



GigaVUE Cloud Suite for AWS - Deployment Guide

GigaVUE Cloud Suite

Product Version: 6.9

Document Version: 1.2

(See Change Notes for document updates.)

Copyright 2025 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.9	1.3	11/20/2025	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.9	1.2	04/04/2025	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.9	1.1	01/18/2025	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.9	1.0	12/06/2024	The original release of this document with 6.9.00 GA.

Contents

GigaVUE Cloud Suite for AWS - Deployment Guide	1
Change Notes	3
Contents	4
Overview of GigaVUE Cloud Suite for AWS	9
GigaVUE-FM	10
UCT-V	11
UCT-V Controller	12
GigaVUE V Series Node	13
GigaVUE V Series Proxy	14
Traffic Acquisition	14
Monitoring Domain	15
Monitoring Session	15
Third Party Orchestration	15
Architecture	16
Cloud Overview Page (AWS)	16
Top Menu	18
Viewing Charts on the Overview Page	19
Viewing Monitoring Session Details	20
Introduction to the Supported Features for AWS	22
Precryption™	22
How Gigamon Precryption Technology Works	23
Why Gigamon Precryption	23
Key Features	24
Key Benefits	24
How Gigamon Precryption Technology Works	24
Supported Platforms	26
Prerequisites	27
Secure Tunnels	28
Prefiltering	30
Prefiltering	31
AWS VPC Traffic Pre-filter	32
Load Balancer	33
Analytics for Virtual Resources	34
Virtual Inventory Statistics and Cloud Applications Dashboard	34
Cloud Health Monitoring	39

Customer Orchestrated Source - Use Case	39
Licensing for GigaVUE Cloud Suite for AWS	40
Purchase GigaVUE Cloud Suite using CPPO	41
Default Trial Licenses	41
Volume Based License (VBL)	42
Base Bundles	43
Add-on Packages	43
How GigaVUE-FM Tracks Volume-Based License Usage	44
Activate Volume-Based Licenses	45
Manage Volume-Based Licenses	45
Prerequisites for AWS	48
Subscribe to GigaVUE Cloud Suite Components	48
Recommended Instance Types for AWS	49
AWS Security Credentials	49
Amazon VPC	49
Subnet for VPC	50
Security Group	50
Key Pair	55
Permissions	55
GigaVUE-FM Version Compatibility	55
Default Login Credentials	56
Points to Note for GigaVUE Cloud Suite for AWS	57
Deployment Options for GigaVUE Cloud Suite for AWS	57
Deploy GigaVUE Fabric Components using AWS	58
Deploy GigaVUE Fabric Components using GigaVUE-FM	58
Traffic Acquisition Method as UCT-V	59
Traffic Acquisition Method as Traffic Mirroring	59
Traffic Acquisition Method as Customer Orchestrated Source	60
Deploy GigaVUE Cloud Suite for AWS	61
Permissions and Privileges (AWS)	62
Minimum Permissions Required for Inline Policies and Basic Authentication	62
GigaVUE-FM Instance Multi Account Support Using Amazon STS	64
Minimum Permissions Required for Acquiring Traffic using the UCT-V	65
Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source	67
Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with GwLB	68
Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with NwLB	69
Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring	70
Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring with Network Load Balancer	72

Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring and GwLB	73
Install GigaVUE-FM on AWS	75
Subscribe to GigaVUE-FM	75
Initial Configuration	76
Install Custom Certificate on AWS	78
Adding Certificate Authority	79
Create AWS Credentials	80
Create a Monitoring Domain	82
Check Permissions while Creating a Monitoring Domain	84
Managing Monitoring Domain	88
Configure GigaVUE Fabric Components in GigaVUE-FM	92
Configure UCT-V Controller	93
Configure GigaVUE V Series Proxy	95
Configure GigaVUE V Series Node	96
Configure Role-Based Access for Third Party Orchestration	97
Role-Based Access for Third Party Orchestration	98
Role	98
User Groups	99
Users	101
Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode	103
Configure GigaVUE V Series Nodes and V Series Proxy in AWS	103
Configure UCT-V Controller in AWS	106
Configure UCT-V in AWS	112
Install UCT-V	114
Supported Operating Systems for UCT-V	114
Linux UCT-V Installation	115
Windows UCT-V Installation	125
Uninstall UCT-V	132
Upgrade or Reinstall UCT-V	132
Upgrade UCT-V manually on Virtual Machine	132
Upgrade UCT-V through GigaVUE-FM	133
Configure Secure Tunnel (AWS)	135
Precrypted Traffic	136
Mirrored Traffic	136
Prerequisites	136
Notes	136
Configure Secure Tunnel from UCT-V to GigaVUE V Series Node	137
Configure Secure Tunnel between GigaVUE V Series Nodes	138
Viewing Status of Secure Tunnel	142

Create Prefiltering Policy Template	143
Create Precryption Template for UCT-V	144
Rules and Notes:	144
Create Precryption Template for Filtering based on Applications	145
Create Precryption Template for Filtering based on L3-L4 details	145
Configure Monitoring Session	147
Create a Monitoring Session (AWS)	147
Monitoring Session Page (AWS)	148
Configure Monitoring Session Options (AWS)	149
Create Ingress and Egress Tunnels (AWS)	153
Create Raw Endpoint (AWS)	159
Create a New Map (AWS)	160
Example- Create a New Map using Inclusion and Exclusion Maps	165
Map Library	165
Add Applications to Monitoring Session (AWS)	166
Interface Mapping (AWS)	166
Deploy Monitoring Session (AWS)	167
View Monitoring Session Statistics (AWS)	168
Visualize the Network Topology (AWS)	169
Migrate Application Intelligence Session to Monitoring Session ..	170
Post Migration Notes for Application Intelligence	172
Configure AWS Elastic Load Balancing	175
AWS Network Load Balancer	176
Architecture	177
Configure Network Load Balancer	178
Deploy Visibility Fabric with Network Load Balancer	181
AWS Gateway Load Balancer	183
Architecture	184
Configure a Gateway Load Balancer	185
Deploy Visibility Fabric with Gateway Load Balancer	188
Check for Required IAM Permissions	189
Upgrade GigaVUE-FM in AWS	190
At a Glance	191
Stop GigaVUE-FM Instance	192
Create Snapshot of the GigaVUE-FM Instance	193
Upgrade GigaVUE-FM Instance	194
Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS	196
Prerequisite	196
Upgrade UCT-V Controller	196
Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy	197

Monitor Cloud Health	200
Configuration Health Monitoring	200
Traffic Health Monitoring	200
Supported Resources and Metrics	201
Create Threshold Templates	203
Apply Threshold Template	204
Clear Thresholds	205
View Health Status	205
Administer GigaVUE Cloud Suite for AWS	207
Configure AWS Settings	208
Configure Proxy Server	210
Role Based Access Control	212
About Events	214
About Audit Logs	216
Glossary	218
Additional Sources of Information	219
Documentation	219
How to Download Software and Release Notes from My Gigamon	221
Documentation Feedback	222
Contact Technical Support	223
Contact Sales	223
Premium Support	223
The VÜE Community	224
Glossary	225

Overview of GigaVUE Cloud Suite for AWS

GigaVUE Cloud Suite for AWS delivers a cloud-based visibility and analytics solution that eliminates network blind spots as you move workloads to the cloud, significantly reducing security and non-compliance risks and helps remediate performance issues.

GigaVUE Cloud Suite for AWS helps you obtain a unified view of all data in motion anywhere on your hybrid, single or multi-cloud network. Easily acquire data from any source, automatically optimize it and send to any destination. It closes the cloud visibility gap, giving your security and monitoring tools visibility across cloud environments, from raw packets up to the application layer and with the added context of network data.

You can deploy the GigaVUE Cloud Suite for AWS using one of the following two options:

- [Subscribe to it in the AWS marketplace](#)
- [Install the individual fabric components using the Amazon Machine Images \(AMI\).](#)

NOTE: You must subscribe to each component individually.

Refer to the following sections for details:

- [GigaVUE-FM](#)
- [UCT-V](#)
- [UCT-V Controller](#)
- [GigaVUE V Series Node](#)
- [GigaVUE V Series Proxy](#)
- [Traffic Acquisition](#)
- [Monitoring Domain](#)
- [Monitoring Session](#)
- [Third Party Orchestration](#)

GigaVUE-FM

GigaVUE-FM gives you unified access, centralized control, and full visibility into all GigaVUE traffic nodes across your enterprise or data center. It offers a global view that individual nodes cannot provide.

Along with management and monitoring, GigaVUE-FM lets you create and manage traffic policies for your visibility fabric. This helps direct network traffic to your monitoring and analytics tools.

You can install GigaVUE-FM on a range of supported platforms. It also works in any supported cloud environment, as long as there is IP connectivity.

You can deploy GigaVUE-FM on-premises as a physical or virtual appliance, or launch it from an Amazon Machine Image (AMI) in the AWS Marketplace.

GigaVUE-FM in AWS

GigaVUE-FM manages the setup of key components in your Amazon Virtual Private Cloud (VPC), including:

- UCT-V Controller (Only if you are using UCT-V as the traffic acquisition method)
- GigaVUE V Series[®] Node
- GigaVUE V Series[®] Proxy (Optional)

GigaVUE-FM Orchestration Capabilities

GigaVUE-FM controls the GigaVUE Cloud Suite for AWS.

It helps you:

- Define monitoring areas in your network where workloads run.
- Provide credentials so GigaVUE-FM can discover workloads and related resources.
- Create and deploy visibility policies (Monitoring Sessions) that collect traffic using your chosen method and send it to GigaVUE V Series Nodes.
- Configure V Series Nodes to process and forward traffic to tools based on your policy rules.
- Monitor network areas continuously and automatically apply visibility policies to new workloads if they meet the criteria.
- Gain full visibility into your AWS environment, optimize tool traffic, and keep security consistent across hybrid and multi-cloud setups.

For detailed steps on installing GigaVUE-FM in AWS, refer to [Install GigaVUE-FM on AWS](#).

UCT-V

Universal Cloud Tap - Virtual Machine (UCT-V), formerly known as the G-vTAP Agent, is a standalone service that installs on a VM instance. UCT-V mirrors selected traffic from virtual machines to the GigaVUE V Series Node. UCT-V is available as:

- Debian (.deb) package
- Red Hat Package Manager (.rpm) package
- ZIP file
- MSI installer

Next-Generation UCT-V

The next-generation UCT-V is a lightweight solution that improves traffic acquisition and mirroring performance. It includes prefiltering at the tap level that:

- Reduces traffic flow from UCT-V to the GigaVUE V Series Node
- Lowers the load on the GigaVUE V Series Node
- Improves overall efficiency

This version supports both Windows and Linux systems running Kernel 4.18 or later.

Benefits of Prefiltering

Prefiltering allows you to cut costs by filtering traffic at the UCT-V before it reaches the GigaVUE V Series Node. Using GigaVUE-FM, you can:

- Create prefiltering policy templates
- Apply templates to monitoring sessions
- Control which traffic is mirrored for analysis

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

UCT-V Controller

UCT-V Controller (earlier known as G-vTAP Controller) manages multiple UCT-Vs and, proxied through GigaVUE-FM, orchestrates the flow of mirrored traffic to GigaVUE V Series Nodes.

GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs. A single UCT-V Controller can only manage UCT-Vs that run the same version. For example, the UCT-V Controller 6.9.00 can only manage UCT-Vs 6.9.00.

If you still have the older version of UCT-V deployed in the EC2 instances, you must configure both the previous version and 6.9.00. While configuring the UCT-V Controllers, you can specify the tunnel type used to carry the mirrored traffic from the UCT-Vs to the GigaVUE V Series Nodes.

GigaVUE V Series Node

GigaVUE® V Series Node is a visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to on-premises devices or tools. GigaVUE Cloud Suite for AWS uses the following tunnels to deliver traffic to tool endpoints:

- TLS-PCAPNG
- ERSPAN
- L2GRE
- UDPGRE
- VXLAN

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

GigaVUE V Series Proxy

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

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

Traffic Acquisition

You can acquire traffic from multiple virtual machines and container pod instances using UCT-V or AWS infrastructure sources such as Traffic Mirroring. The acquired traffic is forwarded to the GigaVUE V Series Node to conduct core intelligence and additional GigaSMART processing.

