Configure Role-Based Access for Third Party Orchestration](#) for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

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

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

Register UCT-V Controller

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

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

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

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

3. When using multiple interfaces or Static IP address, update the **50-cloud-init.yaml** file in the **/etc/netplan/** directory and save the file. Use the following command to apply the changes.
 - **\$ sudo netplan apply**
4. 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 node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller and if that fails as well then GigaVUE-FM unregisters the UCT-V Controller and it will be removed from GigaVUE-FM.

Register UCT-V

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

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

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

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



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

Registration:

```

groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: <Username>
password: <Password>
remoteIP: <IP address of the UCT-V Controller 1>, <IP address of the UCT-V Controller 2>
remotePort: 8891

```



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

4. Restart the UCT-V service.

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

- Linux platform:


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

Register GigaVUE V Series Node

Refer to [Configure GigaVUE V Series Nodes using VMware ESXi](#) topic for step-by-step instructions on how to deploy GigaVUE V Series Node on VMware ESXi host.

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

Deploy Fabric Components using Integrated Mode

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

You can also create a monitoring domain and connection under Third party Orchestration and use the monitoring domain name and connection name as the groupName and subGroupName 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](#)
- [Configure GigaVUE Fabric Components in Azure](#)
- [Configure GigaVUE Fabric Components in OpenStack](#)

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](#)
- [Interface Mapping](#)
- [Create Ingress and Egress Tunnel](#)
- [Create Raw Endpoint](#)
- [Create Map](#)
- [Add Applications to Monitoring Session](#)
- [Deploy Monitoring Session](#)

- [View Monitoring Session Statistics](#)
- [Visualize the Network Topology](#)

Create a Monitoring Session

GigaVUE-FM automatically collects inventory data on all target instances available in your cloud environment. You can design your monitoring session to include or exclude the instances that you want to monitor. You can also choose to monitor egress, ingress, or all traffic. You can filter the traffic and, use a suite of GigaSMART applications as well.

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

You can create multiple monitoring sessions per monitoring domain.

To create a new monitoring session:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page.

Create A New Monitoring Session

Alias	M51
Monitoring Domain	MD
Connection	<input checked="" type="radio"/> Select All <input type="radio"/> Select None
	<input type="text" value="Instance-2 x"/>

3. Enter the appropriate information for the monitoring session as described in the following table.

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

4. Click **Create**. The **Edit Monitoring Session** Canvas page appears.

The Monitoring Session page **Actions** button also has the following options:

Button	Description
Edit	Opens the Edit page for the selected monitoring session. NOTE: In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.
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	You can use this button to apply the threshold template created for monitoring cloud traffic health. Refer to Monitor Cloud Health for more detailed information on cloud traffic health, how to create threshold templates, and how to apply threshold templates.
Apply Policy	You can use this button to enable precryption, prefiltering, or Secure Tunnel. Refer to Enable Prefiltering, Precryption, and Secure Tunnel for more details.

Edit Monitoring Session

In the edit monitoring session canvas page, you can add and configure applications, tunnel endpoints, raw endpoints, and maps.

Refer to the following topics for detailed information:

- [Create Ingress and Egress Tunnels](#)
- [Add Applications to Monitoring Session](#)

- [Create Raw Endpoint](#)
- [Create a New Map](#)

The **Edit Monitoring Session** page has the following buttons:

Button	Description
Options	You can enable or disable Prefiltering, Precryption, and Secure Tunnel here. You can also create prefiltering template and apply it to the monitoring session. Refer to Enable Prefiltering, Precryption, and Secure Tunnel for more detailed information.
Show Targets	Use to refresh the subnets and monitored instances details that appear in the Instances dialog box.
Interface mapping	Use to change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping topic for more details.
Deploy	Deploys the selected monitoring session. Refer to Deploy Monitoring Session topic for more details.

Enable Prefiltering, Precryption, and Secure Tunnel

Prefiltering, Precryption, and Secure tunnel can be enabled for the monitoring session from the Edit Monitoring Session canvas page.

Enable Prefiltering

To enable Prefiltering, follow the steps given below:

1. In the Edit Monitoring Session page, click **Options**. The **Monitoring Session Options** page appears.
2. Enable the **Mirroring** toggle button. Then, enable the **Prefiltering** toggle button.
3. You can select an existing Prefiltering template from the **Template** drop-down menu, or you can create a new template and apply it. Refer to [Prefiltering](#) for more details on how to create a new template.
4. Click Save to apply the template to the monitoring session.

You can save the newly created template by using the **Save as Template** button.

Enable Precryption

To enable Precryption, follow the steps given below:

1. In the Edit Monitoring Session page, click **Options**. The **Monitoring Session Options** page appears.
2. Enable the **Preryption** toggle button. Refer to topic for more details on preryption.

Enable Secure Tunnel

To enable Secure Tunnel, 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 prerypted traffic. For more information about Secure Tunnel, refer to

Prefiltering

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

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

Each monitoring session can have a maximum of 16 rules.

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

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

- Prefiltering is supported only in Next Generation UCT-Vs. It is not supported for classic mirroring mechanism.
- Prefiltering is supported for both Linux and Windows UCT-Vs.
- For a single monitoring session, only one prefiltering policy can be applied. All the agents in that monitoring session are configured with respective prefiltering policy.
- For multiple monitoring sessions, if the same agent is selected by two or more monitoring sessions, then prefiltering policy cannot be applied. It is default to PassAll.

Create Prefiltering Policy Template

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

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

1. Go to **Resources > Prefiltering**, and then click **UCT-V**.
2. Click **New**.
3. Enter the name of the template in the **Template Name** field.
4. Enter the name of a rule in the **Rule Name** field.
5. Click any one of the following options:
 - Pass — Passes the traffic.
 - Drop — Drops the traffic.
6. Click any one of the following options as per the requirement:
 - Bi-Directional — Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
 - Ingress — Filters the traffic that flows in.
 - Egress — Filters the traffic that flows out.
7. Select the value of the priority based on which the rules must be prioritized for filtering. Select the value as 1 to pass or drop a rule in top priority. Similarly, you can select the value as 2, 3, 4 to 8, where 8 can be used for setting a rule with the least priority. Drop rules are added based on the priority and, then pass rules are added.
8. Select the **Filter Type** from the following options:
 - L3
 - L4
9. Select the **Filter Name** from the following options:
 - ip4Src
 - ip4Dst
 - ip6Src
 - ip6Dst
 - Proto - It is common for both ipv4 and ipv6.
10. Select the **Filter Relation** from any one of the following options:
 - Not Equal to
 - Equal to
11. Enter the value for the given filter.
12. Click **Save**.

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

Interface Mapping

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

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select a Monitoring session from the list view and click **Actions > Edit**. The Edit Monitoring session page appears.
3. In the Edit Monitoring session canvas page, click on the **Interface Mapping** button.
4. The **Select nodes to deploy the Monitoring Session dialog box** appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.
5. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual GigaVUE V Series Nodes. Then, click **Deploy**.

Create Ingress and Egress Tunnel

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

To create a new tunnel endpoint:

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.

X **Add Tunnel Spec** Save Add To Library

Alias	Alias *
Description	Description (optional)
Type	<div style="border: 1px solid #ccc; padding: 2px;"><div style="background-color: #f0f0f0; padding: 2px;">Select a type... ▾</div><div style="padding: 2px;">Select a type...</div><div style="background-color: #007bff; color: white; padding: 2px;">L2GRE</div><div style="padding: 2px;">VXLAN</div></div>

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

Field	Description	
Alias	The name of the tunnel endpoint. NOTE: Do not enter spaces in the alias name.	
Description	The description of the tunnel endpoint.	
Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN, or UDPGRE to create a tunnel.	
VXLAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose In (Decapsulation) for creating an Ingress tunnel, 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, Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose Out (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled

Field	Description	
		with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as 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. Accepted value is between 0 and 1048575
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
UDPGRE		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose In (Decapsulation) for creating an Ingress tunnel, 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, 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 value between 0 and 4294967295
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the	

Field	Description												
	GigaVUE V Series Node.												
	<table border="1"> <tr> <td>IP Version</td> <td>The version of the Internet Protocol. Select IPv4 or IPv6.</td> </tr> <tr> <td>Remote Tunnel IP</td> <td>For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.</td> </tr> <tr> <td>Key</td> <td>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 value between 0 and 4294967295.</td> </tr> </table>	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.	Remote Tunnel IP	For Ingress tunnel, 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 value between 0 and 4294967295.						
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.												
Remote Tunnel IP	For Ingress tunnel, 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 value between 0 and 4294967295.												
Out	Choose Out (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.												
	<table border="1"> <tr> <td>Remote Tunnel IP</td> <td>For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.</td> </tr> <tr> <td>MTU</td> <td>The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.</td> </tr> <tr> <td>Time to Live</td> <td>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.</td> </tr> <tr> <td>DSCP</td> <td>Differentiated Services Code Point (DSCP) are the values, which 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 as the lowest priority.</td> </tr> <tr> <td>Flow Label</td> <td>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. Accepted value is between 0 and 1048575.</td> </tr> <tr> <td>Key</td> <td>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 value between 0 and 4294967295.</td> </tr> </table>	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.	DSCP	Differentiated Services Code Point (DSCP) are the values, which 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 as 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. 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 value between 0 and 4294967295.
Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.												
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.												
Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.												
DSCP	Differentiated Services Code Point (DSCP) are the values, which 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 as 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. 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 value between 0 and 4294967295.												
ERSPAN													
Traffic Direction													
The direction of the traffic flowing through the GigaVUE V Series Node.													

Field	Description	
In	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, 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.		
In	IP Version	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, 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	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

Field	Description	
Out	IP Version	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, 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) are the values, which 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 as 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. Accepted value is between 0 and 1048575
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

4. Click **Save**.

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

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

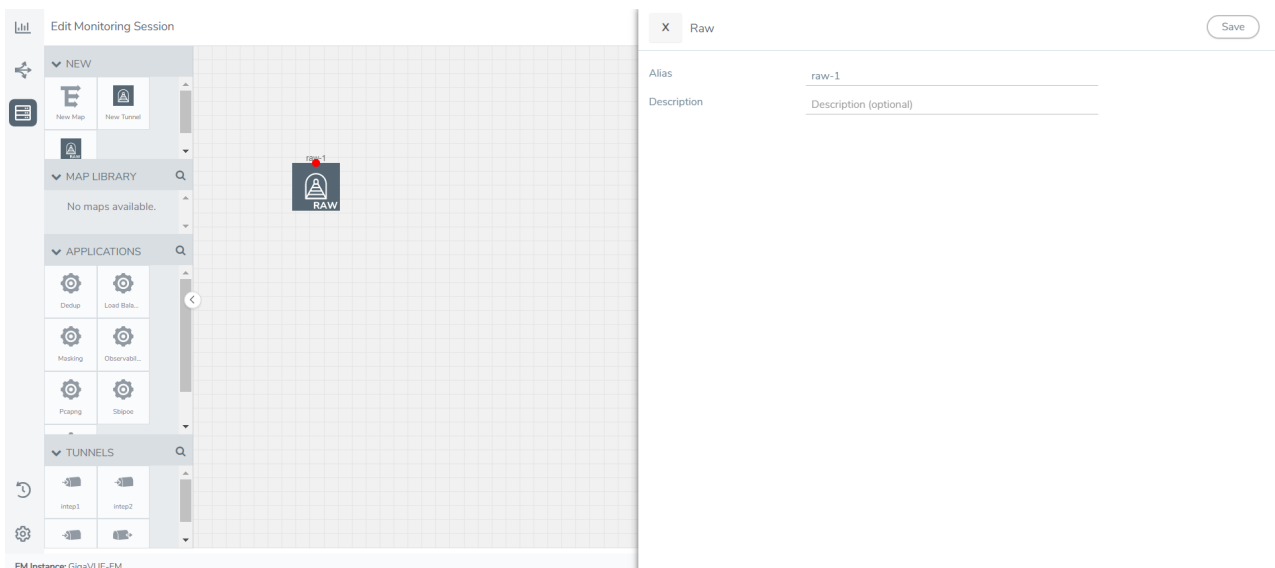
After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When multiple egress tunnels are configured for a monitoring session, then the Egress Tunnel column displays the number of egress tunnels configured in that monitoring session. Hover over the number of egress tunnels to display the names of the egress tunnels used in that particular monitoring session.

Create Raw Endpoint

Raw End Point (REP) is used to pass traffic from an interface. You can optionally use this end point to send traffic to the applications deployed in the monitoring session.

To add Raw Endpoint to the monitoring session:

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



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

Create a New Map

You must have the flow map license to deploy a map in the monitoring session.

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

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

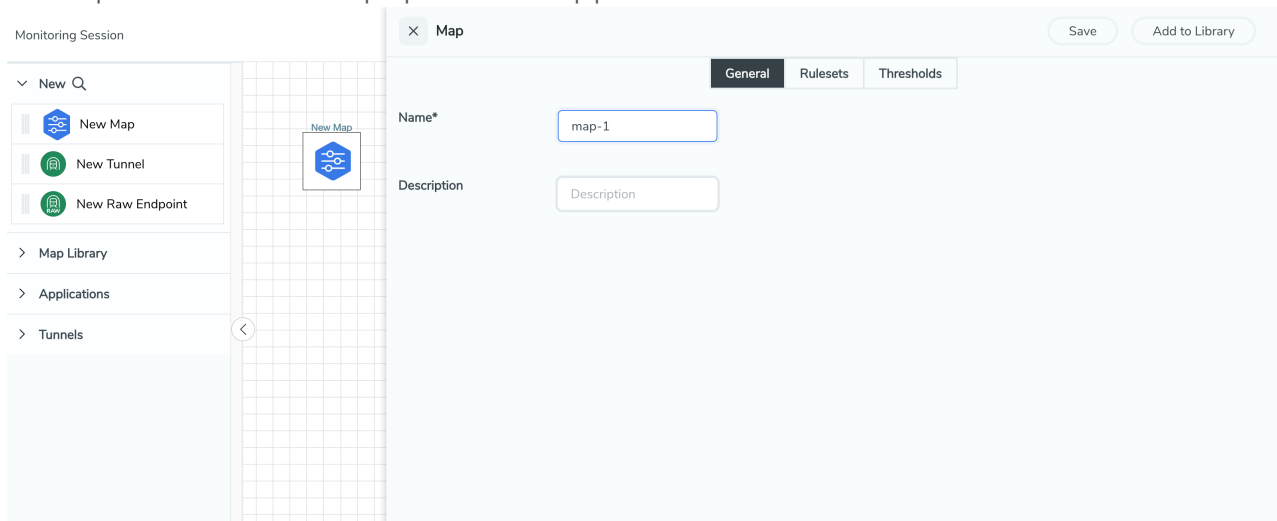
Keep in mind the following when creating a map:

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

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

To create a new map:

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 Map**, drag and drop a new map template to the workspace. The New Map quick view appears.




3. On the New Map quick view, click on **General** tab and enter the required information as described in the following table:

Field	Description
Name	Name of the new map
Description	Description of the map



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

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

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

NOTE: If a packet is fragmented then all the fragments will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Map Statistics" section in *GigaVUE Fabric Management Guide* for detailed information.



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

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

Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.

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

- Click a map and select **Details** to edit the map
- Click a map and select **Delete** to delete the map.
- Click the **Show Targets** button to refresh the subnets and monitored instances details that appear in the **Instances** dialog box.
- Click  to expand the **Targets** dialog box. To view details about a GigaVUE V Series Node, click the arrow next to the VM.
- In the Instances window, click  to filter the list of instances.

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

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

Add Applications to Monitoring Session

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

- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- Application Metadata Exporter
- SSL Decrypt
- 5G-Service based Interface 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*.

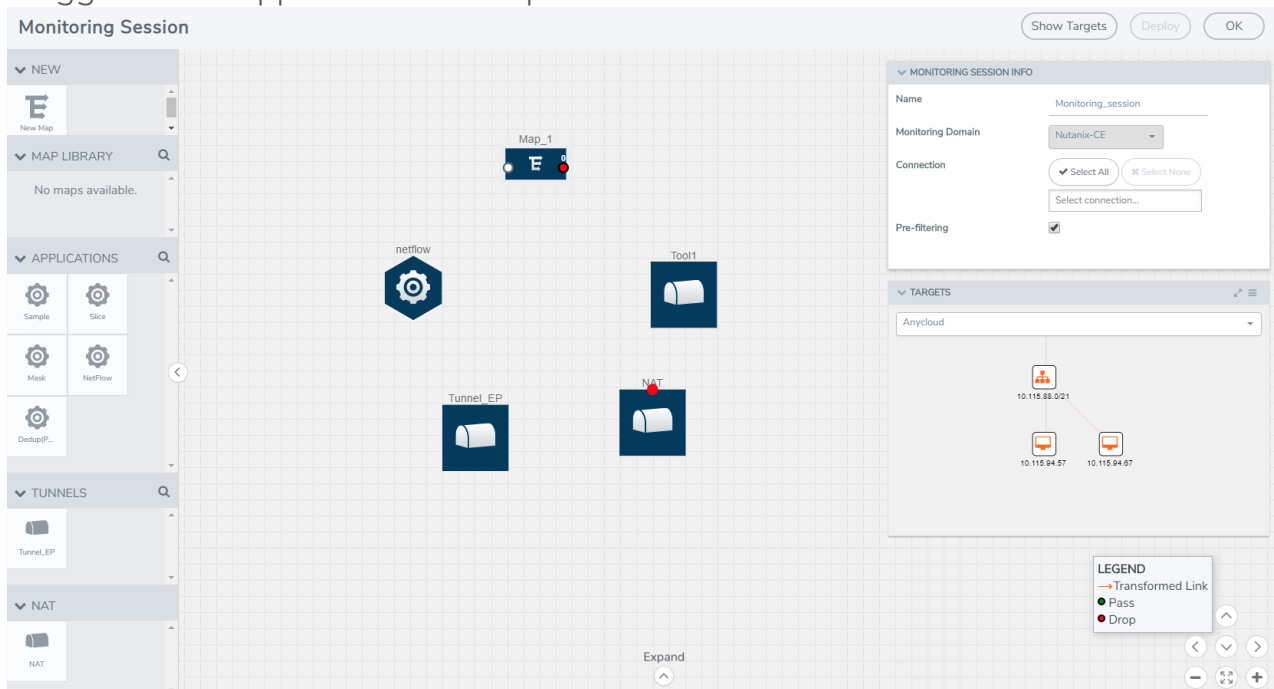
Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop one or more maps from the **MAP Library** to the workspace.
2. (Optional) To add Inclusion and Exclusion maps, drag and drop the maps from the Map Library to their respective section at the bottom of the workspace.
3. (Optional) Drag and drop one or more applications from the APPLICATIONS section to the workspace.

NOTE: For information about adding applications to the workspace, refer to *GigaVUE V Series Applications Guide*

4. Drag and drop one or more tunnels from the TUNNELS section. The following figure illustrates three maps, one exclusion map, one application, and two tunnel endpoints dragged and dropped to the workspace.



You can add up to 8 links from a action set to different maps, applications, or monitoring tools.

5. Hover your mouse on the map, click the red dot, and drag the link over to another map, application, or tunnel. You can drag more than one link from a map to the destination. On these links, you can apply link transformation to alter the packets. For information about adding link transformation, refer to [Add Header Transformations](#).
6. Hover your mouse on the application, click the red dot, and drag the link (arrow) over to the tunnel endpoints. The traffic matching the rules in each action set is routed to maps, applications, or monitoring tools.
7. Click **Show Targets** to view details about the subnets and monitoring instances. The instances and the subnets that are being monitored are highlighted in orange.
8. Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all GigaVUE V Series nodes and UCT-Vs. If the monitoring session is not deployed properly, then one of the following errors is displayed:
 - Partial Success—The session is not deployed on one or more instances due to UCT-V or GigaVUE V Series Node failure.
 - Failure—The session is not deployed on any of the GigaVUE V Series nodes and UCT-Vs.
 Click on the status link to view the reason for the partial success or failure.
9. Click **View** under Statistics to view and analyze the incoming and outgoing traffic.

You can also do the following in the Monitoring Session page:

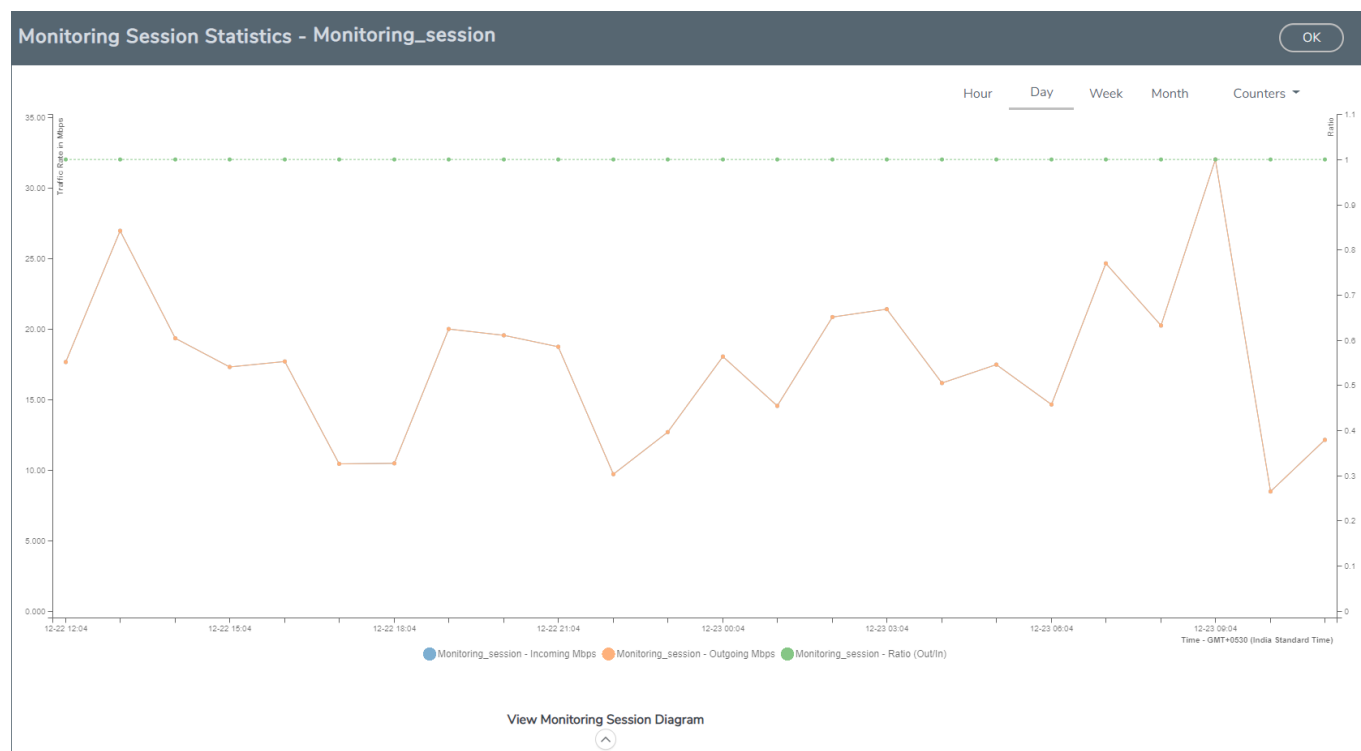
- Use the **Clone** button to duplicate the selected monitoring session.
- Use the **Edit** button to edit the selected monitoring session.
- Use the **Delete** button to delete the selected monitoring session.

View Monitoring Session Statistics

The Monitoring Session Statistics page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. The traffic can be viewed based on kilobits/second, megabits/second or gigabits/second.

On the Monitoring Sessions page, click **View** in the Statistics column to view the Monitoring Session Statistics page. The **Monitoring Session Statistics** page appears where you can analyze incoming and outgoing traffic.

NOTE: If there are multiple monitoring sessions with different target selection, then the incoming maps will not show true statistics and it shows the aggregate traffic from all the targets.



You can also perform the following actions on the Monitoring Session Statistics page:

- Directly below the graph, you can click on **Incoming Mbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view appears.

- On the **Monitoring Session Diagram** page, you can expand any map, or tunnel to open a **Details** quick view of that item to see more details about the incoming and outgoing traffic for that item.
- You can also scroll down the Map **Details** quick view to view the Map Rules, Action Sets, and Map Info for this map. You can select Map Rules or Action Sets to view the traffic matching the selected rule on the graph in the quick view.
- You can also view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual V Series Node, select the name of the V Series Node for which you want to view the statistics from the V Series Node drop-down menu on the top left-corner of the Monitoring Session Statistics page.
- Hover over the V Series Node drop-down to view the number of the applications, end points, and other application environments configured for a particular V Series Node. It also displays the error message related to configuration for the particular V Series Node.

View Health Status on the Monitoring Session Page

You can view the health status of the monitoring session and the components deployed, in the monitoring session page. Refer to [Monitor Cloud Health](#) for more detailed information on how to configure cloud health and view health status.

The following columns in the monitoring session page are used to convey the health status:

Health

This column displays the health status (both traffic and configuration) of the entire monitoring session. The status is marked healthy only if both the traffic and configuration health status is healthy, even if either of them is unhealthy then the health status is moved to unhealthy.