You can acquire traffic using any of the following ways:

- UCT-V
- Traffic Mirroring
- Customer Orchestrated source

For details, refer to [Deployment Options for GigaVUE Cloud Suite for AWS](#).

Monitoring Domain

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

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

Monitoring Session

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

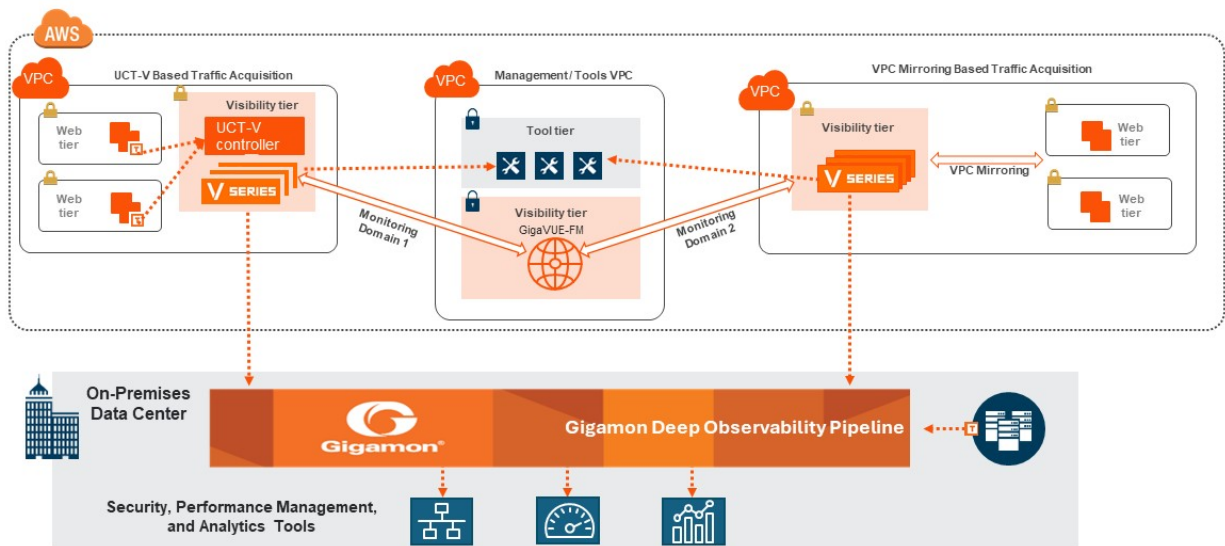
When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance to your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions.

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

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 choice of orchestration system such as terraform or scripts. These fabric components register themselves with GigaVUE-FM using the information the user provides. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

Architecture



The architecture diagram depicts various fabric components deployed in multiple VPC. Lightweight UCT-V are deployed across instances, serving as a conduit for traffic mirroring. This mirrored traffic is then transmitted to the GigaVUE V Series.

In addition to UCT-V based mirroring, you can mirror the traffic using Traffic Mirroring to further acquire traffic. The acquired traffic is subsequently processed by GigaVUE V Series Nodes. GigaVUE V Series Nodes perform functions like aggregation, selection, optimization, de-duplication, and distribution of traffic. You can perform operations such as Slicing, Sampling, and Masking for the selected traffic using GigaSMART®.

GigaVUE-FM facilitates a Centralized orchestration. GigaVUE-FM provides a single-pane-of-glass visualization, enabling administrators to oversee and manage the entire visibility infrastructure seamlessly. It helps in auto-discovery and end-to-end topology visualization, streamlining the deployment and maintenance of the visibility solution while offering comprehensive insights into network operations.

Cloud Overview Page (AWS)

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

This page shows key information at a glance, including:

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

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

How to Access the Overview Page

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

Perform one of the following:

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

The Monitoring Sessions page appears.

The screenshot shows the 'Monitoring Sessions' dashboard. At the top, there are filters for Platform (All) and Monitoring Domains (All), along with buttons for New, Actions, and Filter (labeled 1). Below this is an overview section with four cards: Overview (4/4 V Series Nodes, 2 Monitoring Sessions, 2/2 Connections, 0 V Series Alarms), V Series Alarms (No Data), Connection Status (100% Connected), and Usage (0 GB). Below the overview is an Aggregate Summary section showing 0 Bytes for highest and average daily usage, and 1 TB for average daily allowance (labeled 2). At the bottom is a table of monitoring sessions (labeled 3).

MONITORING SE...	STATUS	MONITORING DO...	PLATFORM	CONNECTIONS	TUNNELS	NODE HEALTH	DEPLOYMENT ST...	THRESHOLDS AP...	PREFILTERING	PRECRIPTION	APPS LOG
UCTV-MS	Healthy	UCTV-MD	OpenStack	UCTV-MD	Egress_Tunnel(2 of 2 are Health	Success	No	No	No	No
OVS-MS	Healthy	OVS-MD	OpenStack	OIVS-MD	Egress_Tunnel(e	2 of 2 are Health	Success	No	No	No	No

Page Layout for Easy Use

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

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

Top Menu

The Top menu consists of the following options:

Options	Description
New	Allows to create a new Monitoring Session and new Monitoring Domain.
Actions	Allows the following actions: <ul style="list-style-type: none"> • Edit: Opens the edit page for the selected Monitoring Session. • Delete: Deletes the selected Monitoring Session. • Clone: Duplicates the selected Monitoring Session. • Deploy: Deploys the selected Monitoring Session. • Undeploy: Undeploys the selected Monitoring Session. • Apply Threshold: Applies the threshold template created for monitoring cloud traffic health. For details, refer to the <i>Monitor Cloud</i> section. • Apply Policy: Enables functions like Precryption, Prefiltering, or Secure Tunnel.
Filter	You can filter the Monitoring Session details based on a criterion or a combination of criteria. For more information, refer to Cloud Overview Page (AWS) .


Filters

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

- [Filter on the left corner](#)
- [Filter on the right corner](#)

Filter on the left corner



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

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

Filter on the right corner

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

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

Viewing Charts on the Overview Page

You can view the following charts on the overview page:

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

Overview

This chart shows:

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

V Series Alarms

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

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

Connection Status

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

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

Usage

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

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

Aggregate Summary

This summary shows key volume usage stats:


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

Viewing Monitoring Session Details

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

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

Details	Description
Deployment Status	Displays the status of the deployment.
Threshold Applied	Specifies if the threshold is applied.
Prefiltering	Specifies if Prefiltering is configured.
Preencryption	Specifies if Preencryption is configured.
APPS logging	Specifies if APPS logging is configured.
Traffic Mirroring	Specifies if Traffic Mirroring is configured.

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

Introduction to the Supported Features for AWS

GigaVUE Cloud Suite for AWS supports the following features:

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

Precryption™

License: Requires **SecureVUE Plus** license.

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

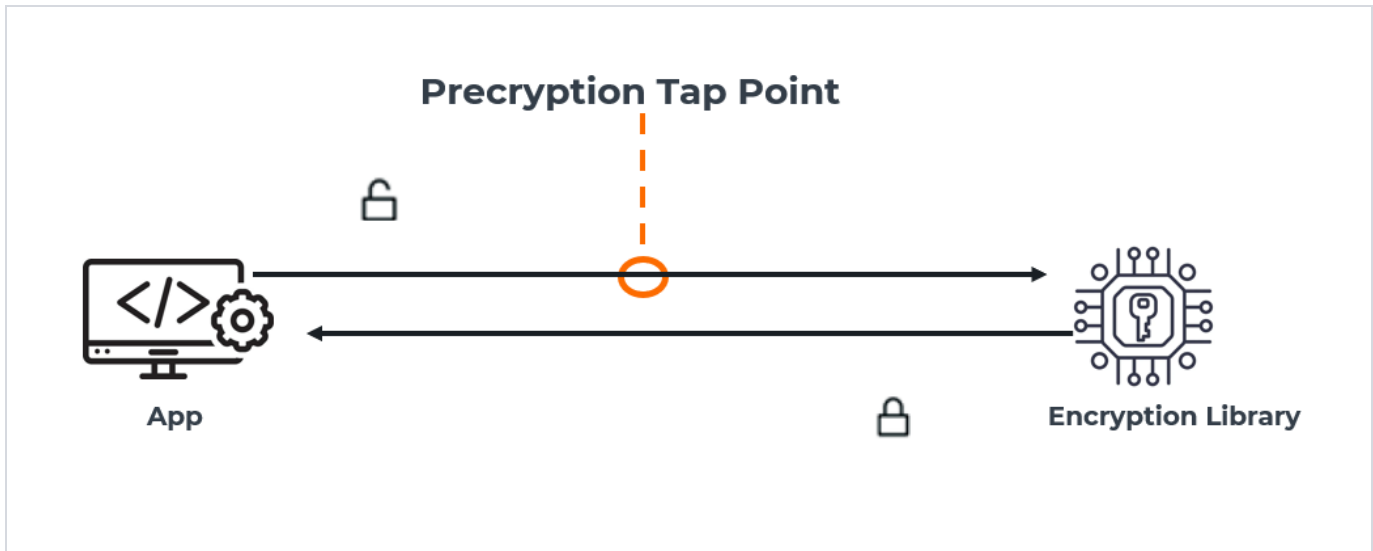
This section explains:

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

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

How Gigamon Precryption Technology Works

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



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

Precryption technology is built on GigaVUE® Universal Cloud Tap (UCT) and works across hybrid and multi-cloud environments, including on-prem and virtual platforms. Moreover, UCT with Precryption technology operates independently of the application and does not need to be integrated into the application development lifecycle.

Why Gigamon Precryption

GigaVUE Universal Cloud Tap with Precryption technology is a lightweight, friction-free solution that eliminates blind spots present in modern hybrid cloud infrastructure. It provides comprehensive visibility into East-West and North-South traffic across virtual, cloud, and container platforms. As long as a packet interacts with the Virtual Machine, it is mirrored, ensuring complete traffic capture. This solution delivers unobscured visibility into all encryption types, including TLS 1.3, without the need to manage and maintain decryption keys. With these capabilities, IT organizations can manage compliance, maintain the privacy of communications, establish a robust foundation for Zero Trust, and enhance security tool effectiveness by a factor of 5x or more.

Key Features

The following are the key features of this technology:

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

Key Benefits

The following are the key benefits of this technology:

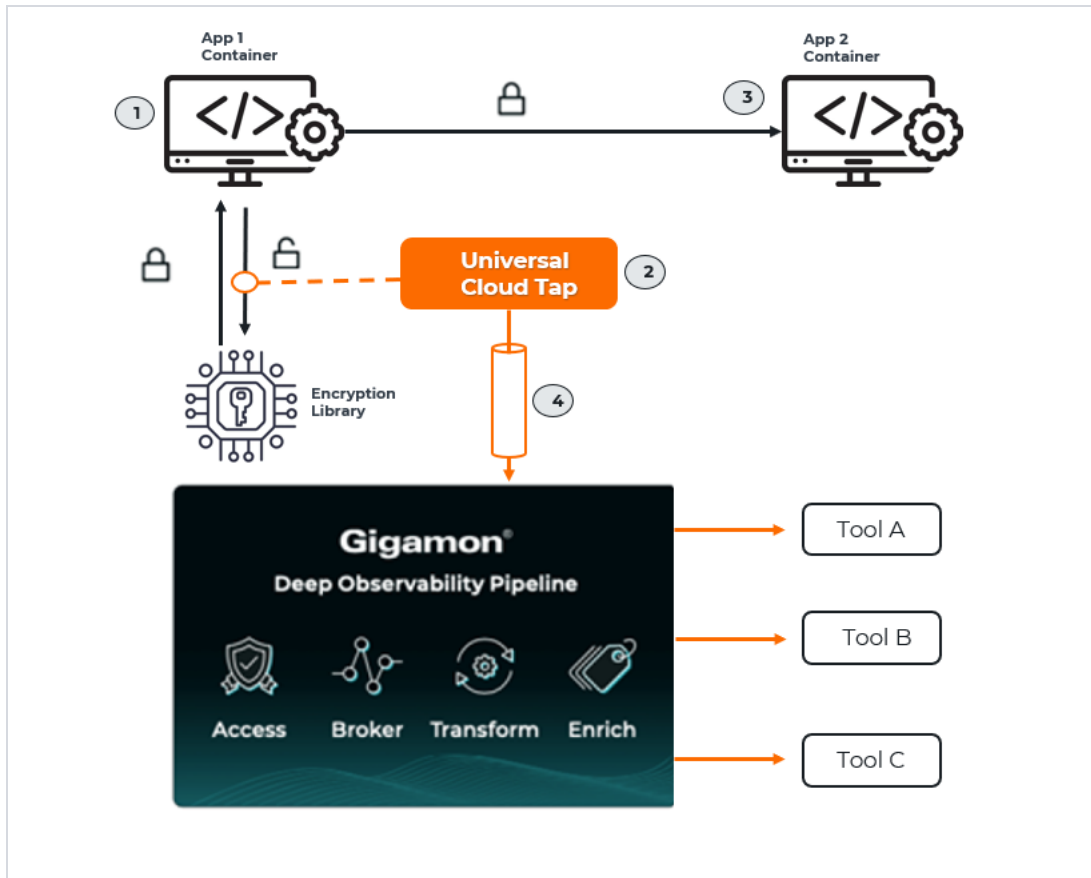
- Eliminate blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.
- Monitor application communications with an independent approach that enhances development team velocity.
- Extend security tools' visibility to all communications,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

How Gigamon Precryption Technology Works

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

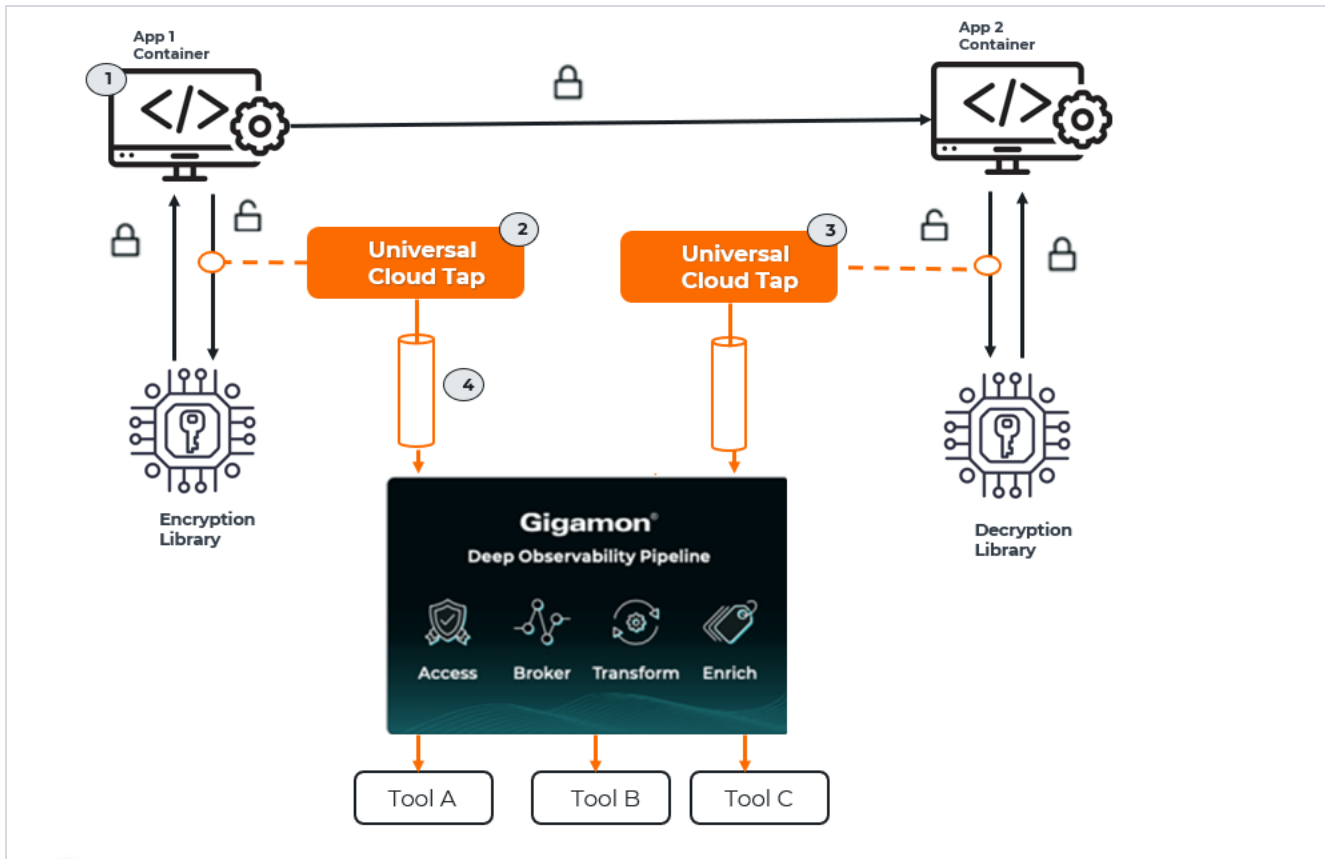
- [Precryption Technology on Single Node](#)
- [Precryption Technology on Multi-Node](#)

Pre-encryption 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 Pre-encryption technology, gets a copy of this message before it's encrypted on the network.
3. The encrypted message is sent to the receiving application with unmodified encryption—no proxy, no re-encryption, no retransmissions.
4. GigaVUE UCT creates packet headers as needed, encapsulates them in a tunnel, and forwards them to GigaVUE V Series in the deep observability pipeline. Gigamon optimizes, transforms, and delivers data to tools without further decryption.

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 Preencryption can also acquire a copy of the message from the server end after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates them in a tunnel, and forwards them to V Series in the deep observability pipeline. There, they are further enriched, transformed, and delivered to tools without further decryption.

Supported Platforms

VM environments: Preencryption™ 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) • Nutanix (via Third Party Orchestration only)

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

Platform Type	Platform
Public Cloud	<ul style="list-style-type: none"> • EKS • AKS
Private Cloud	<ul style="list-style-type: none"> • OpenShift • Native Kubernetes (VMware)

Prerequisites

Deployment Prerequisites

- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x.
- For UCT-C, worker pods should always have libssl installed to ensure that UCT-C Tap can tap the precrypted packets from the worker pods whenever libssl calls are made from the worker pods.
- For GigaVUE-FM, you must add port 5671 in the security group to capture the statistics.
- Port 9900 should be enabled in security group settings on the UCT-V Controller to receive the statistics information from UCT-V.
- For UCT-C, you must add port 42042 and port 5671 to the security group.

License Prerequisite

- Precryption™ requires a SecureVUE Plus license.

Supported Kernel Version

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

Kernel-Version	Operating System
4.18.0-193.el8.x86_64	RHEL release 8.2 (Ootpa)
4.18.0-240.el8.x86_64	RHEL release 8.3 (Ootpa)

Kernel-Version	Operating System
4.18.0-305.76.1.el8_4.x86_64	RHEL release 8.4 (Ootpa)
4.18.0-348.12.2.el8_5.x86_64	RHEL release 8.5 (Ootpa)
4.18.0-372.9.1.el8.x86_64	RHEL release 8.6 (Ootpa)
4.18.0-423.el8.x86_64	RHEL release 8.7 Beta (Ootpa)
4.18.0-477.15.1.el8_8.x86_64	RHEL release 8.8 (Ootpa)
5.3.0-1024-kvm	ubuntu19.10
4.18.0-305.3.1	Rocky Linux 8.4
4.18.0-348	Rocky Linux 8.5
4.18.0-372.9.1	Rocky Linux 8.6
4.18.0-425.10.1	Rocky Linux 8.7
4.18.0-477.10.1	Rocky Linux 8.8
4.18.0-80.el8.x86_64	centos 8.2
4.18.0-240.1.1.el8_3.x86_64	centos 8.3
4.18.0-305.3.1.el8_4.x86_64	centos 8.4
4.18.0-408.el8.x86_64	centos 8.5

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 in the Universal Cloud TAP - Container Deployment Guide for details on how to enable Precryption™ in container environments.
- See how [Secure Tunnels](#) feature can enable secure delivery of precrypted data.

Secure Tunnels

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

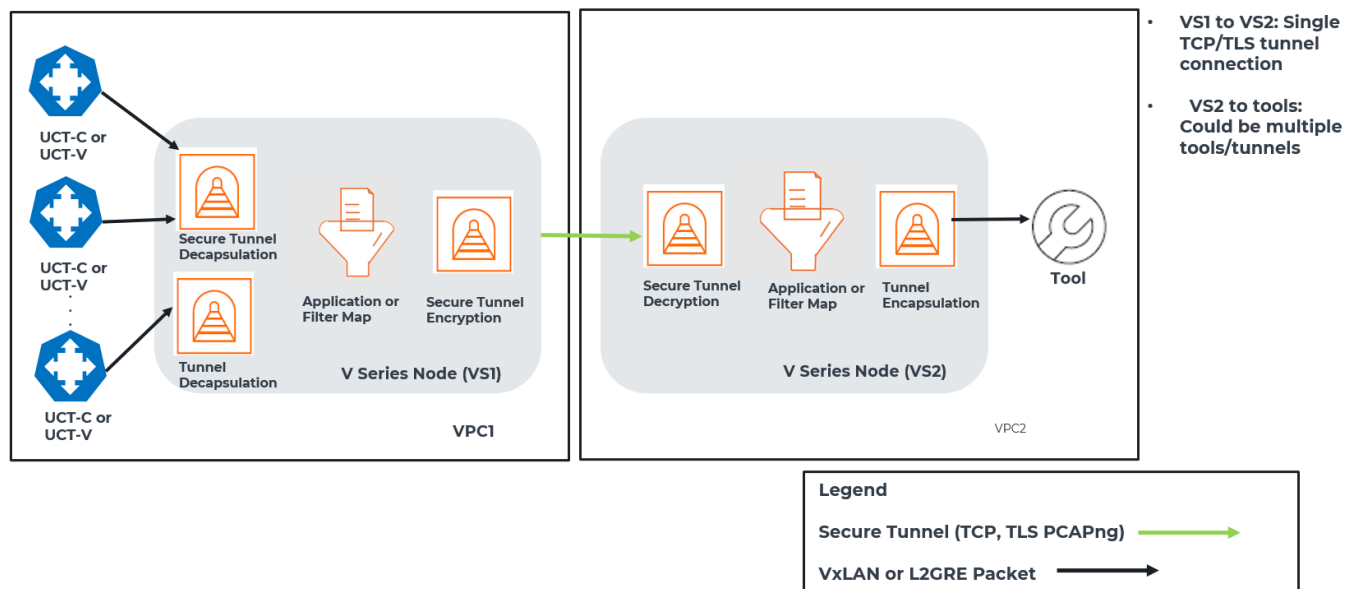
When sending traffic between two V Series Nodes, the source node captures and encapsulates the packets in PCAPng format. It then sends them to the destination V Series Node that decapsulates and processes the traffic based on your configuration.

How Does it Work!

- Forward packets from one V Series Node to another for further analysis.
- Apply processing features such as de-duplication, application intelligence, or load balancing.
- Use the built-in load balancer to distribute traffic across multiple V Series Nodes.

- If the load balancer sends packets to another node, it can re-encapsulate them and send them over another secure tunnel.

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



Supported Platforms

Secure 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 \(AWS\)](#).