V Series Node Health

This column displays the configuration and traffic health status of the monitoring session deployed in V Series Nodes. This column provides information on the number of GigaVUE V Series Nodes that have healthy traffic flow and monitoring session successfully deployed to the total number of V Series Nodes that have monitoring session deployed.

You can view the health status of the individual V Series Nodes by clicking on the V Series Node Health column.

NOTE: V Series Node health only displays the health status therefore even if the V Series Node is down it will not be reflected in the monitoring session page.

Target Source Health

This column displays the configuration health status of the monitoring session deployed in targets. This column provides information on the number of monitoring sessions successfully deployed on a particular target to the total number of monitoring session deployed on that particular target.

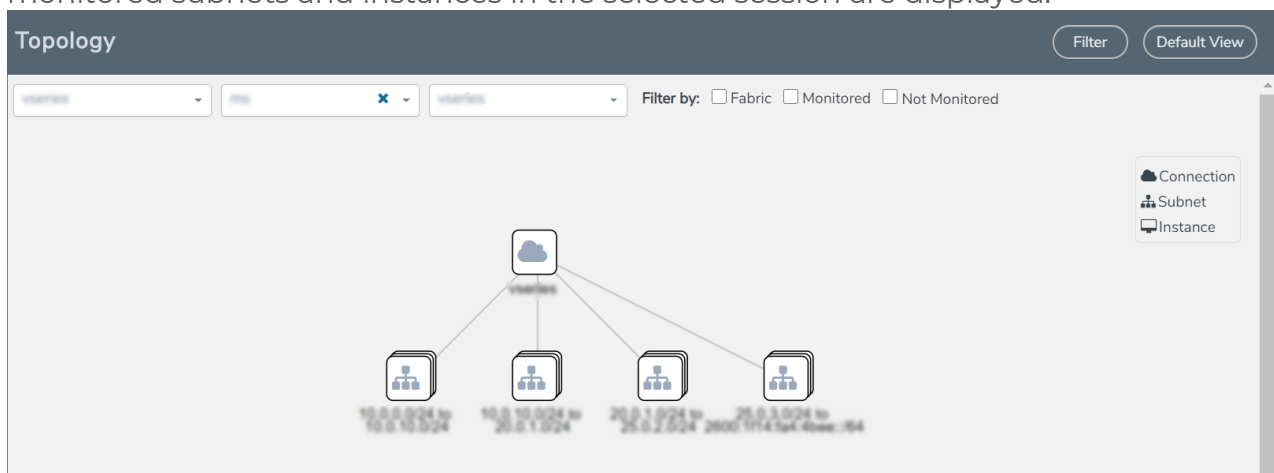
You can view the health status of the individual targets and also the error message associated with them, by clicking on the Target Source Health column.

Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

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



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

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

- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.

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

Configure Application Intelligence Solutions on GigaVUE V Series Nodes using Third Party Orchestration

You can use your own orchestration system to deploy GigaVUE V Series Nodes and then use GigaVUE-FM to configure advanced features like Application Intelligence, Application Metadata Intelligence, and Application Filtering Intelligence.

Deploying the fabric components to configure Application Intelligence session using third party Orchestration can be done in two ways:

- [Generic Mode](#)
- [Integrated Mode](#)

Generic Mode

When using generic mode, GigaVUE-FM automatically creates an environment and connection when you deploy your fabric components in your orchestration system. In this case, the environment and the connections are created after the fabric components registration. The fabric components deployed will listed in both the monitoring page and the connections page. They can only be used in either one of these places. For example: If the GigaVUE V Series Nodes in the Connection page is used to configure Application Intelligence session, then it cannot be used for monitoring purposes in the monitoring domain. The default traffic acquisition method is UCT-Vs. You can edit the connection and change the traffic acquisition method you wish to use.

NOTE: When using generic mode you cannot configure multiple connections under a single connection group.

Integrated Mode

When deploying your fabric components using integrated mode, you must create environments and connections before registering your fabric components. And provide the environment and connection name as groupname and subgroupname in the registration data that will be used in your orchestration system.

To configure the Application Intelligence solution on the GigaVUE V Series Nodes, create a virtual environment with the required connections. After creating the connections, configure the sources and the required destinations for the traffic flow.



Important Notes for Application Intelligence Session:

- You can configure multiple connections under a single connection group (only in integrated mode).
- When upgrading from any previous version to 6.4.00, you cannot enable secure tunnels. You will have to delete the Application Intelligence solution and deploy it again with secure tunnels.
- You cannot enable secure tunnels for an existing Application Intelligence Session, you must delete the Application Intelligence solution and deploy it again with secure tunnels.
- You can deploy multiple GigaVUE V Series Nodes in a connection.
- You can use **V Series Node API Proxy Server** (VPS) to scale and manage multiple V Series Nodes. Refer to the GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide for detailed information.
- You can use tool templates while creating an Application Metadata Intelligence session. To create a custom tool template for GigaVUE V Series Node, signature is required from the node. Refer to the Tool Templates section in the *GigaVUE Fabric Management Guide* for more detailed information.
- When GigaVUE-FM and GigaVUE V Series Nodes are deployed in different cloud platforms, then the GigaVUE-FM public IP address must be added to the **Data Notification Interface** as the Target Address in the Event Notifications page. Refer to [Configuration Settings](#) section in the *GigaVUE Administration Guide* for configuration details.
- When using generic mode the default traffic acquisition method is UCT-V, you can edit the connection and change the traffic acquisition method. This is applicable only when using third party orchestration method. You cannot edit connection when using GigaVUE-FM as your orchestrator.

Configure Environment

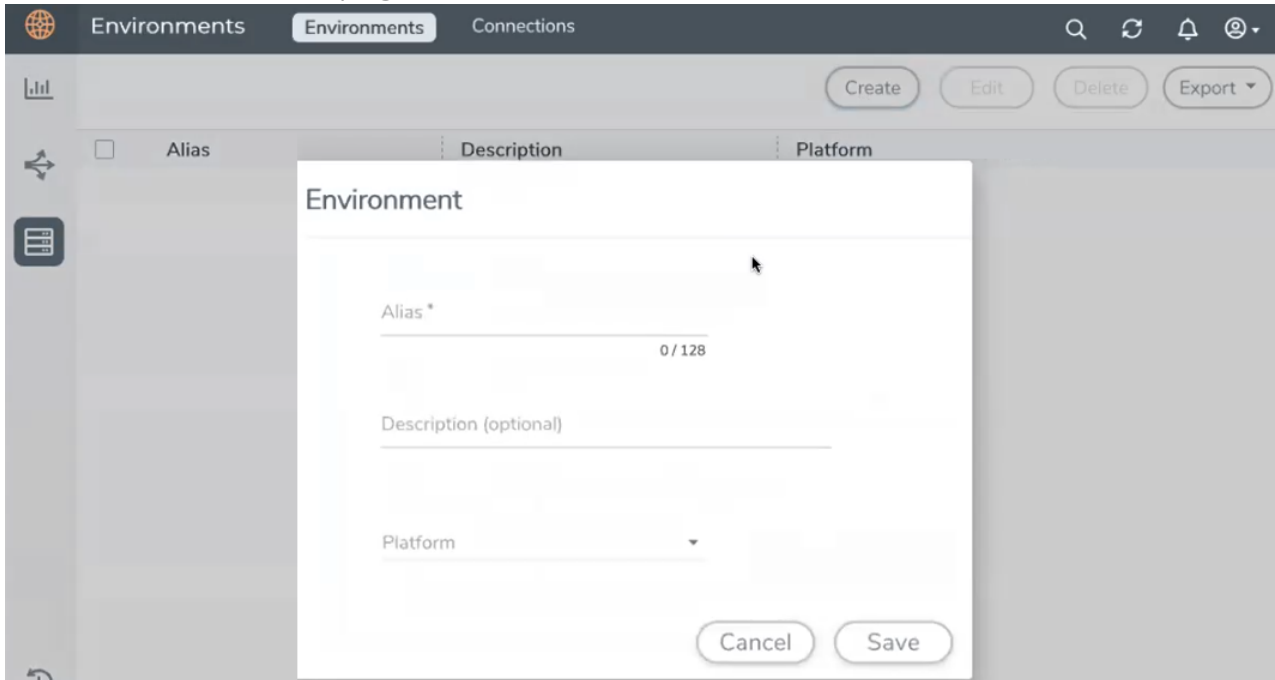
The Environments page allows you to create the following:

- **Environments:** The physical or the virtual environment in which the Application Intelligence solution is to be deployed.
- **Connections:** Connection between GigaVUE-FM and the cloud platform.

Create Environment

To configure the Environment:

1. Select **Inventory > Resources > Environments**.
2. On the **Environments** page, on the **Environments** tab, click **Create**.



3. Select or enter the following details:

Field	Description
Alias	Alias name used to identify the Environment.
Description	Brief description about the Environment.
Platform	Select the cloud platform.

4. Click **Save**. The environment is added to the list view.

Use the following buttons to manage your environment:

Button	Description
Delete	Use to delete an Environment.
Edit	Use to edit the details in an Environment.
Export	Export the details from the Environment page in an XLS or

Button	Description
	CSV file.

Create Credentials

You must configure your AWS and Azure Credentials for configuring the Application Intelligence solution.

Create AWS Credentials

To create AWS credentials:

1. From the left navigation pane, click **Inventory** > **Resources** > **Environment**.
2. On the **Environments** page, on the **Credentials** tab, select **AWS** from the drop-down menu.
3. On the AWS Credential page, click **Add**. The **Configure Credential** page appears.

4. Enter or select the appropriate information as shown in the following table.

Field	Action
Name	An alias used to identify the AWS credential.
Authentication Type	Basic Credentials For more information, refer to AWS Security Credentials .
Access Key	Enter your AWS access key. It is the credential of an IAM user or the AWS account root user.
Secret Access Key	Enter your secret access key. It is the AWS security password or key.

5. Click **Save**.

Create Azure Credentials

To create Azure credentials:

1. From the left navigation pane, click **Inventory > Resources > Environment**.
2. On the **Environments** page, on the **Credentials** tab, select **Azure** from the drop-down menu.
3. In the Azure Credential page, click **Add**. The **Configure Credential** wizard appears.

4. Enter or select the appropriate information for the Azure credential as described in the following table.

Field	Description
Name	An alias used to identify the Azure credential.
Authentication Type	<p>Application ID with Client Secret: Connection with Azure with a service principal. Enter the values for the following fields.</p> <ul style="list-style-type: none"> o Tenant ID—a unique identifier of the Azure Active Directory instance. o Application ID—a unique identifier of an application in Azure platform. o Application Secret—a password or key to request tokens. <p>Refer to Application ID with client secret for detailed information.</p>
Azure Environment	Select an Azure environment where your workloads are located. For example, Azure_US_Government.

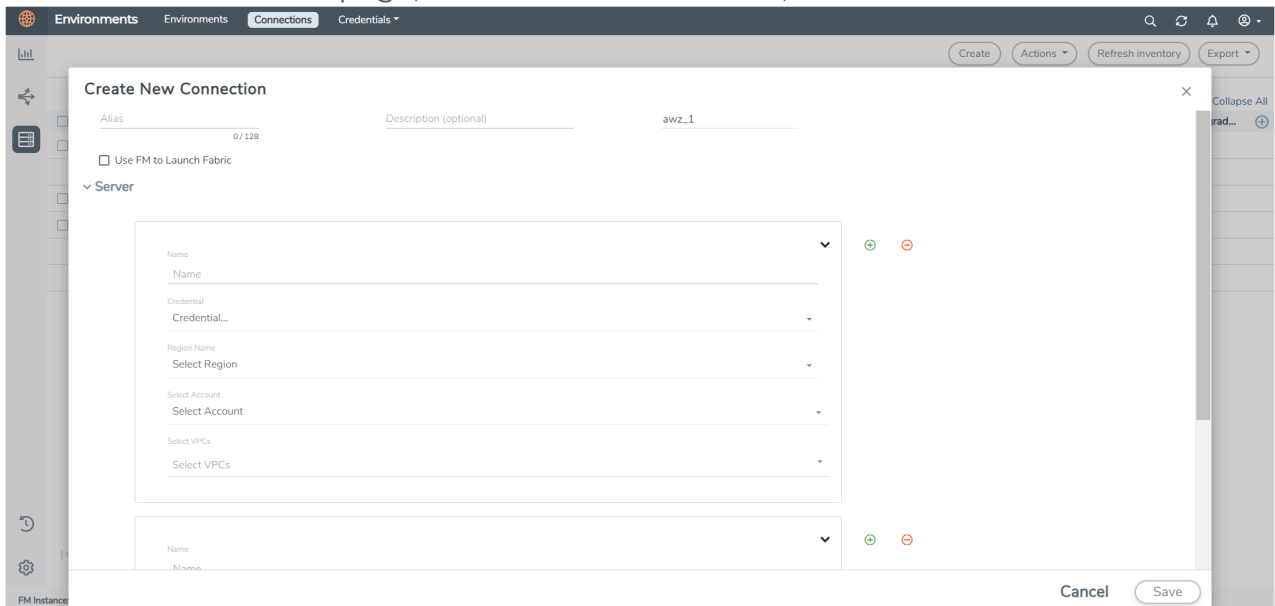
5. Click **Save**.