Prefiltering

Prefiltering allows you to filter the traffic before sending it to the GigaVUE V Series Node. Depending on your deployment type, you can perform prefiltering in one of the following methods:

- [Prefiltering](#)
- [AWS VPC Traffic Pre-filter](#)

For more information on configuring a prefilter, refer to [Create a Monitoring Session \(AWS\)](#).

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. You can apply an existing policy template 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.

Points to Remember for prefiltering in Next Generation UCT-Vs are:

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

For more information on configuring a prefilter, refer to [Create a Monitoring Session \(AWS\)](#).

AWS VPC Traffic Pre-filter

When you create a Monitoring Session, GigaVUE-FM creates a traffic mirror filter with a "Pass All" rule and associates it with the traffic mirroring session. The Pass All filter forwards all the traffic without filtering.

If you want to filter the traffic, then you can create a traffic mirror filter on AWS and add rules to determine the traffic that is mirrored. This traffic mirror filter acts as a pre-filter and pass only the filtered traffic to the GigaVUE V Series Nodes.

To apply the filter to the traffic mirror session that is created by the FM, you must add the tag "in_use_by_gigamon" to the traffic mirror filter. The GigaVUE-FM collects all the traffic mirror filters that has the tag "in_use_by_gigamon". It then applies these filters on the traffic mirror sessions to replace the default Pass All filter.

In addition to "in_use_by_gigamon" tag, you can add the tag "vpcs" to apply specific VPCs. The tag value is a list of vpc separated by comma ",".

You can apply filters at two levels. The two level filters can work together. The VPC level filter overrides the Account level filter for the VPC defined in VPC level filter.

1. Account level: You can define a filter (only one filter) which applies on every VPC in an account. The filter should be tagged with "in_use_by_gigamon" only. The "vpcs" tag should not be used.
2. VPC level: To filter the traffic at VPC level, in addition to the tag "in_use_by_gigamon" , add the tag "vpcs" .

Tags - optional
 A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="in_use_by_gigamon"/> ✕	<input type="text" value="Enter value"/> Remove
<input type="text" value="vpcs"/> ✕	<input type="text" value="vpc-94372df0,vpc-0661a4db9f738700a,vpc-05469543577a2507d"/> ✕ Remove
<input type="button" value="Add new tag"/>	

NOTE: A filter can be defined for multiple VPCs. Two filters should not have intersection on VPC. If there is an intersection on VPC, then the GigaVUE-FM will pick a random filter and no error will be displayed.

For more information on creating a traffic mirror, refer to the [AWS documentation](#).

Load Balancer

You can use a load balancer to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series nodes. The load balancer distributes the traffic to the GigaVUE V Series Nodes and the GigaVUE-FM auto-scales the GigaVUE V Series Nodes based on the traffic.

Supported load balancers:

- [Elastic Load Balancer](#)
- [Gateway Load Balancer](#)

Analytics for Virtual Resources

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


Rules and Notes:

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

Virtual Inventory Statistics and Cloud Applications Dashboard

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

To access the dashboards:

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

The following table lists the various virtual dashboards:

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

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

Dashboard	Displays	Visualizations	Displays
		<i>V Series Network Interfaces with Most Rx for Past 5 mins</i>	Total packets received by each of the V Series network interface for the past 5 minutes. NOTE: You cannot use the time based filter options to filter and visualize the data.
		<i>V Series Node Tunnel Rx Packets/Errors</i>	Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation.
		<i>V Series Node Tunnel Tx Packets/Errors</i>	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: <ul style="list-style-type: none"> Platform Connection V Series Node 	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload.
		<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the de-duplicated packets received against the de-duplication application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get updated:	<i>Tunnel Bytes</i>	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes. <ul style="list-style-type: none"> For input tunnel, transmitted traffic is displayed as zero. For output tunnel, received traffic is displayed as zero.

Dashboard	Displays	Visualizations	Displays
	<ul style="list-style-type: none"> • Monitoring session: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V Series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. • V Series node: Management IP of the V Series node. Choose the required V Series node from the drop-down. • Tunnel: Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. <p>The following statistics are displayed for the tunnel:</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets 	<p><i>Tunnel Packets</i></p>	<p>Displays packet-level statistics for input and output tunnels that are part of a monitoring session.</p>
App (Virtual)	<p>Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V Series node.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session • V Series node • Application: Select the required application. By default, the visualizations displayed includes all the applications. <p>By default, the following statistics are displayed:</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes 	<i>App Bytes</i>	<p>Displays received traffic vs transmitted traffic, in Bytes.</p>

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

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

Cloud Health Monitoring

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

For more information on how to configure cloud health monitoring, refer to the topic [Monitor Cloud Health](#).

Customer Orchestrated Source - Use Case

Customer Orchestrated Source is a traffic acquisition method that allows to tunnel traffic directly to the GigaVUE V Series Nodes. In cases where UCT-V or Traffic Mirroring firewall or other restrictions prevent configurations, you can use this method and tunnel the traffic to GigaVUE V Series Node, where the traffic is processed.

When using Customer Orchestrated Source, you can directly configure tunnels or raw endpoints in the monitoring session, where you can use other applications like Slicing, Masking, Application Metadata, Application Filtering, and so on, to process the tunneled traffic. For details on how to configure Tunnels and Raw End Points in the Monitoring Session, refer to [Create Ingress and Egress Tunnels \(AWS\)](#) and [Create Raw Endpoint \(AWS\)](#).

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

Licensing for GigaVUE Cloud Suite for AWS

You can license the GigaVUE Cloud Suite for AWS using one of the following methods:

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

Upon installing GigaVUE-FM, you receive a complimentary 30-day SecureVUE Plus trial Volume-Based License (VBL) with a 1TB capacity, valid from the installation date. For details on the applications supported with this license, refer to [Default Trial Licenses](#).

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

Purchase GigaVUE Cloud Suite using CPPO

GigaVUE Cloud Suite is available as an Amazon Machine Image (AMI) product within the AWS Marketplace. GigaVUE Cloud Suite purchased through the AWS Marketplace with Channel Partner Private Offers (CPPO) comes with a Volume-Based License.

The list of SKUs¹, available on the AWS Marketplace through the Channel Partner Private Offers (CPPO) are:

- VBL-250T-BN-SVP
- VBL-50T-BN-SVP
- VBL-2500T-BN-NV

For detailed information on VBL and the available add-on packages, refer to Volume Based License (VBL).

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

Default Trial Licenses

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

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

This license includes the following applications:

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

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

NOTE: If you do not have any other Volume-Based Licenses installed, the deployed monitoring sessions are undeployed from the existing GigaVUE V Series Nodes after 30 days at the expiration of the trial license.

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

Volume Based License (VBL)

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

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

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

Related Information

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

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUEPlus

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

Bundle Replacement Policy

Refer to the following notes:

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

Add-on Packages

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

The following add-on SKUs are available:

- VBL-50T-ADD-5GC
- VBL-250T-ADD-5GC

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

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

Rules for add-on packages:

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

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

- [GigaVUE Cloud Suite for VMware Data Sheet](#)
- [GigaVUE Cloud Suite for AWS Data Sheet](#)
- [GigaVUE Cloud Suite for Azure Data Sheet](#)
- [GigaVUE Cloud Suite for OpenStack](#)
- [GigaVUE Cloud Suite for Nutanix](#)
- [GigaVUE Cloud Suite for Kubernetes](#)

How GigaVUE-FM Tracks Volume-Based License Usage


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

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

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

Activate Volume-Based Licenses

To activate Volume-Based Licenses,


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

Manage Volume-Based Licenses

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

View active Volume-Based License

To view active Volume-Based License (VBL):

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


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

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

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

View Inactive Volume-Based License

To view inactive Volume-Based License (VBL):

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

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

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

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

Use the following buttons to manage your VBL.

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

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

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

Prerequisites for AWS

Refer to the following topics for details:

- [Subscribe to GigaVUE Cloud Suite Components](#)
- [Recommended Instance Types for AWS](#)
- [AWS Security Credentials](#)
- [Amazon VPC](#)
- [Permissions](#)
- [GigaVUE-FM Version Compatibility](#)
- [Default Login Credentials](#)

Subscribe to GigaVUE Cloud Suite Components

To deploy the GigaVUE Cloud Suite for AWS from the AWS Marketplace, you can subscribe to the following GigaVUE Cloud Suite components.

- GigaVUE V Series Node
- GigaVUE V Series Proxy
- GigaVUE V Series Controller
- GigaVUE-FM BYOL
- GigaVUE Cloud Suite BYOL

Note: You will not be charged for subscribing to these components.

To subscribe to the GigaVUE components, perform the following steps:

1. Log in to your AWS account.
2. Go to <https://aws.amazon.com/marketplace/>.
3. In the **Search** field, type Gigamon and click Search.
4. Select the latest GigaVUE Cloud Suite version link from the list for Gigamon products.
5. Select **Continue to Subscribe**.

Recommended Instance Types for AWS

Product	Instance Type	vCPU	RAM
GigaVUE-FM	m5.xlarge	4 vCPU	16GB
GigaVUE V Series Node	c5n.xlarge (AMD)	4 vCPU	10.5GB
	c7gn.xlarge (ARM)	4 vCPU	8GB
GigaVUE V Series Proxy	t2.medium (AMD)	2 vCPU	4GB
	t4g.micro (ARM)	2 vCPU	1GB
UCT-V	t2.micro	1 vCPU	1GB
UCT-V Controller	t2.xlarge	4 vCPU	16GB

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

AWS Security Credentials

To establish the initial connection between GigaVUE-FM and AWS, you will require the security credentials for AWS. These credentials are necessary to verify your identity and determine whether you have authorization to access the resources you are requesting. AWS employs these security credentials to authenticate and authorize your requests.

You need one of the following security credentials:

- **Identity and Access Management (IAM) role**— If GigaVUE-FM is running within AWS, it is recommended to use an IAM role. By using an IAM role, you can securely make API requests from the instances. Create an IAM role and ensure that the permissions and policies listed in Permissions are associated to the role and also ensure that you are using Customer Managed Policies or Inline Policies.
- **Access Keys**—If GigaVUE-FM is configured in the enterprise data center, then you must use the access keys or basic credentials to connect to the VPC. Basic credentials allow full access to all the resources in your AWS account. An access key consists of an access key ID and a secret access key. For detailed instructions on creating access keys, refer to the AWS documentation on [Managing Access Keys for Your AWS Account](#).

NOTE: To obtain the IAM role or access keys, contact your AWS administrator.

Amazon VPC

You must have a Amazon Virtual Private Cloud (VPC) to launch GigaVUE components into your virtual network.

NOTE: To create a VPC, refer to [Create a VPC](#) topic in the AWS Documentation.

Your VPC must have the following elements to configure the GigaVUE Cloud Suite for AWS components:

Subnet for VPC

VPC must have a subnet to configure the GigaVUE Cloud Suite for AWS components. You can either have the components deployed in a single subnet or in multiple subnets.

- **Management Subnet** that the GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers and UCT-V Controllers.
- **Data Subnet** that can accept incoming mirrored traffic from agents or be used to egress traffic to a tool.

If a single subnet is used, then the Management subnet is also used as a Data Subnet

Security Group

When you launch GigaVUE-FM, GigaVUE V Series Proxies, GigaVUE V Series Nodes, and UCT-V Controllers, a security group can be utilized to define virtual firewall rules for your instance, which in turn regulates inbound and outbound traffic. You can add rules to manage inbound traffic to instances, and a distinct set of rules to control outbound traffic.

It is recommended to create a separate security group for each component using the rules and port numbers listed in the following table.

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

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

GigaVUE-FM				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	443	Administrator Subnet	Allows GigaVUE-FM to accept Management connection using REST API. Allows users to access GigaVUE-FM UI securely through an HTTPS connection.
Inbound	TCP	22	Administrator Subnet	Allows CLI access to user-initiated management and diagnostics.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-V Controller using REST API.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Node using REST API when GigaVUE V Series Proxy is not used.

Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Proxy using REST API.
Inbound	TCP	443	UCT-C Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-C Controller using REST API.
Inbound	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive traffic health updates from GigaVUE V Series Nodes.
Inbound	TCP	5671	UCT-V Controller IP	Allows GigaVUE-FM to receive statistics from UCT-V Controllers.
Inbound	TCP	5671	UCT-C Controller IP	Allows GigaVUE-FM to receive statistics from UCT-C Controllers.
Inbound	UDP	2056	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive Application Intelligence and Application Visualization reports from GigaVUE V Series Node.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	9900	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic with UCT-V Controller.
Outbound (optional)	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Proxy.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Node.
Outbound	TCP	8443 (default)	UCT-C Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic to UCT Container Controller.
Outbound	TCP	443	Any IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.
UCT-V Controller				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate control and management plane traffic with GigaVUE-FM.
Inbound	TCP	9900	UCT-V or Subnet IP	Allows UCT-V Controller to receive traffic health updates from UCT-V.
Inbound (This is the port used	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests from UCT-V.

for Third Party Orchestration)				
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using Third Party Orchestration.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows UCT-V Controller to send the registration requests to GigaVUE-FM using REST API.
Outbound	TCP	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
UCT-V				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9901	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V Controller IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat.
Outbound	UDP (VXLAN)	VXLAN (default 4789)	GigaVUE V Series Node IP	Allows UCT-V to tunnel VXLAN traffic to GigaVUE V Series Nodes.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	GigaVUE V Series Node IP	Allows UCT-V to tunnel L2GRE traffic to GigaVUE V Series Nodes.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	GigaVUE V Series Node IP	Allows UCT-V to securely transfer the traffic to the GigaVUE V Series Node
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V to send traffic health updates to UCT-V Controller.
GigaVUE V Series Node				
Direction	Protocol	Port	Source CIDR	Purpose

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

Outbound	UDP	2055	Tool IP	Allows GigaVUE V Series Node to send NetFlow Generation traffic to an external tool.
Outbound	UDP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	<ul style="list-style-type: none"> echo request echo reply 	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic.
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE V Series Proxy when GigaVUE V Series Proxy is used.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE-FM when GigaVUE V Series Proxy is not used.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	Tool IP	Allows to securely transfer the traffic to an external tool.
GigaVUE V Series Proxy (optional)				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using Third Party Orchestration.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate control and

				management plane traffic with GigaVUE V Series Node.
Universal Cloud Tap - Container deployed inside Kubernetes worker node				
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	42042	Any IP address	Allows UCT-C to send statistical information to UCT-C Controller.
Outbound	UDP	VXLAN (default 4789)	Any IP address	Allows UCT-C to tunnel traffic to the GigaVUE V Series Node or other destination.
UCT-C Controller deployed inside Kubernetes worker node				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8443 (configurable)	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-C Controller.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	5671	Any IP address	Allows UCT-C Controller to send statistics to GigaVUE-FM.
Outbound	TCP	443	GigaVUE-FM IP	Allows UCT-C Controller to communicate with GigaVUE-FM.

Key Pair

A key pair consists of a public key and a private key. When you define the specifications for the UCT-V Controllers, GigaVUE V Series nodes, and GigaVUE V Series Proxy in your VPC, you must create a key pair and specify the name of this key pair.

To create a key pair, refer to [Create a key pair using Amazon EC2](#) topic in the AWS Documentation.

Permissions

If you use an account-wide policy to encrypt all volumes with KMS keys, you must add the "kms:GenerateDataKeyWithoutPlaintext" permission to the IAM policy.

For more information on permissions, see the topic [Check for Required IAM Permissions](#).

GigaVUE-FM Version Compatibility

GigaVUE-FM version 6.9.00 supports the latest version (6.9.00) of GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, and UCT-V, as well as (n-2) versions. For better compatibility, we recommend to use the latest version of fabric components with GigaVUE-FM.

Default Login Credentials

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

Product	Login credentials
GigaVUE V Series Node	You can login to the GigaVUE V Series Node by using ssh. The default username and password is: Username: gigamon Password: Use the SSH key.
GigaVUE V Series Proxy	You can login to the GigaVUE V Series proxy by using ssh. The default username and password is: Username: gigamon Password: Use the SSH key.
UCT-V Controller	You can login to the GigaVUE V Series proxy by using ssh. The default username and password is: Username: ubuntu Password: Use the SSH key.

Points to Note for GigaVUE Cloud Suite for AWS

Considerations when deploying GigaVUE Cloud Suite:

- We recommend to deploy the GigaVUE-FM on the AWS to manage AWS workload.
- If the GigaVUE-FM is deployed outside of the AWS, then the GigaVUE-FM encrypts and stores the access key and the secret key in its database.
- Always attach an IAM role to the instance running GigaVUE-FM in AWS to connect it to your AWS account.
- If you are launching the GigaVUE-FM instance from the AWS Marketplace, you need to have only the IAM roles.
- Deployment of GigaVUE fabric components through a third-party orchestrator is supported on Linux and Windows platforms.
- Fragmentation in the network should be avoided from UCT-V to GigaVUE V Series Node and from GigaVUE V Series Node to tool by setting appropriate MTU for the interfaces. If the tool VM MTU is less than that of GigaVUE V Series Node, then GigaVUE V Series Node fragments the packets. This results in packet loss as ENA (Elastic Network Adapter) of AWS drops all fragments over 200 packet per second.
- Set appropriate MTU for the interfaces to avoid fragmentation in the network from UCT-V to GigaVUE V Series Node and from GigaVUE V Series Node to tool.
- If the tool VM MTU is less than that of GigaVUE V Series Node, then GigaVUE V Series Node fragments the packets. Fragment packets are reordered on arrival at the V-series node.
- When GigaVUE-FM and GigaVUE V Series Nodes are deployed on different cloud platforms, then you must add the GigaVUE-FM public IP address to the **Data Notification Interface** as the Target Address in the Event Notifications page. For details, refer to the [Configuration Settings](#) section in GigaVUE Administration Guide.
- When GigaVUE-FM and the workload VMs requiring monitoring are in different AWS accounts (cross-account) and AWS Traffic Mirroring is the Traffic Acquisition Method, you must either configure a Network Load Balancer or Gateway Load Balancer. For details, refer to [Configure AWS Elastic Load Balancing](#).

Deployment Options for GigaVUE Cloud Suite for AWS

This section provides a detailed information on the multiple ways in which GigaVUE Cloud Suite for AWS-GigaVUE V Series 2 can be configured to provide visibility for physical and virtual traffic. There are three different ways in which GigaVUE Cloud Suite for AWS-GigaVUE V Series 2 can be configured based on

the traffic acquisition method and the method in which you want to deploy fabric components. For information on the prerequisites and work flow refer the following topics:

- [Prerequisites for AWS](#)
- [Deploy GigaVUE Fabric Components using AWS](#)
- [Deploy GigaVUE Fabric Components using GigaVUE-FM](#)
 - [Traffic Acquisition Method as UCT-V](#)
 - [Traffic Acquisition Method as Traffic Mirroring](#)
 - [Traffic Acquisition Method as Customer Orchestrated Source](#)

Deploy GigaVUE Fabric Components using AWS

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

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

Deploy GigaVUE Fabric Components using GigaVUE-FM

You can deploy GigaVUE fabric components using GigaVUE-FM using one of the following three traffic acquisition methods:

Traffic Acquisition Method as UCT-V

In traffic acquisition using UCT-V, the traffic from Virtual Machines is acquired using the UCT-Vs and forwarded to the V Series nodes. To acquire traffic using UCT-V, perform the following steps:

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

Traffic Acquisition Method as Traffic Mirroring

Perform the following steps to use Traffic Mirroring as your traffic acquisition method:

NOTE: When GigaVUE-FM and the workload VMs requiring monitoring are in different AWS accounts (cross-account) and AWS Traffic Mirroring is the Traffic Acquisition Method, you must either configure a Network Load Balancer or Gateway Load Balancer. Refer to [Configure AWS Elastic Load Balancing](#) for more details.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Create a Monitoring Domain Ensure that the Use FM to Launch Fabric toggle button is enabled.	Create a Monitoring Domain
3	Configure GigaVUE Fabric Components NOTE: Select Traffic Mirroring as the Traffic Acquisition Method. You can configure a prefilter and determine the VPC endpoint traffic that is mirrored. For more information on prefiltering, see Configure a Traffic Pre-filter .	Configure GigaVUE Fabric Components in GigaVUE-FM

Step No	Task	Refer the following topics
4	Create Monitoring session	Create a Monitoring Session (AWS)
5	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (AWS)
6	Deploy Monitoring Session	Deploy Monitoring Session (AWS)
7	View Monitoring Session Statistics	View Monitoring Session Statistics (AWS)

Traffic Acquisition Method as Customer Orchestrated Source

You can use tunnels as a source where the traffic is directly tunneled to V Series nodes without deploying UCT-Vs or UCT-V Controllers. Perform the following steps to use Tunnel as your traffic acquisition method:

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

Deploy GigaVUE Cloud Suite for AWS

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

If you already have GigaVUE-FM running outside of your AWS environment, you can connect that existing GigaVUE-FM to your AWS using the Basic Credentials (Access Keys).

Refer to the following sections:

- [Permissions and Privileges \(AWS\)](#)
- [Install GigaVUE-FM on AWS](#)
- [Create a Monitoring Domain](#)
- [Configure GigaVUE Fabric Components in GigaVUE-FM](#)
- [Configure Role-Based Access for Third Party Orchestration](#)
- [Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode](#)
- [Install UCT-V](#)

Permissions and Privileges (AWS)

GigaVUE-FM requires access to AWS EC2 APIs to deploy the solution. IAM allows you to control the actions that GigaVUE-FM can take on your EC2 resources.

To configure the components,

1. Enable the permissions listed below and attach the policies to an IAM role.
2. Attach the IAM role to the GigaVUE-FM instance running in AWS.

If the GigaVUE-FM is running outside the AWS, then you must use the access key id and secret access keys.

For details, refer to [IAM roles for Amazon EC2](#) in the AWS Documentation.

The following topics list the minimum permissions that are required for traffic acquisition:

- [GigaVUE-FM Instance Multi Account Support Using Amazon STS](#)
- [Minimum Permissions Required for Acquiring Traffic using the UCT-V](#)
- [Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source](#)
- [Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with GwLB](#)
- [Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with NwLB](#)
- [Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring](#)
- [Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring with Network Load Balancer](#)
- [Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring and GwLB](#)

Minimum Permissions Required for Inline Policies and Basic Authentication

IMPORTANT: Review the examples below.

IAM permissions required for Inline Policies

If inline policies are attached to the user, then include the following permission:

```
"iam:GetUserPolicy"
```

If there are inline policies attached to the user group, then include the following permission:

```
"iam:GetGroupPolicy"
```

IAM instance role for authentication

Use the following permissions if you are using the IAM instance role for authentication:

```
"iam:ListAttachedRolePolicies",  
"iam:GetPolicy",  
"iam:GetPolicyVersion",  
"iam:ListRolePolicies",  
"iam:ListAccountAliases",
```

IAM permissions required for Basic Authentication

```
"iam:ListGroupsForUser"  
"iam:ListAttachedUserPolicies"  
"iam:ListAttachedGroupPolicies"  
"iam:GetPolicy",  
"iam:GetPolicyVersion",  
"iam:ListUserPolicies"  
"iam:ListGroupPolicies"  
"iam:ListAccountAliases",
```

GigaVUE-FM Instance Multi Account Support Using Amazon STS

This section provides instructions on how to set up your GigaVUE-FM instance to work with multiple accounts using Amazon Security Token Service (STS).

Prerequisites

You must complete the following prerequisites before configuring GigaVUE-FM for Amazon STS support.

- Include a policy in other accounts as well.
- These policies must allow GigaVUE-FM to assume the role in that account.

Procedure

For the purposes of these instructions, the AWS account that runs the GigaVUE-FM instance is called the source account, and any other AWS account that runs monitored instances is called a target account.