You can view the list of available AWS and Azure credentials in the Credentials page.

Create Connection

To create a new Connection:

1. Select **Inventory > Resources > Environment**.
2. On the **Environments** page, on the **Connections** tab, click **Create**.



3. The **Create New Connection** dialog box opens.

Field	Description
Alias	Alias name used to identify the connection.
Description	Brief description about the connection.
Environment	Select the environment. Refer to the Configure Environment section Create Connection
Use FM to Launch Fabric	Disable this check box, if you wish to deploy GigaVUE fabric components using third party orchestration.

Connect to AWS

To connect to AWS, select or enter the following details under the server details:

Field	Description
Name	Name used to identify the connection.
Credential	Select your credentials from the drop-down menu. Refer Create Credentials for detailed information on how to create credentials.
Secret Region	The AWS region for the connection. For example, EU (London). <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> NOTE: If the region you want to choose is not available in the Region Name list, you </div>

Field	Description
	<p>can add a custom region.</p> <p>Adding a Custom Region</p> <p>To add a custom region:</p> <ol style="list-style-type: none"> In the Region Name drop-down list, select Custom Region. In the Custom Region Name field, enter the name of the region that is not available in the list.
Select Account	Select the AWS account name/id.
Select VPCs	Select the VPC
Traffic Acquisition Method	<p>Select a Tapping method. The available options are:</p> <ul style="list-style-type: none"> UCT-V: If you select UCT-V as the tapping method, you must configure the UCT-V Controller to monitor the UCT-Vs. You can also configure the UCT-V Controller and UCT-Vs using your own orchestrator. Refer to Configure GigaVUE Fabric Components using AWS Orchestrator for detailed information. VPC Traffic Mirroring: If you select VPC Traffic Mirroring option as tapping method, only nitro-based agent is support. If you wish to use an external load balancer (optional). Select Yes to use a load balancer. Refer to Configure an External Load Balancer for detailed information. UCT-V Controller configuration is not required for VPC Traffic Mirroring. <p>NOTE: VPC Traffic Mirroring is not applicable when generic mode.</p> <ul style="list-style-type: none"> Tunnel: If you use select Tunnel as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to GigaVUE V Series Nodes without deploying UCT-Vs or UCT-V Controllers.. <p>NOTE: For VPC Traffic Mirroring option, additional permissions are required. Refer to the Permissions for details.</p>
MTU	<p>The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry.</p> <p>NOTE: The default MTU is 1450. You can edit the MTU value according to your requirements. The valid range is between 1450 to 9000.</p>

Connect to Azure

To connect to Azure, select or enter the following details:

Field	Description
Name	Name used to identify the connection.
Credential	Select your credentials from the drop-down menu. Refer Create Credentials

Field	Description
	for detailed information on how to create credentials.
Subscription ID	Select the subscription ID.
Region Name	The Azure region for the connection. For example, East Asia.
Resource Groups	The Resource Groups created in Azure for communication between the controllers, nodes, and GigaVUE-FM. A Resource Group must contain the VMs that needs to be monitored.
Traffic Acquisition Method	Select a Tapping method. The available options are: <ul style="list-style-type: none"> ● UCT-V: If you select UCT-V as the tapping method, you must configure the UCT-V Controller to monitor the UCT-Vs. ● Tunnel: If you use select Tunnel as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to V Series nodes without deploying UCT-Vs or UCT-V Controllers.
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: The default MTU is 1450. You can edit the MTU value according to your requirements when using integrated mode. The valid range is between 1450 to 9000. However when using generic mode, ensure the MTU is set to 1450.</p> </div>

Connect to VMware ESXi

To connect to VMware, select or enter the following details:

NOTE: You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using the Third Party Orchestration in VMware ESXi host.

Field	Description
vCenter IP Address/ Hostname	The IP address of the virtual server.
vCenterUserName	Valid user name
vCenterPassword	Password for the user

Connect to VMware NSX-T

Rules and Notes

- NSXT- manager version must be 3.1.3. Otherwise after editing the solution, the packets will not reach the GigaVUE V Series Node.
- NSX-T manager cannot be registered for more than one GigaVUE-FM.

- For GigaVUE-FM software version 5.13.00, you cannot deploy more than one GigaVUE V Series Node.
- **For GigaVUE-FM software version 5.13.00:** If you configure a GigaVUE V Series Node with the Application intelligence solution, then you must not configure other basic GigaSMART applications, such as slicing, masking, and vice-e-versa. These GigaSMART applications cannot work in parallel.

To connect to VMware NSX-T, select or enter the following details:

Field	Description
Alias	Alias name used to identify the connection.
Description	Brief description about the connection.
Environment	Select the environment configured in the Create Connection
Server	The IP address or the DNS name of the virtual server.
vCenterUserName	Valid user name
vCenterPassword	Password for the user
NSX-T Manager IP Address	IP address or Hostname of your VMware NSX-T.
NSX-T User Name	Username of your NSX-T account.
NSX-T Password	Password of your NSX-T account.
Image URL	Web Server URL of the directory where V Series node OVA, VMDK, and OVF files are available. The Web Server URL must be in the following format: <i>http://<server-IP:port>/<path to where the OVF files are saved></i> and the port can be any valid number.
GigaVUE-FM User Name	GigaVUE-FM username.
GigaVUE-FM Password	GigaVUE-FM password

After creating a connection, deploy your fabric components. Refer to [Deploy Fabric Components using Generic Mode](#) for more detailed information on how to deploy fabric components like UCT-Vs, UCT-V Controllers, and GigaVUE V Series Node and Proxy using your own orchestrator for the above mentioned platforms.

NOTE: When a UCT-V Controller is unregistered, the solution goes to a failed state, to resolve this ensure either deploy a new UCT-V Controller or redeploy the existing UCT-V Controller.

Create Source Selectors

When setting up a traffic flow, it is important to define the selection criteria for the source of traffic. Use the Source Selectors page for configuring the source of traffic to the GigaVUE V Series nodes.

NOTE: When deploying the Application Intelligence using Source Selector, if the GigaVUE V Series Node is down, you will not be able to view the Selected Targets and UCT-Vs.

To configure the Source Selectors:

1. Select **Inventory > Resources > Source Selectors**.
2. On the **Source Selectors** page, on the **VM** tab, click **Create**. The **Create Source Selector** wizard appears.

Create Source Selector



Alias Description

0 / 128 0 / 128

Filters

Criteria 1 -

Filter Operator + -

[+ New Criteria](#)

Cancel Save

3. Enter or select the required information:

Field	Description
Alias	Name of the source
Description	Description of the source
Filters	You can create a filter template from the Filters option
Criteria 1	Criteria to filter the traffic source. NOTE: You can create multiple criteria.
Filter	The criteria based on which the traffic is filtered. Select from the list of available filters. NOTE: Ensure that the registered traffic agents match the filter criteria.
Operator	Select the required operator based on the filter selected. Options are: <ul style="list-style-type: none"> Starts with Ends with excludes equals between
Values	The values for the filter.

4. Click Save to save the source selector.



Note: You can create multiple filter criteria. Within each criterion, you can configure multiple filters.



- If you have configured multiple filters in a criterion, then the traffic will be filtered only if all the filter rules are true.
- If you have configured multiple criteria, then the traffic will be filtered even if one of the criteria is true.
- A maximum of 25 inclusion rulesets and 25 exclusion rulesets can be added.

Create Tunnel Specifications

A tunnel endpoint can be created using a standard L2GRE, VXLAN, or ERSPAN tunnel. The tunnel can be an ingress tunnel or an egress tunnel.

NOTE: VXLAN is the only supported tunnel type for Azure.

To configure the tunnels:

1. Select **Inventory > Resources > Tunnel Specifications**.
2. On the **Tunnel Specifications** page, navigate to **VM** tab and click **Create**. The Create Tunnel Specification wizard appears.

Create tunnel specification

✕

Alias

Description

Alias *


Description (optional)

Tunnel type

Cancel

Save

3. Enter or select the following information:

Field	Description
Alias	<p>The name of the tunnel endpoint.</p> <p>NOTE: Do not enter spaces in the alias name.</p>
Description	The description of the tunnel endpoint.
Tunnel Type	<p>The type of the tunnel.</p> <p>Select ERSPAN, or L2GRE, or VXLAN to create a tunnel.</p> <p>Do not select UDPGRE tunnel type.</p> <p>NOTE: VXLAN is the only supported tunnel type for Azure.</p>
Traffic Direction	<p>The direction of the traffic flowing through the V Series node.</p> <ul style="list-style-type: none"> Choose In (Decapsulation) for creating an Ingress tunnel, Tunnel Spec for the Source should always have the Traffic Direction as IN, signifying an ingress tunnel. Enter values for the Key. Choose Out (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint. Select or enter values for MTU, Time to Live, DSCP, PREC, Flow Label, and Key. <p> ERSPAN, L2GRE, and VXLAN are the supported Ingress tunnel types. You can configure Tunnel Endpoint as your first level entity in Monitoring Session.</p> <ul style="list-style-type: none"> L2GRE and VXLAN are the supported Egress tunnel types. For Azure connection, VXLAN is the supported Ingress and Egress tunnel type.
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
Remote Tunnel IP	<p>For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.</p> <p>For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.</p>

4. Click **Save** to save the configuration.

User Defined Application

This feature gives you the ability to classify the applications by the DPI engine. This allows unclassified TCP, UDP, HTTP, and HTTPS applications to be identified and named with the help of user defined application signatures.

To configure User Defined Application signatures :

Step Number	Task	Refer the following
1	Create rules under User Defined Application Section	Create rules under User Defined Application
2	Configure Application Intelligence Session	For Physical: Application Intelligence Session For Virtual: Configure Application Intelligence Session
3	Monitor User Defined Application	View the Application Intelligence Dashboard

Create Rules under User Defined Application

1. Click **Inventory**.
2. Click **User Defined Applications** to create rules based on a set of **Supported Protocols and Attributes**. For information on **Supported protocols and Attributes** refer **User Defined Application** topic. This helps the physical or virtual node to classify the traffic based on the protocols and attributes selected in the created rule.
3. Click **New** in the **User Defined Applications** screen to create a new rule.
4. Enter **Application Name**.
5. Enter **Priority**. The value must be between 1 and 120.
Note: The least value will have the highest priority.
6. In the created rule:
 - a. Choose the **Protocol** from the list of protocols.
 - b. Choose the **Attributes** from the list of attributes.
 - c. Choose the **Values** from the list of values.

7. Click **Apply**. The rule is now created. For information on the limitations for creating rules refer Configuration Limitations section.
8. Click the application listed under the **Applications** column.
9. Click the **Rule** tab.
10. Select a rule to view its protocol details.

Supported Protocols and Attributes

The DPI engine will match the rules defined based on the following protocols and attributes within the first 500 bytes of a packet payload.

For supported Regexp patterns, refer [Supported RegExp Syntax](#)

Protocol	Attributes	Attribute Labels	Description	Direction	Supported Data Type	Example Value
http	cts-uri	Request URI	Partially Normalized URL (path + request)	Client to Server Only	REGEXP	<code>\fupload\(create_file new_slice upload_slice)\?.*upload_token=.*</code>
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	<code>(.*\.)?gigamon\.com</code>
	mime_type	MIME Type	Content type of Request or the Web page	Both, Client to Server or Server to Client	REGEXP	http
	cts-user_agent	User Agent	Software / Browser used for request	Client to Server Only	REGEXP	mozilla
	cts-	Referer	Source	Client	REGEXP	<code>http:\Wgigamon.com\</code>

	referer	URI	address where client got the URI	to Server Only		
	stc-server_agent	Server Agent	Software used for the server	Server to Client Only	REGEXP	NWS_TCloud_PX
	stc-location	Redirect Location	Destination address where the client is redirected to	Server to Client Only	REGEXP	.*\Vfootball\ .*
	cts-cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Content	Message body content	Both, Client to Server or Server to Client	REGEXP	.*GIGAMON.* mindata = 206 Refer Mindata
ssl	common_name	Domain Name	Domain name from Client Hello message or the certificate		REGEXP	(.*\.)?gigamon\.com
	stc-	Subject	List of	Server	REGEXP	(.*\.)?gigamon\.com

	subject_ alt_ name	t Alt Name (s)	host names which belong to the same certificat e	to Client Only		
rtmp	cts- page_ url	Page URL	URL of the webpage where the audio/vid eo content is streame d	Client to Server Only	REGEXP	http:\\\\www.music.tv\\recode d\\1234567
tcp	stream	Payloa d Data	Data payload for a packet, excludin g the header.		REGEXP	.*GIGAMON.* mindata = 70 Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
udp	stream	Payloa d Data	Data payload for a packet, excludin g the header		REGEXP	.*GIGAMON.* mindata = 100 Refer Mindata
	port	Server Port	Server (listen)		UINT16 RANGE	80-4350

			port number		as REGEXP String	
sip	user_agent	User Agent	Software used	Both, Client to Server or Server to Client	REGEXP	GVUE-release 6.2.0
icmp	code	Message Code	Code of the ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	200
	typeval	Message Type	Type of ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	10
ip	address	Server IP Addresses	IP address of the server		IPV4 as REGEXP String	62.132.12.30/24
	dscp	DSCP Value	DSCP from Differentiated Service (DS) Field in IP header		UINT8 as REGEXP String	33

	resolv_name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Address	IP address of the server		IPV6 as REGEXP String	2001:0:9d38:6ab8:307b:16a4:9c66:5f4 2001:0:9d38::9c66:5f4/64
	dscp	DSCP Value	DSCP from Differentiated Service (DS) Field in IP header		UINT8 as REGEXP String	43

Mindata

The mindata value is the number of payload bytes to buffer and match a given pattern. You can configure mindata value for HTTP content, TCP stream, and UDP stream. The buffer size is calculated from the start of the payload and the default buffer size is different for each protocol (HTTP - 206, TCP - 67, and UDP - 48.)

For example, for pattern ".*TEST.*" that may be present within the first 67 bytes of TCP payload, you can specify the mindata value as 4 (which is the length of the input string) or as 67 (which is the default buffer size of TCP payload). In case, the pattern is present in between 65 to 68 bytes of the payload and the mindata is specified as 4 or 67, it will not match. For this case, you must specify the mindata value as 68.

Supported RegExp Syntax

Pattern	Description
.	Matches any symbol
*	Searches for 0 or more occurrences of the symbol or character set that precedes it
+	Searches for 1 or more occurrences of the symbol or character set that precedes it
?	Searches for 0 or 1 occurrence of the symbol or character set that precedes it
()	Groups a series of expressions together

[]	Matches any value included within the bracket at its current position Example: [Dd]ay matches Day and day
 [<start>-<end>]	Separates values contained in (). Searches for any one of the values that it separates. Example: The following expression matches dog or cat: (dog cat). Matches any value contained within the defined range (a hyphen indicates the range). You can mix character class and a hexadecimal range Example: [AaBbCcDdEeFf0-9]
\0 <octal_ number>	Matches for a direct binary with octal input
\x<hexadecimal- number>\x	Matches for a direct binary with hexadecimal input
\[<character- set>\]	Matches a character set while ignoring case. WARNING: Not performance friendly

Limitations

- The maximum number of user defined application that can be configured is 120 per FM. These applications can be spread across one or more application intelligence sessions.
- The maximum number of rules that can be created per application is 8.
- The maximum number of protocols that can be configured per rule is 3.

Configure Application Intelligence Session

Application Intelligence provides a comprehensive solution that:

- identifies the applications contributing to the network traffic.
- isolates preferred application-specific traffic and directs it to the appropriate tools.
- exports relevant application metadata for further analytics and analysis.

Application Intelligence provides the following capabilities for both physical devices and virtual nodes:

- **Application Visualization (earlier known as Application Monitoring)** - Identifies and monitors all applications contributing to the network traffic, and reports on the total applications and the total bandwidth they consume over a select period. Able to identify more than 3,200 applications. It displays the traffic statistics in bytes, packet and flows.

- **Application Filtering Intelligence**- Enables traffic filtering by layer 7 applications, which means you can filter out high-volume, low-risk traffic from reaching the tools and distribute high-risk network traffic of interest to the right tool at the right time.
- **Application Metadata Intelligence** - Supports exporting over 5000 attributes of metadata that provide relevant usage context on over 3,200 applications, thus enabling you to rapidly identify indicators of compromise (IoC) for security analytics and forensics tools.

Prerequisites

- The environment on which the Application Intelligence solution is to be deployed must already be created and the nodes must be deployed on it.
- In virtual environment, the destination tunnels for the Application Filtering Intelligence Map must already be created.

NOTE: For Application Visualization and Application Metadata Intelligence, the destination(s) are defined internally by the solution.

Create an Application Intelligence Session in Virtual Environment

To create an Application Intelligence Session:

1. On the left navigation pane, select **Traffic > Solutions > Application Intelligence**.
2. Click **Create New**. The **Create Application Intelligence Session** page appears.

3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created:
 - Virtual- connects to the specific environment.
4. In the Environment section, select the **Environment Name**, and the **Connection Name**. To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides..

5. In the **Configurations** section, complete the following:
- Select an **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization. The valid range is 60–900 seconds.
 - Select the required interface. By default, **Management Interface** is enabled. To export the data through tunnel interface, uncheck the Management Interface check box.
 - Enter a value for the **Scale Unit**. The scale unit represents the number of flows supported by the application. If the scale unit value is 1, the maximum active flow limit will be 100k.
Refer to the following table for the maximum scale unit supported for VMware, AWS Nutanix, and Azure platforms.

Cloud Platform	Instance Size	Maximum Scale Unit	
		Secure Tunnel Disabled	Secure Tunnel Enabled
VMware	Large (8 vCPU and 16 GB RAM)	3	2
AWS	Large (c5n.2xlarge)	4	3
	Medium (t3a.xlarge)	3	1
Azure	Large (Standard_D8s_V4)	9	5
	Medium (Standard_D4s_v4)	3	1
Nutanix	Large (8 vCPU and 16 GB RAM)	3	2

NOTE: If the Application Intelligence Session deployment fails, due to using a scale unit other than the recommended scale unit, then reload the GigaVUE V Series Node.

6. In the **Source Traffic** section, select anyone of the following:
- **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to [Create Source Selectors](#).
 - **Prefilter** - Enable the mirroring option, select the prefilter checkbox and then select the policy. If you want to enable Secure tunnel, then select the secure tunnel checkbox.
 - **Precryption**: Select the Precryption checkbox and then select the policy. If you want to enable Secure tunnel, then select the secure tunnel checkbox.

NOTE: You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using the Third Party Orchestration in VMware ESXi host.

- **Tunnel Specification-** Select the tunnel from the drop-down list box. To create new tunnel, select **New Source Tunnel Spec** and add the details for the tunnel. For more information on creating a new tunnel, refer to [Create Tunnel Specifications](#).

NOTE: Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration.

- **Raw End Point-** Select the Raw End Point Interface from the drop-down menu which will trap the traffic for application monitoring.


NOTE: This field is applicable only when you deploy your GigaVUE V Series Nodes using third party orchestration in VMware ESXi Host, Nutanix and Google Cloud Platform.




- Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel.
- For Azure Connection, VXLAN is the only supported Tunnel Type.

7. Click **Save**. The session created is added in the list view.
8. In the **User Defined Applications** section, select the template from the list. For information on **Supported protocols and Attributes** and **Limitations** refer **User Defined Application** topic.


The total applications participating in the network traffic are displayed in the Application Intelligence Dashboard. For more information about the dashboard, refer to the [View the Application Intelligence Dashboard](#).

Select the session from the Application Intelligence Sessions pane and click on the  icon and select **View Details** from the drop-down menu, to view the deployed UCT-V, their status and more information about source selectors, selected target.

If the session configuration is unsuccessful, troubleshoot the error notified (refer to [View the Health Status of a Solution](#)). Click the **Reapply all pending solutions** button  in the dashboard to redeploy the configuration.

NOTE: GigaVUE-FM takes few minutes to display the application statistics.

NOTE: The option **Reapply all pending solutions** is applicable for physical solution only.

When the Application Intelligence solution is in suspended state, you cannot delete the session. You can click on the  icon and select **View Details** from the drop-down menu, to view the details.

You can also filter the traffic based on the applications. For more information, see [Create Application Filtering Intelligence](#).

Slicing and Masking in Application Filtering Intelligence

When the traffic passes through the Application Filtering Intelligence, application metadata is created. With the addition of slicing and masking parameters to the existing application filtering functionality, you will be able to slice, mask, or slice and mask the filtered packets before sending them to the destination tunnel endpoint.

For step-by-step instructions on how to configure Application Filtering Intelligence refer to [Create Application Filtering Intelligence by Editing Monitoring Session from Dashboard](#) topic from *GigaVUE Fabric Management Guide*.

Configuring Application Filtering Intelligence with Slicing

You can enable the slicing configuration and provide inputs for each **Application Filtering** rule set:

1. From the **Select a Protocol** drop-down list, choose a protocol.
2. In the **Offset** field, specify the length of the packet that must be sliced.

The filtered traffic will be sliced before forwarding it to the destination tunnel endpoint.

Refer to Slicing section in the *GigaVUE V Series Applications Guide* for more detailed information on Slicing.

Configuring Application Filtering Intelligence with Masking

You can enable the masking configuration and provide inputs for each **Application Filtering** rule set:

1. From the **Select a Protocol** drop-down list, choose a protocol.
2. In the **Offset** field, specify the length of the packet that must be masked.
3. In the Pattern field, enter the pattern for masking the packet.
4. In the Length field, enter the length of the packet that must be masked.

The filtered traffic will be masked before forwarding it to the destination tunnel endpoint.

Refer to Masking section in the *GigaVUE V Series Applications Guide* for more detailed information on Masking.

Configuring Application Filtering Intelligence with Slicing and Masking

You can enable both slicing and masking configurations, and provide inputs for each **Application Filtering** rule set.

The filtered traffic will be sent to the slicing application, the sliced traffic will be sent to masking application and then to the destination tunnel Endpoint.

NOTE: When combining slicing and masking operations, the offset range of the masking must be lesser than the offset value entered for the slicing operation, as the slicing operation is performed first.

Application Metadata Intelligence

Application Metadata Intelligence generates more than 5000 attributes for more than 3200 applications without impacting the users, devices, applications, or the network appliances. The feature identifies applications even when the traffic is encrypted.

Application Metadata Intelligence (AMI) is enabled to multi-collect protocols with more than one metadata attribute of the same type. The multi-collect feature supports additional protocols such as DNS, GTP,GTPV2, DHCP, HTTP, HTTPS, SSL, HTTP_PROXY, HTTP2, KERBEROS5, and DHCP6.

The generated metadata is exported in IPFIX (IP Flow Information Export) format and CEF (Common Even Format) to security analytics and forensics tools thereby providing greater visibility to enforce corporate compliance.

The output from the Application Metadata Intelligence in CEF format can also be converted to JSON format using Application Metadata Exporter (AMX) application. To learn more about AMX application refer to Application Intelligence—Application Metadata Exporter


Application Metadata Intelligence generates metadata only if the application is allowed to be passed in Application Filtering Intelligence. For example, Application Metadata Intelligence has the capability to generate metadata for HTTP traffic only if Application Filtering Intelligence filters in the HTTP traffic.

Refer to [Create Application Metadata Intelligence Session for Virtual Environment](#) topic for step-by-step instructions on how to configure Application Metadata Intelligence on Virtual Environment.

Create Application Metadata Intelligence Session for Virtual Environment

You can create an Application Metadata Intelligence session for virtual environment.

To create an Application Metadata Intelligence session, follow these steps:

1. Go to **Traffic > Solutions > Application Intelligence**.
2. From the Sessions pane, click  and select **Edit**. The **Edit Application Intelligence Session** window appears.
3. In the **Edit Application Intelligence Session** window, click **Application Metadata**.

NOTE: If Application Filtering Intelligence License is available, you must create Application Filtering to create Application Metadata Intelligence. For more information, refer to [Create Application Filtering Intelligence by Editing Monitoring Session from Dashboard](#)


4. In the **Destination Traffic** section, click **+ Add New** to create an exporter to receive application-specific traffic. You can also create multiple exporters.
- a. Enter the following details:

Field	Description
Tool Name	Enter the tool Name
Tool IP Address	Enter the tool IP address
Template	Select the tool template. Refer to Tool Templates for more details on what are tool templates and to create custom tool templates.
L4 Source Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
L4 Destination Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
APPLICATION ID	Enable to export the data with Application Id.
Format	Select NetFlow or CEF
NetFlow: Select this option to use Netflow	
Record / Template type	<ul style="list-style-type: none"> ● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds
CEF: Select this option to use CEF	
Record / Template type	<ul style="list-style-type: none"> ● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.