To configure GigaVUE-FM for Amazon STS support,

1. In each target account, create an IAM role with the source account number as a trusted entity and attach policies with permissions allowing GigaVUE-FM to perform its functions. Record the ARN of each role created.

NOTE: This role must exist in all accounts to support the ability to create a single Monitoring Domain in GigaVUE-FM that includes multiple accounts.

2. In the source account, create a new IAM policy that allows GigaVUE-FM to retrieve IAM policies.

IMPORTANT: The following example is provided as an example.

- a. Use the following permissions if you are using the IAM instance role for authentication:

```
"iam:ListAttachedRolePolicies",  
"iam:GetPolicy",  
"iam:GetPolicyVersion",  
"iam:ListRolePolicies",  
"iam:ListAccountAliases",
```

If inline policies are linked to the role, then you must include the following permission:

```
"iam:GetRolePolicy"
```

- b. Use the following permissions for basic authentication:

```
"iam:ListGroupsForUser"  
"iam:ListAttachedUserPolicies"  
"iam:ListAttachedGroupPolicies"  
"iam:GetPolicy",  
"iam:GetPolicyVersion",  
"iam:ListUserPolicies"  
"iam:ListGroupPolicies"  
"iam:ListAccountAliases",
```

If inline policies are attached to the user, then include the following permission:

```
"iam:GetUserPolicy"
```

If inline policies are attached to the user group, then include the following permission:

```
"iam:GetGroupPolicy"
```

3. In the source account, create a new IAM policy that allows the "sts:AssumeRole" action on all role ARNs created in Step 1.

IMPORTANT: The following example is provided as an example.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Action": "sts:AssumeRole",  
      "Resource": [  
        "arn:aws:iam::123456789012:role/FM-Role-target-account"  
      ]  
    }  
  ]  
}
```

NOTE: In this example, 123456789012 is a target account and FM-Role-target-account is the role in the target account configured in step 1 with permissions required for GigaVUE-FM.

4. In the source account, attach the policies created in steps 2 and 3 to the IAM role that is attached to the GigaVUE-FM instance.

Minimum Permissions Required for Acquiring Traffic using the UCT-V

Prerequisites:

Before configuring the required permissions and privileges in AWS, you must install GigaVUE-FM. For details, refer to [Install GigaVUE-FM on AWS](#).

Minimum permissions required to acquire traffic using the UCT-V and authenticate using an IAM instance role

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumes",
        "ec2:DescribeAddresses",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListAccountAliases",
        "iam:ListRolePolicies",
        "kms:ListAliases",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*"
    }
  ]
}

```

For more information regarding policies and permissions, refer to [AWS Documentation](#).

If you are using inline policy or basic authentication, then update the policy with the relevant IAM service. For more information, see [GigaVUE-FM Instance Multi Account Support Using Amazon STS](#).

What to do Next:

Configure the AWS credentials in GigaVUE-FM to monitor workloads across multiple AWS accounts within one Monitoring Domain. For details, refer to [Create AWS Credentials](#).

Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source

Prerequisites:

Before configuring the required permissions and privileges in AWS, you must install GigaVUE-FM. For details, refer to [Install GigaVUE-FM on AWS](#).

If you are using inline policy or basic authentication, then update the policy with the relevant IAM service. For more information, see [Minimum Permissions Required for Inline Policies and Basic Authentication](#).

Minimum permissions required to acquire traffic using the customer orchestrated, use a GigaVUE V Series Proxy and authenticate using an IAM instance role.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumes",
        "ec2:DescribeAddresses",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListAccountAliases",
        "kms:ListAliases",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
    }
  ],
}
```

```

    "Resource": "*"
  }
]
}

```

For more information regarding policies and permissions, refer to [AWS Documentation](#).

What to do Next:

Configure the AWS credentials in GigaVUE-FM to monitor workloads across multiple AWS accounts within one Monitoring Domain. For details, refer to [Create AWS Credentials](#).

Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with GwLB

Prerequisites:

Before configuring the required permissions and privileges in AWS, you must install GigaVUE-FM. For details, refer to [Install GigaVUE-FM on AWS](#).

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see [Minimum Permissions Required for Inline Policies and Basic Authentication](#).

Minimum permissions required to acquire traffic using Customer Orchestrated Source with Gateway Load Balancer and authenticate using an IAM instance role

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAddresses",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateTags",
        "ec2>DeleteTags",

```

```

    "ec2:DescribeImages",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcEndpoints",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:ListAttachedRolePolicies",
    "iam:ListRolePolicies",
    "iam:ListAccountAliases",
    "ram:CreateResourceShare",
    "ram>DeleteResourceShare",
    "ram:AssociateResourceShare",
    "ram:GetResourceShareInvitations",
    "ram:AcceptResourceShareInvitation",
    "ram:DisassociateResourceShare",
    "kms:ListAliases",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*"
}
]

```

For more information regarding policies and permissions, refer to [AWS Documentation](#).

What to do Next:

Configure the AWS credentials in GigaVUE-FM to monitor workloads across multiple AWS accounts within one Monitoring Domain. For details, refer to [Create AWS Credentials](#).

Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with NwLB

Prerequisites:

Before configuring the required permissions and privileges in AWS, you must install GigaVUE-FM. For details, refer to [Install GigaVUE-FM on AWS](#).

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see [Minimum Permissions Required for Inline Policies and Basic Authentication](#).

Minimum permissions required to acquire traffic using Customer Orchestrated Source with Network Load Balancer and authenticate using an IAM instance role

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",

```

```

    "Effect": "Allow",
    "Action": [
      "autoscaling:DescribeAutoScalingGroups",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:DeregisterTargets",
      "elasticloadbalancing:DescribeTargetHealth",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeAddresses",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeSecurityGroups",
      "ec2:CreateTags",
      "ec2>DeleteTags",
      "ec2:DescribeImages",
      "ec2:DescribeVolumes",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedRolePolicies",
      "iam:ListRolePolicies",
      "iam:ListAccountAliases",
      "ram:CreateResourceShare",
      "ram>DeleteResourceShare",
      "ram:AssociateResourceShare",
      "ram:GetResourceShareInvitations",
      "ram:AcceptResourceShareInvitation",
      "ram:DisassociateResourceShare",
      "kms:ListAliases",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*"
  }
]

```

For more information regarding policies and permissions, refer to [AWS Documentation](#).

What to do Next:

Configure the AWS credentials in GigaVUE-FM to monitor workloads across multiple AWS accounts within one Monitoring Domain. For details, refer to [Create AWS Credentials](#).

Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring

Prerequisites:

Before configuring the required permissions and privileges in AWS, you must install GigaVUE-FM. For details, refer to [Install GigaVUE-FM on AWS](#).

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see [Minimum Permissions Required for Inline Policies and Basic Authentication](#).

Minimum permissions required to acquire traffic using Traffic Mirroring and authenticate using an IAM instance role

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumes",
        "ec2:DescribeAddresses",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:CreateTrafficMirrorTarget",
        "ec2:CreateTrafficMirrorSession",
        "ec2>DeleteTrafficMirrorTarget",
        "ec2>DeleteTrafficMirrorSession",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam>ListAttachedRolePolicies",
        "iam>ListRolePolicies",
        "iam>ListAccountAliases",
        "kms>ListAliases"
      ],
      "Resource": "*"
    }
  ]
}
```

For more information regarding policies and permissions, refer to [AWS Documentation](#).

What to do Next:

Configure the AWS credentials in GigaVUE-FM to monitor workloads across multiple AWS accounts within one Monitoring Domain. For details, refer to [Create AWS Credentials](#).

Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring with Network Load Balancer

Prerequisites:

Before configuring the required permissions and privileges in AWS, you must install GigaVUE-FM. For details, refer to [Install GigaVUE-FM on AWS](#).

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see [Minimum Permissions Required for Inline Policies and Basic Authentication](#).

Minimum permissions required to acquire traffic using Traffic Mirroring with Network Load Balancer and authenticate using an IAM instance role

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAddresses",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "ec2:CreateTrafficMirrorFilterRule",
        "ec2:CreateTrafficMirrorTarget",
        "ec2:CreateTrafficMirrorSession",
        "ec2:CreateTrafficMirrorFilter",
        "ec2>DeleteTrafficMirrorTarget",
        "ec2>DeleteTrafficMirrorSession",
        "ec2>DeleteTrafficMirrorFilter",
        "ec2:DescribeTrafficMirrorSessions",

```

```

        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTrafficMirrorFilters",
        "ram:CreateResourceShare",
        "ram>DeleteResourceShare",
        "ram:GetResourceShareInvitations",
        "ram:AcceptResourceShareInvitation",
        "ram:DisassociateResourceShare",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListAccountAliases",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ListAliases",
    ],
    "Resource": "*"
}
]
}

```

For more information regarding policies and permissions, refer to [AWS Documentation](#).

What to do Next:

Configure the AWS credentials in GigaVUE-FM to monitor workloads across multiple AWS accounts within one Monitoring Domain. For details, refer to [Create AWS Credentials](#).

Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring and GwLB

Prerequisites:

Before configuring the required permissions and privileges in AWS, you must install GigaVUE-FM. For details, refer to [Install GigaVUE-FM on AWS](#) for more detailed information on how to install GigaVUE-FM in AWS.

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see [Minimum Permissions Required for Inline Policies and Basic Authentication](#).

This policy allows you to acquire traffic using Traffic Mirroring with Gateway Load Balancer and authenticate using an IAM instance role.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",

```

```

    "Action": [
      "autoscaling:DescribeAutoScalingGroups",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:DeregisterTargets",
      "elasticloadbalancing:DescribeTargetHealth",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeAddresses",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeSecurityGroups",
      "ec2:CreateTags",
      "ec2:DeleteTags",
      "ec2:DescribeImages",
      "ec2:DescribeVolumes",
      "ec2:CreateTrafficMirrorFilterRule",
      "ec2:CreateTrafficMirrorTarget",
      "ec2:CreateTrafficMirrorSession",
      "ec2:CreateTrafficMirrorFilter",
      "ec2>DeleteTrafficMirrorTarget",
      "ec2>DeleteTrafficMirrorSession",
      "ec2>DeleteTrafficMirrorFilter",
      "ec2:DescribeTrafficMirrorSessions",
      "ec2:DescribeTrafficMirrorTargets",
      "ec2:DescribeTrafficMirrorFilters",
      "ec2:DescribeVpcEndpointServiceConfigurations",
      "ec2:DescribeVpcEndpoints",
      "ram:CreateResourceShare",
      "ram>DeleteResourceShare",
      "ram:GetResourceShareInvitations",
      "ram:AcceptResourceShareInvitation",
      "ram:DisassociateResourceShare",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedRolePolicies",
      "iam:ListRolePolicies",
      "iam:ListAccountAliases",
      "kms:ListAliases",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*"
  }
}

```

For more information regarding policies and permissions, refer to [AWS Documentation](#).

What to do Next:

Configure the AWS credentials in GigaVUE-FM to monitor workloads across multiple AWS accounts within one Monitoring Domain. For details, refer to [Create AWS Credentials](#).

Install GigaVUE-FM on AWS

You can subscribe to GigaVUE-FM in the marketplace and launch in AWS by subscribing.

Refer to the following topics for instruction on installing GigaVUE-FM in AWS:

- [Subscribe to GigaVUE-FM](#)
- [Initial Configuration](#)

Subscribe to GigaVUE-FM

You can deploy the GigaVUE Cloud Suite for AWS from the AWS Marketplace.

NOTE: Only users with `aws-marketplace:ViewSubscriptions` permission in their IAM policy can subscribe to GigaVUE products.

To subscribe to the GigaVUE-FM, perform the following steps:

1. Log in to your AWS account.
2. Go to AWS Marketplace: <https://aws.amazon.com/marketplace/>.
3. In the **Search** field, type Gigamon and select **Search**.
4. Select the latest version GigaVUE Cloud Suite BYOL version. For more information on Licensing, refer to [Licensing for GigaVUE Cloud Suite for AWS](#)
5. Select **View Purchase Options**. The terms and condition page is displayed.
6. Review the Terms and Conditions and then select "**Accept Terms**".
7. Review the summary and select **Continue to Configuration**.
8. In the **Configure this software** page, enter the following details for your deployment:
 - a. Set **Fulfillment Option** to the default value.
 - b. Select the latest version in the **Software Version** field.
 - c. Select your deployment **Region**.
 - d. Select **Continue to Launch**.