- b. Click **App Editor**, to select the applications and its attributes. You can select a maximum of 64 attributes for each of the application. (Not applicable when using NetFlow V5 Template in the above **Template** drop-down menu.) The Application Editor screen appears as shown:

- c. Select an **Application Family** and the **Applications** that needs to be filtered from the traffic. You can also select **Add All Applications in Family** or **Delete All Applications in Family**. The selected applications and their families appear in the **Selected Applications** section.

NOTE: You can select the required applications without selecting the application family.

5. In the **Advanced Settings > Collects** section, you can select the following packet attributes:
 - Counter - Select the Bytes, and Packets.
 - IPv4 - Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.
 - IPv6 - Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
 - Transport -Select the required attributes. By default, Source Port, Destination Port are enabled.
- a. By default, the above collect types are displayed. Click  to add the following collect types:
 - Data Link - Select any one of the parameters such as Source Mac, Destination Mac and VLAN.
 - Timestamp - Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
 - Flow - Select the parameter as End Reason if required.
 - Interface - Select any one of the parameter such as Input Physical, Output Physical and Input Name.

6. In the **Application Metadata Settings** section:
 - a. Select the Flow Behavior as any one of the following:
 - Uni-Directional
 - Bi-Directional. The default value is Bi-Directional.
 - b. Enter the Timeout and Cache Size.
 - c. You can enable or disable the **Multi-Collect** option to perform the following:
 - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
 - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.
 - d. You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

NOTE: You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

- e. You can enable or disable the **Advance Hash** option to perform the following:
 - **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
 - **Disable** — Disables the metadata cache advance-hash for flows.
 - f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.
 - g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.
7. Click **Save**.

The metrics of the Application Metadata traffic appear on the dashboard.

Create NetFlow Session for Virtual Environment

Note: This configuration is applicable only when using NetVUE Base Bundle.

NetFlow Generation is a simple and effective way to increase visibility into traffic flows and usage patterns across systems. The flow-generated data can be used to build relationships and usage patterns between nodes on the network.

To create an NetFlow session, follow these steps:

1. On the left navigation pane, select **Traffic > Solutions > Application Intelligence**.
2. Click **Create** . The **Create Application Intelligence Session** page appears.
3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created.
4. In the Environment section, select the **Environment Name**, and the **Connection Name**. To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides.
5. In the **Configurations** section, complete the following:
 - a. The **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization is 5 seconds
 - b. By default, **Management Interface** is enabled.

6. In the **Source Traffic** section, select anyone of the following:
 - a. **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to [Create Source Selectors](#)

NOTE: You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using Third Party Orchestration in VMware ESXi Host

- b. **Tunnel Specification**- Select the tunnel from the drop-down list box. To create new tunnel, select **New Source Tunnel Spec** and add the details for the tunnel. For more information on creating a new tunnel, refer to [Create Tunnel Specifications](#).

NOTE: Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration. Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel. For Azure Connection, VXLAN is the only supported Tunnel Type.

- c. **Raw End Point**- Select the Raw End Point Interface from the drop-down menu which will tap the traffic for application monitoring.

NOTE: This field is applicable only when you deploy your GigaVUE V Series Nodes using third party orchestration in VMware ESXi Host, Nutanix and Google Cloud Platform.

7. Click on the **Application Metadata** tab.

8. In the **Destination Traffic** section, click **+ Add New** to create an exporter to receive application-specific traffic. You can only create a maximum of 5 exporters. Enter the following details:

Field	Description
Tool Name	Enter the tool name.
Tool IP Address	Enter the tool IP address.
Template	Select the tool template. Refer to Tool Templates for more details on what tool templates are and to create custom tool templates.
L4 Source Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
L4 Destination Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
APPLICATION ID	Enable to export the data with Application Id.
Format	NetFlow
Record / Template type	<ul style="list-style-type: none"> ● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds.

9. In the **Advanced Settings > Collects** section, the following details are already configured.

NOTE: When the template is NetFlow v5 or when the format is NetFlow and the version as V5 you cannot modify the **Collects**.

- TimeStamp
- Counter
- Interface
- IPv4
- Transport

10. In the **Application Metadata Settings** section:
- Select the Flow Behavior as any one of the following:
 - Uni-Directional
 - Bi-Directional. The default value is Bi-Directional.
 - Enter the Timeout and Cache Size.
 - You can enable or disable the **Multi-Collect** option to perform the following:
 - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
 - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.
 - You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

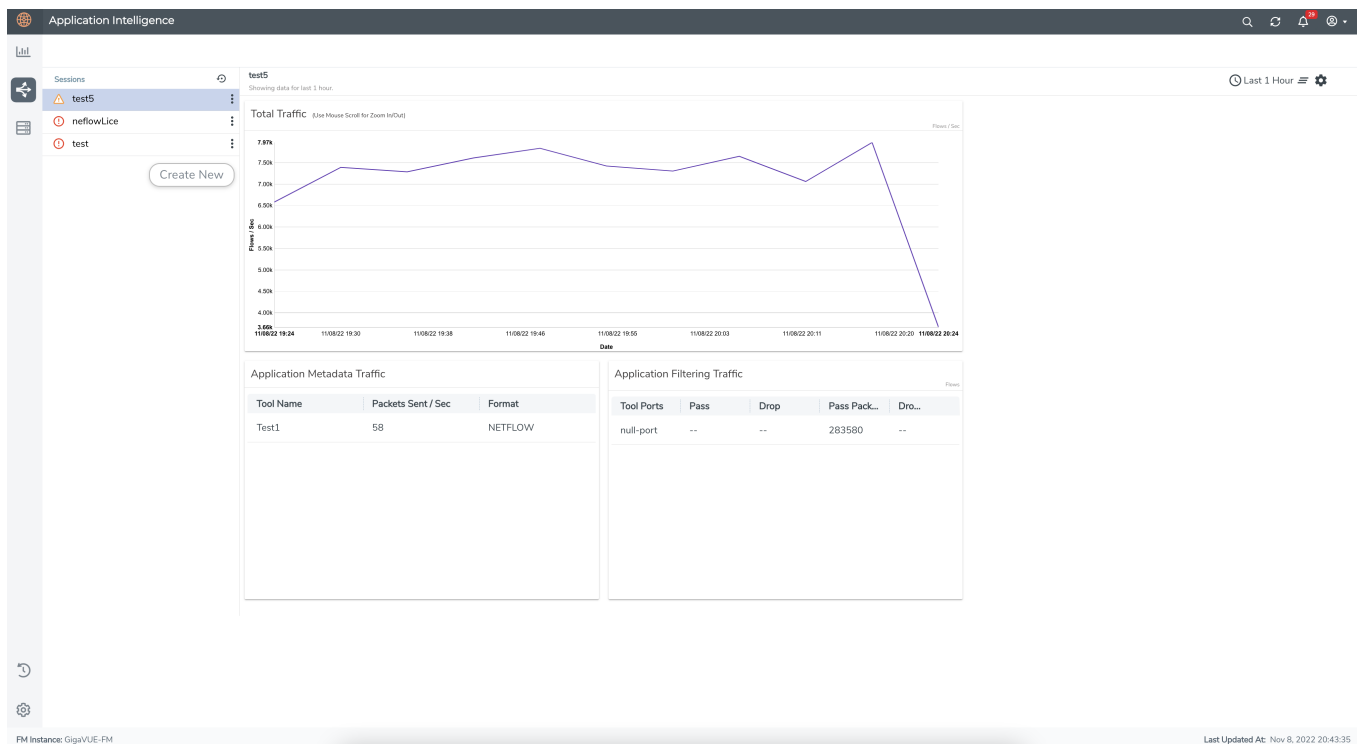
Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

NOTE: You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

- e. You can enable or disable the **Advance Hash** option to perform the following:
 - **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
 - **Disable** — Disables the metadata cache advance-hash for flows.
 - f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.
 - g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.
11. Click **Save**.

NetFlow Dashboard

In Appviz, only the traffic statistics are displayed as applications cannot be configured and used in the NetFlow configuration



Secure Tunnels

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

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

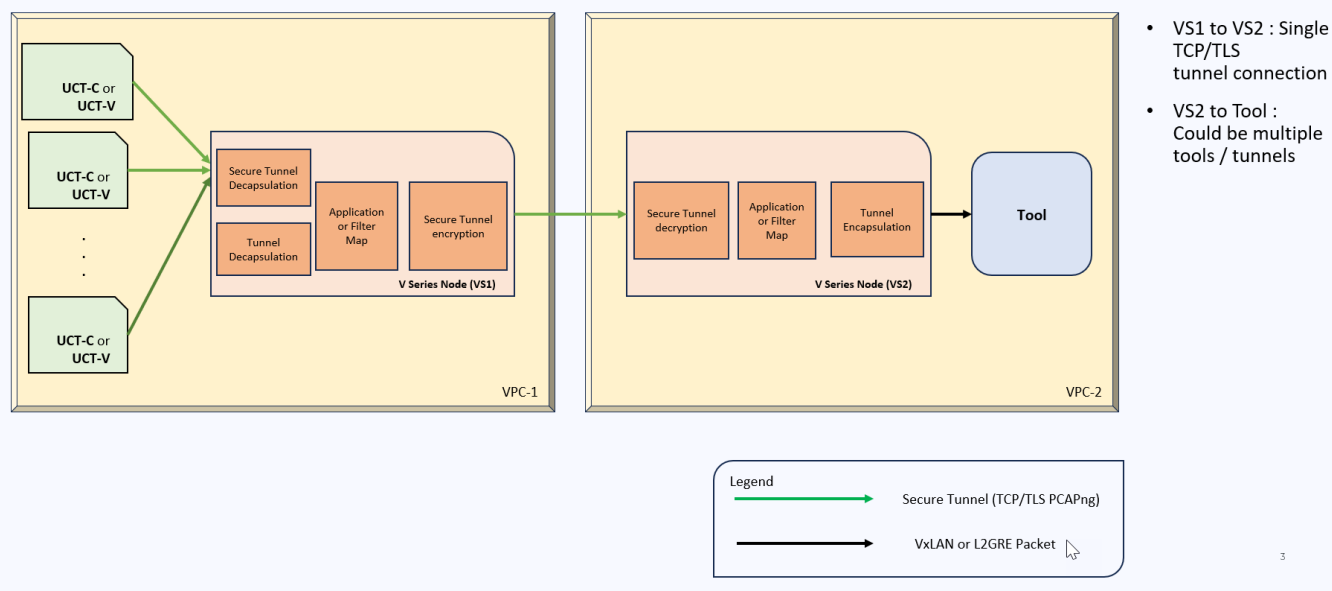
In case of GigaVUE V Series Node to GigaVUE V Series node, the traffic from the GigaVUE V Series Node 1 is encapped using PCAPNG format and transported to GigaVUE V Series Node 2 where the traffic is decapped. The secure tunnels between V Series Node to V Series Node have multiple uses cases.

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

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

Secure Tunnel Use Case

Tool in remote Virtual Private Cloud (VPC) – Single V Series Node



Supported Platforms

Secure tunnel is supported on:

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

For information about how to configure secure tunnels, refer to the section [Configure Secure Tunnel for Third Party Orchestration](#)

Configure Secure Tunnel for Third Party Orchestration

Secure tunnel can be configured on:

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

Precrypted Traffic

You can send the precrypted traffic through secure tunnel. When secure tunnel for precryption is enabled, packets are framed and sent to the TLS socket. PCAPng format is used to send the packet.

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

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

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

Mirrored Traffic

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

Refer to the following sections for Secure Tunnel Configuration:

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

- [Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2](#)

Prerequisites

While creating Secure Tunnel, you must provide the following details:

- SSH key pair
- CA certificate

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

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

S. No	Task	Refer to						
1.	Upload a Custom Authority Certificate (CA)	<p>You must upload a Custom Certificate to UCT-V Controller for establishing a connection with the GigaVUE V Series Node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> 1. Go to Inventory > Resources > Security > CA List. 2. Click New, to add a new Custom Authority. The Add Custom Authority page appears. 3. Enter or select the following information. <table border="1" data-bbox="571 1144 1474 1310"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>Alias name of the CA.</td> </tr> <tr> <td>File Upload</td> <td>Choose the certificate from the desired location.</td> </tr> </tbody> </table> 4. Click Save. <p>For more information, refer to the section Adding Certificate Authority</p>	Field	Action	Alias	Alias name of the CA.	File Upload	Choose the certificate from the desired location.
Field	Action							
Alias	Alias name of the CA.							
File Upload	Choose the certificate from the desired location.							
2.	Upload a SSL Key	<p>You must add a SSL key to GigaVUE V Series Node. To add SSL Key, follow the steps in the section SSL Decrypt.</p>						

S. No	Task	Refer to
3	Enable the secure tunnel	<p>You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE V Series Node. To enable the secure tunnel feature follow these steps:</p> <ol style="list-style-type: none"> 1. In the Edit Monitoring Session page, click Options. The Monitoring Session Options page appears. 2. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and preencrypted traffic.
4.	Select the SSL Key and CA certificate, after deploying the fabric components.	You must select the added SSL Key and CA Authority in GigaVUE V Series Node after creating a monitoring domain configuring the fabric components in GigaVUE-FM. Refer to Edit SSL Configuration for more detailed information on how to select the added SSL Key and CA Authority in GigaVUE V Series Node.

Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2

You can create secure tunnel in the following ways:

- Between GigaVUE V Series Node 1 to GigaVUE V Series Node 2
- From GigaVUE V Series Node 1 to multiple GigaVUE V Series nodes.

You must have the following details before you start the configuration of secure tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2:

- IP address of the tunnel destination endpoint (GigaVUE V Series Node 2).
- SSH key pair (pem file).

To configure secure tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2, refer to the following steps:

S. No	Task	Refer to						
1.	Upload a Certificate Authority (CA) Certificate	<p>You must upload a Custom Certificate to UCT-V Controller for establishing a connection between the GigaVUE V Series Node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> 1. Go to Inventory > Resources > Security > CA List. 2. Click Add, to add a new Certificate Authority. The Add Certificate Authority page appears. 3. Enter or select the following information. <table border="1" data-bbox="712 606 1471 806"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>Alias name of the CA.</td> </tr> <tr> <td>File Upload</td> <td>Choose the certificate from the desired location.</td> </tr> </tbody> </table> 4. Click Save. 5. Click Deploy All. <p>For more information, refer to the section Adding Certificate Authority</p>	Field	Action	Alias	Alias name of the CA.	File Upload	Choose the certificate from the desired location.
Field	Action							
Alias	Alias name of the CA.							
File Upload	Choose the certificate from the desired location.							
2.	Upload a SSL Key	You must add a SSL key to GigaVUE V Series node. To add SSL Key, follow the steps in the section Upload SSL Keys .						
3	Create a secure tunnel between UCT-V and GigaVUE V Series Node 1.	<p>You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE V Series node 1. To enable the secure tunnel feature follow these steps:</p> <ol style="list-style-type: none"> 1. In the Edit Monitoring Session page, click Options. The Monitoring Session Options page appears. 2. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and precrypted traffic. 						
4	Select the SSL Key and CA certificate, after deploying the fabric components.	You must select the added SSL Key and CA Authority in GigaVUE V Series Node after creating a monitoring domain configuring the fabric components in GigaVUE-FM. Refer to Edit SSL Configuration for more detailed information on how to select the added SSL Key and CA Authority in GigaVUE V Series Node.						
5	Create an Egress tunnel from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session.	<p>You must create a tunnel for traffic to flow out from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to Create Ingress and Egress Tunnels for more detailed information on how to create tunnels.</p> <p>To create the egress tunnel, follow these steps:</p> <ol style="list-style-type: none"> 1. After creating a new monitoring session, or click Actions > Edit on an existing monitoring session, the GigaVUE-FM canvas appears. 2. In the canvas, select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick 						

S. No	Task	Refer to														
		<p>view appears.</p> <p>3. On the New Tunnel quick view, enter or select the required information as described in the following table:</p> <table border="1" data-bbox="634 373 1471 1677"> <thead> <tr> <th data-bbox="634 373 821 449">Field</th> <th data-bbox="821 373 1471 449">Action</th> </tr> </thead> <tbody> <tr> <td data-bbox="634 449 821 495">Alias</td> <td data-bbox="821 449 1471 495">The name of the tunnel endpoint.</td> </tr> <tr> <td data-bbox="634 495 821 541">Description</td> <td data-bbox="821 495 1471 541">The description of the tunnel endpoint.</td> </tr> <tr> <td data-bbox="634 541 821 617">Type</td> <td data-bbox="821 541 1471 617">Select TLS-PCAPNG for creating egress secure tunnel</td> </tr> <tr> <td data-bbox="634 617 821 1528">Traffic Direction</td> <td data-bbox="821 617 1471 1528"> Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: <ul style="list-style-type: none"> o MTU- The default value is 1500. o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64. o DSCP - Enter the Differentiated Services Code Point (DSCP) value. o Flow Label - Enter the Flow Label value. o Source L4 Port- Enter the Souce L4 Port value o Destination L4 Port - Enter the Destination L4 Port value. o Flow Label o Cipher- Only SHA 256 is supported. o TLS Version - Select TLS Version1.3. o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments. o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments. </td> </tr> <tr> <td data-bbox="634 1528 821 1604">IP Version</td> <td data-bbox="821 1528 1471 1604">The version of the Internet Protocol. Only IPv4 is supported.</td> </tr> <tr> <td data-bbox="634 1604 821 1677">Remote Tunnel IP</td> <td data-bbox="821 1604 1471 1677">Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).</td> </tr> </tbody> </table> <p>4. Click Save.</p>	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.	Type	Select TLS-PCAPNG for creating egress secure tunnel	Traffic Direction	Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: <ul style="list-style-type: none"> o MTU- The default value is 1500. o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64. o DSCP - Enter the Differentiated Services Code Point (DSCP) value. o Flow Label - Enter the Flow Label value. o Source L4 Port- Enter the Souce L4 Port value o Destination L4 Port - Enter the Destination L4 Port value. o Flow Label o Cipher- Only SHA 256 is supported. o TLS Version - Select TLS Version1.3. o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments. o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments. 	IP Version	The version of the Internet Protocol. Only IPv4 is supported.	Remote Tunnel IP	Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).
Field	Action															
Alias	The name of the tunnel endpoint.															
Description	The description of the tunnel endpoint.															
Type	Select TLS-PCAPNG for creating egress secure tunnel															
Traffic Direction	Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: <ul style="list-style-type: none"> o MTU- The default value is 1500. o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64. o DSCP - Enter the Differentiated Services Code Point (DSCP) value. o Flow Label - Enter the Flow Label value. o Source L4 Port- Enter the Souce L4 Port value o Destination L4 Port - Enter the Destination L4 Port value. o Flow Label o Cipher- Only SHA 256 is supported. o TLS Version - Select TLS Version1.3. o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments. o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments. 															
IP Version	The version of the Internet Protocol. Only IPv4 is supported.															
Remote Tunnel IP	Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).															
6	Select the added SSL Key after deploying the fabric components in GigaVUE V	You must select the added SSL Key in GigaVUE V Series Node 2. Select the GigaVUE V Series Node 2 and follow the steps given in Edit SSL Configuration .														

S. No	Task	Refer to														
	Series Node 2															
7	Create an ingress tunnel in the GigaVUE Node 2 with tunnel type as TLS-PCAPNG while creating the monitoring session for GigaVUE Node 2.	<p>You must create an ingress tunnel for traffic to flow in from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to Create a Monitoring Session to know about monitoring session.</p> <p>To create the ingress tunnel, follow these steps:</p> <ol style="list-style-type: none"> 1. After creating a new monitoring session, or click Actions > Edit on an existing monitoring session, the GigaVUE-FM canvas appears. 2. In the canvas, select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears. 3. On the New Tunnel quick view, enter or select the required information as described in the following table: <table border="1"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>The name of the tunnel endpoint.</td> </tr> <tr> <td>Description</td> <td>The description of the tunnel endpoint.</td> </tr> <tr> <td>Type</td> <td>Select TLS-PCAPNG for creating egress secure tunnel</td> </tr> <tr> <td>Traffic Direction</td> <td>Choose In (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6.</td> </tr> <tr> <td>IP Version</td> <td>The version of the Internet Protocol. Only IPv4 is supported.</td> </tr> <tr> <td>Remote Tunnel IP</td> <td>Enter the interface IP address of the GigaVUE V Series Node 1 (Destination IP).</td> </tr> </tbody> </table> <ol style="list-style-type: none"> 4. Click Save. 	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.	Type	Select TLS-PCAPNG for creating egress secure tunnel	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. Only IPv4 is supported.	Remote Tunnel IP	Enter the interface IP address of the GigaVUE V Series Node 1 (Destination IP).
Field	Action															
Alias	The name of the tunnel endpoint.															
Description	The description of the tunnel endpoint.															
Type	Select TLS-PCAPNG for creating egress secure tunnel															
Traffic Direction	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. Only IPv4 is supported.															
Remote Tunnel IP	Enter the interface IP address of the GigaVUE V Series Node 1 (Destination IP).															

You can also configure Secure Tunnels when using Application Intelligence Session. Refer to [Configure Application Intelligence Solutions on GigaVUE V Series Nodes using Third Party Orchestration](#) for more detailed information on how to enable secure tunnels when using Application Intelligence.

Edit SSL Configuration

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

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

Viewing Status of Secure Tunnel

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

To verify the status of secure tunnel, go to **UCT-C > Monitoring Damain**. In the monitoring domain page, **Tunnel status** column shows the status of the tunnel. The green color represents that the tunnel is connected and the red represents that the tunnel is not connected.

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

Preryption™

License: Requires **SecureVUE Plus** license.

Gigamon Preryption™ technology¹ redefines security for virtual, cloud, and containerized applications, delivering plaintext visibility of encrypted communications to the full security stack, without the traditional cost and complexity of decryption.

This section explains about:

- [How Gigamon Preryption Technology Works](#)
- [Why Gigamon Preryption](#)

Disclaimer: The Preryption feature allows users to acquire traffic after it has been decrypted. This traffic can be acquired from both virtual machine (VM) and container-based solutions, and is then sent to the V Series product for further processing. The Preryption feature provides an option to use encrypted tunnels for communication between the acquisition (via UCT or G-vTAP) of unencrypted traffic and the traffic processing (at the V Series) which will better safeguard the traffic while in transit. However, if a user does not use the option for encrypted tunnels for communication, decrypted traffic will remain unencrypted while in transit between the point of acquisition and processing.

Please note that this information is subject to change, and we encourage you to stay updated on any modifications or improvements made to this feature.

By using this feature, you acknowledge and accept the current limitations and potential risks associated with the transmission of decrypted traffic.

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

How Gigamon Precryption Technology Works

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



In this way, Precryption captures network traffic in plaintext, either before it has been encrypted, or after it has been decrypted. Precryption functionality doesn't interfere with the actual encryption of the message nor its transmission across the network. There's no proxy, no retransmissions, no break-and-inspect. Instead, this plaintext copy is forwarded to the Gigamon Deep Observability Pipeline for further optimization, transformation, replication, and delivery to tools.

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

Why Gigamon Precryption

GigaVUE Universal Cloud Tap with Precryption technology is a lightweight, friction-free solution that eliminates blind spots present in modern hybrid cloud infrastructure, providing East-West visibility into virtual, cloud, and container platforms. It delivers unobscured visibility into all encryption types including TLS 1.3, without managing and maintaining decryption keys. IT organizations can now manage compliance, keep private communications private, architect the necessary foundation for Zero Trust, and boost security tool effectiveness by a factor of 5x or more.