9. In the **Configure this software** page, perform the following:
 - a. In the **Choose Action** field, select the **Launch from Website** option.
 - b. From the **EC2 Instance Type** drop-down list, select the instance type. Refer to [Recommended and Supported Instance Types for AWS](#).
 - c. From the **VPC Settings** drop-down list, select the VPC for deploying GigaVUE-FM.
 - d. In the **Subnet Settings**, choose your select Subnet.
 - e. Configure the security group in the **Security Group Settings** to match your access and permissions needs. Refer to [Security Group](#) for more details.
 - f. Select your preferred **Key Pair** for secure access to the instance.
 - g. In the **Advanced details** section, select **V1 and V2 (token optional)** from the **Metadata version** drop-down list.
 - h. Select **Launch**.

GigaVUE-FM is launched in AWS. You must perform the initial configuration to view the GigaVUE-FM UI.

Initial Configuration

It may take several minutes for the GigaVUE-FM instance to start up. Once it is up and running, you can verify that it is working properly.

Follow these steps:

1. In your EC2 Instances page, select the **Instance ID** of the launched GigaVUE-FM to view the instance information.
2. Copy and paste the **Public IP address** into a new browser window or tab. The GigaVUE-FM GUI appears.



NOTE:

- If GigaVUE-FM is deployed inside AWS, use **admin** as the username and the **Instance ID** as the default password for the admin user to log in to GigaVUE-FM, for example i-079173111e2d73753 (**Instance ID**). You can get the **Instance ID** of GigaVUE-FM in the EC2 Instances page.
- If GigaVUE-FM is deployed outside the AWS, use admin123A!! as the default admin password.

When you first log in to GigaVUE-FM, you are asked to change your default password.

What to do Next:

Configure the required permission and privileges in AWS. For detailed instructions on configuring required AWS permissions and privileges for your chosen deployment option, refer to the following topics:

Deployment Options	Reference Topics
Acquire Traffic using UCT-V	Minimum Permissions Required for Acquiring Traffic using the UCT-V
Acquire Traffic using Customer Orchestrated Source	Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source
Acquire Traffic using Customer Orchestrated Source when configuring Gateway Load Balancer in AWS	Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with GwLB
Acquire Traffic using Customer Orchestrated Source when configuring Network Load Balancer in AWS	Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with NwLB
Acquire Traffic using Traffic Mirroring	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring
Acquire Traffic using Traffic Mirroring when configuring Gateway Load Balancer in AWS	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring and GwLB
Acquire Traffic using Traffic Mirroring when configuring Network Load Balancer in AWS	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring with Network Load Balancer

Install Custom Certificate on AWS

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 certificates to avoid the trust issues that occur 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 a name for the certificate in the **Certificate Name** field.
4. To upload the certificate, select the **Choose File** Button in the **Certificate** field.
5. To upload private key associated with the certificate, select the **Choose File** Button in the **Private Key** field.
6. Select **Save**.

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

You can link the uploaded certificates to the respective GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller in the Fabric Launch Configuration Page. For details, refer to the *Configure GigaVUE Fabric Components in GigaVUE-FM* topic in the respective cloud guides.

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 Controllers using your own cloud platform at the time of deploying the fabric components. Refer to the following topics for 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 using Third Party Orchestration - Integrated Mode](#)

For generic mode:

- Refer to Configure GigaVUE Fabric Components in AWS section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

Adding Certificate Authority

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

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

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

Create AWS Credentials

You can monitor workloads across multiple AWS accounts within one Monitoring Domain.



- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

Refer to [Create a Monitoring Domain](#) for more details on how to create a Monitoring Domain.

Prerequisite:

Configure the required permission and privileges in AWS. Refer to the following topics for more detailed information on how to configure the required permission and privileges in AWS based on your deployment option:

Deployment Option	Reference Topics
Acquire Traffic using UCT-V	Minimum Permissions Required for Acquiring Traffic using the UCT-V
Acquire Traffic using Customer Orchestrated Source	Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source
Acquire Traffic using Customer Orchestrated Source when configuring Gateway Load Balancer in AWS	Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with GwLB
Acquire Traffic using Customer Orchestrated Source when configuring Network Load Balancer in AWS	Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with NwLB
Acquire Traffic using Traffic Mirroring	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring
Acquire Traffic using Traffic Mirroring when configuring Gateway Load Balancer in AWS	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring and GwLB
Acquire Traffic using Traffic Mirroring when configuring Network Load Balancer in AWS	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring with Network Load Balancer

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and then select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.

Configure Credential Save Cancel

Name*	Credential Name
Authentication Type	Basic Credentials
Access Key*	Access Key
Secret Access Key*	Secret Access Key

3. In the **Name** Field, enter a name to identify the AWS Credential.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to [AWS Security Credentials](#).
5. In the **Access Key** field, enter the credential of an IAM user or the AWS account root user.
6. In the **Secret Access Key** field, enter the security password or key.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

What to do Next:

After creating AWS credentials in GigaVUE-FM, based on your deployment option, perform any of the following actions.

Deployment Options	Reference Topics
With Load balancer	
Using Network Load balancer	Configure Network Load Balancer
Using Gateway Load balancer	Configure a Gateway Load Balancer
Without Load Balancer and GigaVUE-FM Orchestration	
Deploying GigaVUE Fabric Components using GigaVUE-FM with Traffic Acquisition Method as VPC Mirroring or Customer Orchestrated Source	Create a Monitoring Domain
Deploying GigaVUE Fabric Components using GigaVUE-FM with Traffic Acquisition Method as UCT-V	Configure UCT-V
Without Load Balancer and Third Party Orchestration	
Deploying GigaVUE Fabric Components using AWS Traffic Acquisition Method as VPC Mirroring or Customer Orchestrated Source	Configure Role-Based Access for Third Party Orchestration
Deploying GigaVUE Fabric Components using GigaVUE-FM with Traffic Acquisition Method as UCT-V	Configure UCT-V

Create a Monitoring Domain

GigaVUE-FM connects to the AWS Platform through the public API endpoint. HTTPS is the default protocol which GigaVUE-FM uses to communicate with the API. For more information about the endpoint and the protocol used, refer to [AWS service endpoints](#).

GigaVUE-FM provides you the flexibility to monitor multiple VPCs. You can choose the VPC ID and launch the GigaVUE fabric components in the desired VPCs.

NOTE: To configure the Monitoring Domain and launch the fabric components in AWS, you must be a user with **fm_super_admin** role or a user with write access to the **Infrastructure Management** category. Refer to [Role Based Access Control](#) for more detailed information.

Prerequisites:

Complete one of the following actions, depending on your deployment option.

Deployment Options	Reference Topics
GigaVUE-FM Orchestration	
Deploying GigaVUE Fabric Components using GigaVUE-FM with Traffic Acquisition method as Traffic Mirroring or Customer Orchestrated Source	Create AWS Credentials
Deploying GigaVUE Fabric Components using AWS with Traffic Acquisition method as UCT-V	Configure UCT-V
Third Party Orchestration	
Deploying GigaVUE Fabric Components using AWS with Traffic Acquisition method as Traffic Mirroring or Customer Orchestrated Source	Configure Role-Based Access for Third Party Orchestration
Deploying GigaVUE Fabric Components using AWS with Traffic Acquisition method as UCT-V	Configure UCT-V

To create a Monitoring Domain:

1. Go to **Inventory > VIRTUAL > AWS**, and then select **Monitoring Domain**.
2. On the Monitoring Domain page, select **New**. The **Monitoring Domain Configuration** page appears.
3. Select **Check Permissions** and validate whether you have the required permissions.
4. In the **Monitoring Domain** field, enter an alias used to identify the Monitoring Domain.

5. From the **Traffic Acquisition Method** drop-down list, select one of the following tapping method:
- **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. You can also configure the UCT-V Controller and UCT-Vs from your own orchestrator. For details, refer to [Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode](#).
 - **VPC Traffic Mirroring:** If you select the VPC Traffic Mirroring option, the mirrored 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. For more information on VPC Peering, refer to [VPC peering connections](#) in the AWS Documentation. Peering is required to send mirrored traffic from other VPCs into a centralized GigaVUE V Series deployment. You can choose to use an external load balancer for Traffic Mirroring. Select **Yes** to use load balancer. For details, refer to [Configure AWS Elastic Load Balancing](#).

**NOTE:**

- UCT-V Controller configuration is not applicable for Traffic Mirroring.
- Traffic Mirroring does not support cross-account solutions without a load balancer.
- For VPC Traffic Mirroring option, additional permissions are required. For details, refer to [Permissions and Privileges \(AWS\)](#).
- After deploying the Monitoring Session, a traffic mirror session is created in your AWS VPC consisting of a session, a filter, sources, and targets. For more details, refer to [Traffic Mirroring](#) in AWS Documentation.

- **Customer Orchestrated Source:** If you use select **Customer Orchestrated Source** as the tapping method, you can use the Customer Orchestrated Source as a source option in the monitoring session, where the traffic is directly tunneled to the GigaVUE V Series nodes without deploying UCT-Vs and UCT-V Controllers. The user is responsible for creating this tunnel feed and pointing it to the GigaVUE V Series Node(s).

NOTE: When using Application Metadata Exporter (AMX) application, select the **Traffic Acquisition Method** as **Customer Orchestrated Source**.

6. In the **Traffic Acquisition Tunnel MTU**, enter the MTU value.
- 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 default value is 8951.
 - When using IPv4 tunnels, the maximum MTU value is 8951. Ensure that the UCT-V tunnel MTU is 50 bytes less than the destination interface MTU size of the UCT-V.
 - When using IPv6 tunnels, the maximum MTU value is 8931. Ensure that the UCT-V tunnel MTU is 70 bytes less than the destination interface MTU size of the UCT-V.

7. Turn on the **Use FM to Launch Fabric** toggle, to deploy GigaVUE Fabric Components using GigaVUE-FM.
 - Select **Yes** to [Configure GigaVUE Fabric Components in GigaVUE-FM](#)
 - Select **No** to [Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode](#).
8. Turn on the **Enable IPv6 Preference** toggle, to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

NOTE: This appears only when **Use FM to Launch Fabric** is disabled and **Traffic Acquisition Method** is **UCT-V**.

9. Under Connections, in the **Name** field, enter an alias used to identify the connection.
10. From the **Credential** drop-down list, select an AWS credential. For detailed information, refer to [Create AWS Credentials](#).
11. From the **Region** drop-down list, select AWS region for the Monitoring Domain. For example, US West.
12. From the **Accounts** drop-down list, select the AWS accounts.
13. From the **VPCs** drop-down list, select the VPCs to monitor.
14. Select **Save**.

You can view the new Monitoring Domain in the **Monitoring Domain** page list view.

To edit a Monitoring Domain, select the deployed Monitoring Domain and select **Actions**. From the drop-down list, select **Edit**, the **Monitoring Domain Configuration** page appears.

Check Permissions while Creating a Monitoring Domain

To check the permissions while creating a Monitoring domain, follow these steps:

1. Go to **Inventory > VIRTUAL > AWS**, and then select **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select **New**. The **Monitoring Domain Configuration** page appears.
3. Enter the details as mentioned in the [Create a Monitoring Domain](#) section.
4. Select the **Check Permission** button. The **Check Permissions** widget opens.
5. Select the connection for which you wish to check the required permissions and then click **Next**.
6. Select on the **Permission Status** to view the missing permissions. The **ACCOUNTS** tab lists the accounts and the permissions status.
7. Review the accounts that has an error in the permission status. The **PERMISSIONS** tab lists the permissions required to run GigaVUE Cloud Suite for AWS.

- Make sure to include all the permissions with Access Status as **Denied** in the IAM policy. The **IAM POLICY** tab lists the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite for AWS.