Key Features

The following are the key features of this technology:

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

Key Benefits

The following are the key benefits of this technology:

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

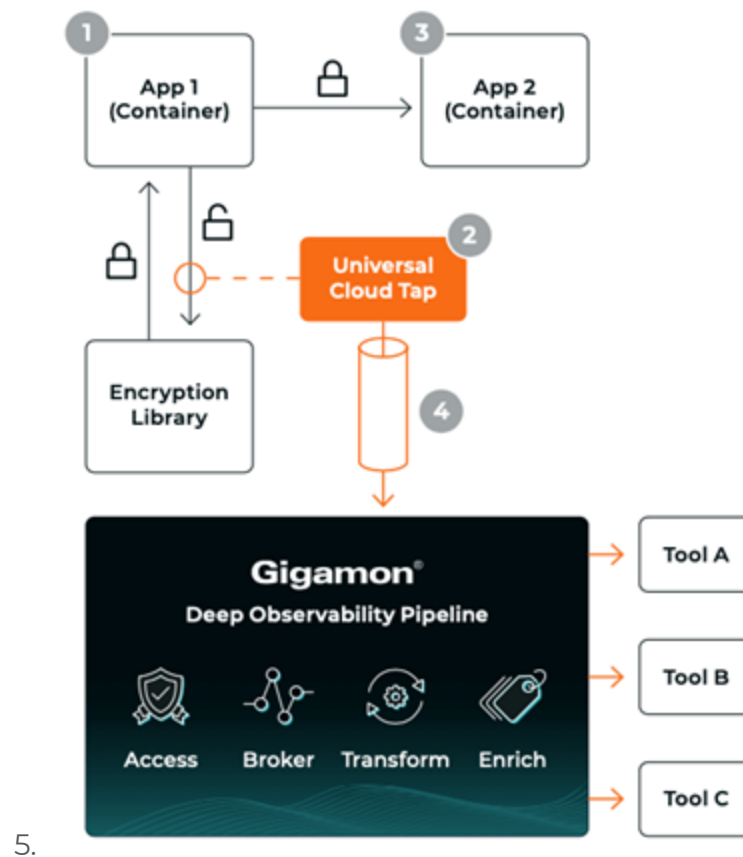
How Gigamon Precryption Technology Works

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

- [Precryption Technology on Single Node](#)
- [Precryption Technology on Multi-Node](#)

Preencryption Technology on Single Node

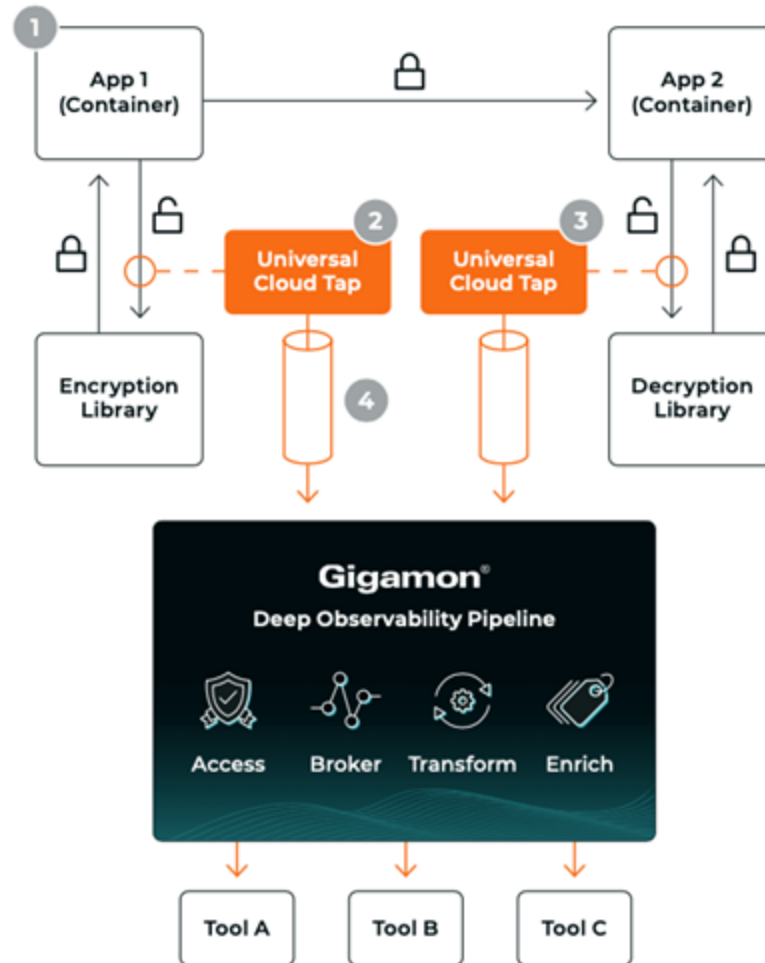
1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Preencryption technology, gets a copy of this message before it's encrypted on the network.
3. The encrypted message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



Preencryption Technology on Multi-Node

1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. . GigaVUE Universal Cloud Tap (UCT), enabled with Preencryption, gets a copy of this message before it's encrypted on the network.

3. Optionally, GigaVUE UCT enabled with Precryption can also acquire a copy of the message from the server end, after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to V Series in the deep observability pipeline where it is further enriched, transformed, and delivered to tools, without further decryption.



5.

Supported Platforms

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

Platform Type	Platform
Public Cloud	<ul style="list-style-type: none"> ● AWS ● Azure ● GCP (via Third Party Orchestration)
Private Cloud	<ul style="list-style-type: none"> ● OpenStack ● VMware ESXi (via Third Party Orchestration only) ● VMware NSX-T (via Third Party Orchestration only)

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

Platform Type	Platform
Public Cloud	<ul style="list-style-type: none"> ● EKS ● AKS
Private Cloud	<ul style="list-style-type: none"> ● OpenShift ● Native Kubernetes (VMware)

Prerequisites

Deployment Prerequisites

- Linux Kernel version 5.4 and above
- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x
- Protocol version IPv4
- For GigaVUE-FM, to capture the statistics, you must add the port 5671 in the security group
- Port 9900 should be enabled in security group settings on the UCT-V controller to receive the statistics information from UCT-V agent
- For UCT-C, you must add the port 42042 and port 5671 in the security group

License Prerequisite

- Precryption™ requires SecureVUE Plus license.

Note

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

Configure Precryption in UCT-V

GigaVUE-FM allows you to enable or disable the Precryption feature for a monitoring session.

To enable or disable the Precryption feature in UCT-V, refer to Create monitoring session.

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

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

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

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

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

Validate Precryption connection

To validate the Precryption connection, follow the steps:

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

Rules and Notes

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

Monitor Cloud Health

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

- [Configuration Health Monitoring](#)
- [Traffic Health Monitoring](#)
- [View Health Status](#)

Configuration Health Monitoring

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

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

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Nutanix

For UCT-Vs:

- AWS
- Azure
- OpenStack

For VPC Mirroring:

- AWS

For OVS Mirroring and VLAN Trunk Port:

- OpenStack

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

Traffic Health Monitoring

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

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

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

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware

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

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

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

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

Create Threshold Template

To create threshold templates:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Then, click on the **Threshold Template** tab in the top navigation bar.
2. The **Threshold Template** page appears. Click **Create** to open the **New Threshold Template** page.
3. Enter the appropriate information for the threshold template as described in the following table.

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

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

Apply Threshold Template

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

Apply Threshold Template to Monitoring Session

To apply the threshold template across a monitoring session, follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds** page appears. To apply a threshold template across a monitoring session, select the template you wish to apply across the monitoring session from the Threshold Template drop-down menu or enter the threshold values manually.
4. Click **Done**.

Apply Threshold Template to Applications

To apply the threshold template to a particular application in the monitoring session follow the steps given below:

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

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

Edit Threshold Template

To edit a particular threshold template follow the steps given below:

1. On the Threshold Template page, Click **Edit**. The **Edit Threshold Template** page appear.
2. The existing threshold templates will be listed here. Edit the templates you wish to modify.
3. Click **Save**.

NOTE: Editing a threshold template does not automatically apply the template to monitoring session. You must apply the edited template to monitoring session for the changes to take effect.

Clear Thresholds

You can clear the thresholds across the entire monitoring session and also to a particular application.

Clear Thresholds for Applications

To clear the thresholds of a particular application in the monitoring session follow the steps given below:

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

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a monitoring session follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds page appears**. Click **Clear**.

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](#)

Supported Resources and Metrics

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

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

	<ul style="list-style-type: none"> 2. Rx Packets 3. Packets Dropped 	<ul style="list-style-type: none"> 2. Derivative 	<ul style="list-style-type: none"> 2. Under
LoadBalancing	<ul style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ul style="list-style-type: none"> 1. Difference 2. Derivative 	<ul style="list-style-type: none"> 1. Over 2. Under
SSLDecryption	<ul style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ul style="list-style-type: none"> 1. Difference 2. Derivative 	<ul style="list-style-type: none"> 1. Over 2. Under
Application Metadata	<ul style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ul style="list-style-type: none"> 1. Difference 2. Derivative 	<ul style="list-style-type: none"> 1. Over 2. Under
AMI Exporter	<ul style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ul style="list-style-type: none"> 1. Difference 2. Derivative 	<ul style="list-style-type: none"> 1. Over 2. Under
Geneve	<ul style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ul style="list-style-type: none"> 1. Difference 2. Derivative 	<ul style="list-style-type: none"> 1. Over 2. Under
5G-SBI	<ul style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 3. Packets Dropped 	<ul style="list-style-type: none"> 1. Difference 2. Derivative 	<ul style="list-style-type: none"> 1. Over 2. Under

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 the Entire Monitoring Session

To view the health status of a monitoring session:

1. On the Monitoring Session details page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed, click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

This displays the configuration health and traffic health of the monitoring session and also the thresholds applied to that monitoring session.

View Health Status of an Application

To view the health status of an application across an entire monitoring session:

1. On the Monitoring Session page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed.
3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **Status** tab.

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

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

View Health Status for Individual V Series Nodes

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

1. On the Monitoring Session page, click on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu and then click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

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, click on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu.
3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **Status** tab.

The subsession toggle button available in the top-left corner of the canvas allows you to view the statistics of individual paths in the monitoring session. If the traffic health is not configured for monitoring session or a particular application, the traffic health is displayed as **Not Applicable**.

You can also view the cloud health Status in the Monitoring Session Page, refer to [View Health Status on the Monitoring Session Page](#) topic for more detailed information on how to view cloud health status in the Monitoring Session page.

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 Third Party Orchestration Settings

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

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

Refresh interval for instance target selection inventory (secs)	120
Refresh interval for fabric deployment inventory (secs)	900
Number of G-vTap Agents per V Series Node	100
Refresh interval for G-vTAP agent inventory (secs)	900

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

Settings	Description
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of the instances.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for deploying the fabric nodes
Number of UCT-Vs per V Series Node	Specifies the maximum number of instances that can be assigned to the GigaVUE V Series node.
Refresh interval for UCT-V inventory (secs)	Specifies the frequency for discovering the UCT-Vs available.
Traffic distribution tunnel range start	Specifies the start range value of the tunnel ID.
Traffic distribution tunnel range end	Specifies the closing range value of the tunnel ID.

Role Based Access Control

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

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

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

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

NOTE: Cloud APIs are also RBAC enabled.

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

GigaVUE-FM Version Compatibility Matrix

The following tables list the different versions of GigaVUE Cloud Suite Cloud solution components available with different versions of GigaVUE-FM.

NOTE: GigaVUE-FM version 6.4 supports the latest fabric components version as well as (n-2) versions. It is always recommended to use the latest version of fabric components with GigaVUE-FM, for better compatibility.

GigaVUE-FM Version Compatibility



The following fabric components are renamed as follows:

- G-vTAP Agents - UCT-V
- Next Generation G-vTAP Agents - Next Generation UCT-V
- G-vTAP Controller - UCT-V Controller

GigaVUE-FM	UCT-V Version	Next Generation UCT-V Version	UCT-V Controller Version	GigaVUE V Series Proxy	GigaVUE V Series Nodes
6.4.00	v6.4.00	v6.4.00	v6.4.00	v6.4.00	v6.4.00

GigaVUE-FM	G-vTAP Agent Version	Next Generation G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Proxy	GigaVUE V Series Nodes
6.3.00	v6.3.00	v6.3.00	v6.3.00	v6.3.00	v6.3.00
6.2.00	v6.2.00	v6.2.00	v6.2.00	v6.2.00	v6.2.00
6.1.00	v6.1.00	N/A	v6.1.00	v6.1.00	v6.1.00

Additional Sources of Information

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

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

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.4 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, rack-mount, 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-HC2 Hardware Installation Guide
	GigaVUE-HC3 Hardware Installation Guide
	GigaVUE-HC1-Plus Hardware Installation Guide
	GigaVUE-TA25 Hardware Installation Guide
	GigaVUE-TA25E Hardware Installation Guide
	GigaVUE-TA100 Hardware Installation Guide

GigaVUE Cloud Suite 6.4 Hardware and Software Guides

GigaVUE-TA200 Hardware Installation Guide

GigaVUE-TA200E Hardware Installation Guide

GigaVUE-TA400 Hardware Installation Guide

GigaVUE-OS Installation Guide for DELL S4112F-ON

G-TAP A Series 2 Installation Guide

GigaVUE M Series Hardware Installation Guide

GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW

Software Installation and Upgrade Guides

GigaVUE-FM Installation, Migration, and Upgrade Guide

GigaVUE-OS Upgrade Guide

GigaVUE V Series Migration Guide

Fabric Management and Administration Guides

GigaVUE Administration Guide

covers both GigaVUE-OS and GigaVUE-FM

GigaVUE Fabric Management Guide

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

Cloud Guides

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

GigaVUE V Series Applications Guide

GigaVUE V Series Quick Start Guide

GigaVUE Cloud Suite Deployment Guide - AWS

GigaVUE Cloud Suite Deployment Guide - Azure

GigaVUE Cloud Suite Deployment Guide - OpenStack

GigaVUE Cloud Suite Deployment Guide - Nutanix

GigaVUE Cloud Suite Deployment Guide - VMware

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

Universal Cloud Tap - Container Deployment Guide

Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite 6.4 Hardware and Software Guides	
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide	
	GigaVUE Cloud Suite Deployment Guide - AWS 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 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)
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 & Docs page on to My Gigamon . Refer to How to Download Software and Release Notes from My Gigamon .
In-Product Help	
GigaVUE-FM Online Help	how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	
For Online Topics	Online doc link	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to 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 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)