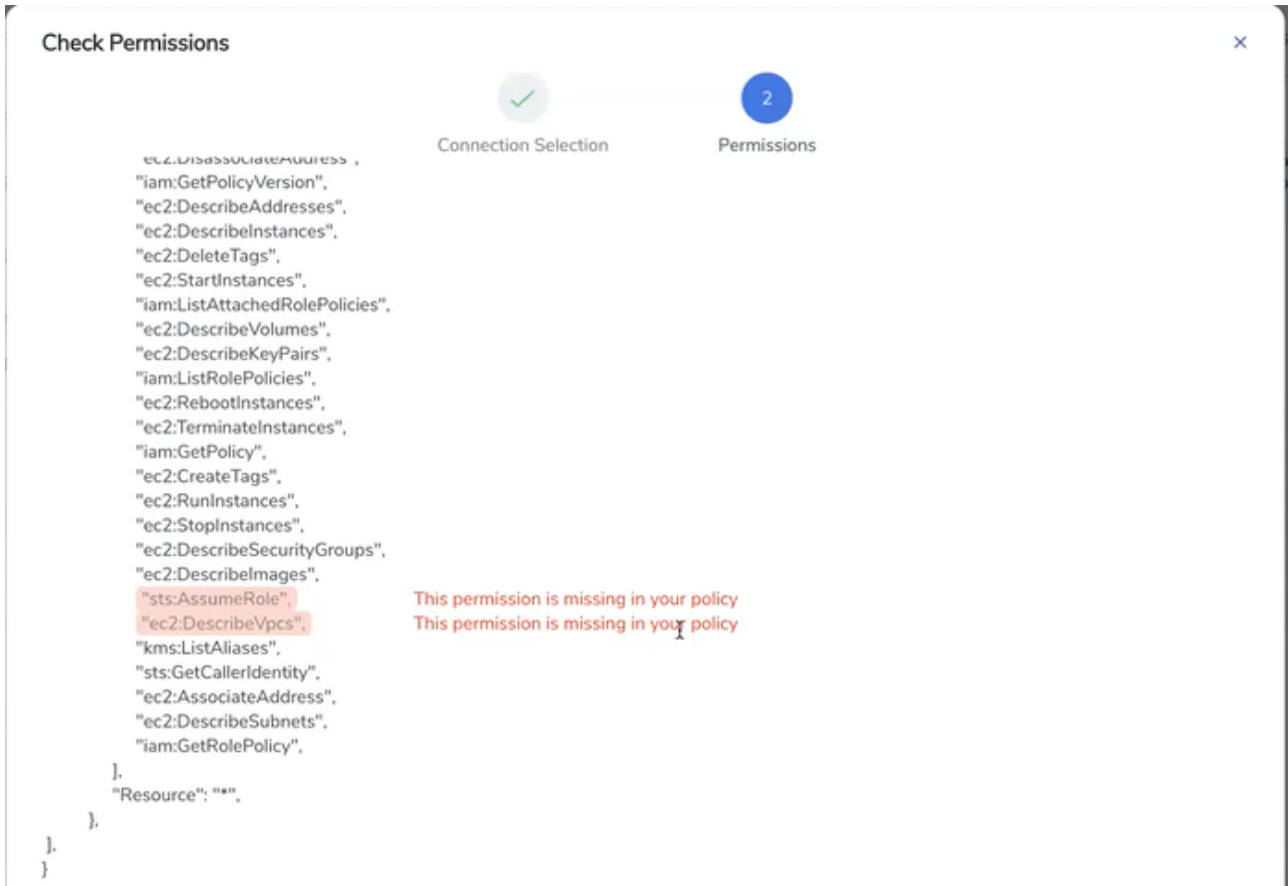
The table below lists the missing permissions. Make sure to include all the permissions with the access status as 'Denied' in the **IAM Policy** which is attached to the GigaVUE FM.

Access Status: All ▾ Recheck Export

PERMISSION	ACCOUNT	ACCESS STATUS	REASON	RESOURCE	
sts:AssumeRole	[Redacted]	❌ Denied	software.amazon.aw...	arn:aws:iam:*	
ec2:DescribeVpcs	[Redacted]	❌ Denied	software.amazon.aw...	arn:aws:iam:*	
sts:GetCallerIdentity	--	✅ Allowed	--	--	
iam:ListRolePolicies	--	✅ Allowed	--	--	
iam:ListAttachedRole...	--	✅ Allowed	--	--	
iam:GetPolicy	--	✅ Allowed	--	--	

- Update the AWS IAM policy with the missing permissions that are highlighted in the JSON.

10. Go to the **PERMISSIONS** tab and select **Recheck** to recheck the IAM policy.



When you select Copy or Download, the entire JSON file is copied or downloaded.

NOTE: After updating the IAM Policy, it takes around 5 minutes for the changes to reflect on the Check Permissions screen.

You can view the permission status reports in the **Monitoring Domain** page. Permission status reports consist of previously run **Check permissions** reports. They are auto purged once every 30 days. You can change the purge interval from the **Advanced Settings** page. For details, refer to [Configure AWS Settings](#).

- **View permission status report:** In the **Monitoring Domain** page, select **Actions > View Permission Status Report**.
- **View or delete individual reports:** Select the report and select **Actions**.

What to do Next:

Based on your chosen deployment option, perform any of the following actions:

- **Use FM to Launch Fabric** is enabled: You are navigated to the **AWS Fabric Launch Configuration** page. For details, refer to [Configure GigaVUE Fabric Components in GigaVUE-FM](#).


- **Use FM to Launch Fabric** is disabled: You must deploy GigaVUE Fabric Components using AWS. For details, refer to [Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode](#).

Managing Monitoring Domain

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

- [Monitoring Domain](#)
- [Connections Domain](#)
- [Fabric](#)
- [UCT-V](#)
- [UCT-V Upgrade](#)

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

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

To edit or delete a specific monitoring domain,


1. Select the Monitoring Domain
2. Select the ellipses "...".

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

Monitoring Domain

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

- Monitoring Domain
- Connections
- Tunnel MTU
- Acquisition Method
- Load Balancer
- Centralized connection
- Management Subnet

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

Use the following buttons to manage your Monitoring Domain:

Button	Description
New	Use to create new connection
Actions	<p>You can select a Monitoring Domain and then perform the following options:</p> <ul style="list-style-type: none"> • Edit Monitoring Domain- Select a Monitoring Domain and then click Edit Monitoring Domain to update the configuration. • Delete Fabric- You can delete all the fabrics associated with the Monitoring Domain of the selected Fabric. • Delete Monitoring Domain - You can select a Monitoring Domain or multiple Monitoring Domains to delete them. • Deploy Fabric - -You can select a Monitoring Domain to deploy a fabric, you cannot choose multiple Monitoring Domains at the same time to deploy fabrics. This option is only enabled when there is No FABRIC (launch configuration) for that specific Monitoring Domain and GigaVUE-FM orchestration is enabled. You must create a fabric in the monitoring domain, if the option is disabled • Upgrade Fabric-You can select a Monitoring Domain or multiple Monitoring Domains to upgrade the fabric. You can upgrade the GigaVUE V Series Nodes using this option. • Edit SSL Configuration - You can use this option to add Certificate Authority and the SSL Keys when using the Secure Tunnels. • Check Permissions - You can use this option to validate whether policy attached to the GigaVUE-FM using "EC2 Instance Role" or "Access Credential" has the required IAM permissions and notifies the users about the missing permissions. • View Permission Status Report - You can use this option to get the reports of previously run Check permissions.
Filter	<p>Filters the Monitoring Domain based on the list view options that are configured:</p> <ul style="list-style-type: none"> • Tunnel MTU • Load Balancer • Acquisition Method • Centralised Connection • Management Subnet <p>You can view the filters applied on the top of the Monitoring Domain page as a button. You can remove the filters by closing the button.</p>

Connections Domain

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

The list view shows the following details:

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

Fabric

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

The list view shows the following details:

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

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

- **Edit Fabric** - You can select one fabric or multiple fabrics of the same Monitoring Domain to edit a fabric. You cannot choose different fabrics of multiple Monitoring Domains at the same time and edit their fabric components.
- **Delete Fabric** - You can delete all the fabrics associated with the Monitoring Domain of the selected fabric.
- **Upgrade Fabric** - You can select a Monitoring Domain or multiple Monitoring Domains to upgrade the fabric. You can upgrade the GigaVUE V Series Nodes using this option.

UCT-V

To view all the UCT-Vs associated with the available Monitoring Domains click the **UCT-V** tab.

The list view shows the following details:

- Monitoring Domain
- IP address
- Registration time
- Last heart beat time
- Mode
- Secure Tunnel Status
- Status
- Version

UCT-V Upgrade

To upload and upgrade the UCT-V packages, click the **UCT-V Upgrade** tab . UCT-V Upgrade drop-down includes Dashboard, Jobs, and Images options.

Dashboard

The Dashboard list view shows the following details:

- Overview Stages
- UCT-V Upgrade Stages
- Name
- IP address
- Mode
- Type
- Monitoring Domain
- Fetch
- Install
- Verify
- Upgrade Status
- Image Version
- Image Type
- Health
- Registration Mode

Jobs

You can view Immediate and scheduled tasks in the Jobs tab. The list view shows the following details:

Immediate tab	Scheduled tab
Shows the following details: <ul style="list-style-type: none"> ▪ Task Name ▪ Task Status ▪ Created Time ▪ Created By ▪ Start Time ▪ End Time 	Shows the following details: <ul style="list-style-type: none"> ▪ Task Name ▪ Task Status ▪ Created By ▪ Created Time ▪ Start Time ▪ End Time ▪ Scheduled Time ▪ Time Left

Images

The Images list view shows the following details:

- Image Name
- Version
- Image Type
- Build Number

- Size

Configure GigaVUE Fabric Components in GigaVUE-FM

GigaVUE Fabric Components can be deployed in the **AWS Fabric Launch Configuration** page. You can navigate to the **AWS Fabric Launch Configuration** page in any of the following ways:

- Create a Monitoring Domain and reach directly the **AWS Fabric Launch Configuration** page.
- Open **AWS Fabric Launch Configuration** page from the **Monitoring Domain** page. To launch the **AWS Fabric Launch Configuration** from the Monitoring Domain,
 1. Go to **Inventory > VIRTUAL > AWS**.
 2. Select **Actions > Deploy Fabric**.
The **AWS Fabric Launch Configuration** page appears.

Prerequisite:

Create a Monitoring Domain in GigaVUE-FM to establish connection between your AWS environment and GigaVUE-FM. For details, refer to [Create a Monitoring Domain](#).

In the **AWS Fabric Launch Configuration** page, you can configure the following fabric components:

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

In the **AWS Fabric Launch Configuration** page, select **Check Permissions** and validate whether you have the required permissions and then enter or select the required information as described in the following table:

Fields	Description
Centralized VPC	Alias of the centralized VPC in which the UCT-V Controllers, V Series Proxies and the GigaVUE V Series Nodes are launched.
EBS Volume Type	The Elastic Block Store (EBS) volume that you can attach to the fabric components. The available options are: <ul style="list-style-type: none"> ▪ gp2 (General Purpose SSD) ▪ io1 (Provisioned IOPS SSD) ▪ Standard (Magnetic)
Enable Encryption	Select Yes to enable encryption or select No to disable encryption. On selecting Yes to enable encryption, a KMS Key field appears. Enter the KMS key for the encryption.
SSH Key Pair	The SSH key pair for the GigaVUE fabric nodes. For more information on Key Pairs, refer to Key Pairs .
Management	The subnet that is used for communication between the controllers and the nodes, as well as to

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

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

SSH Key Pair

Availability Zone

Security Groups

Configure a V Series Proxy No

Configure UCT-V Controller

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



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

**UCT-V
Controller**



Controller Versions

Agent Tunnel Type

Agent CA

IP Address Type

Additional Subnets

Tags

Add

Version
gigamon-gigavu... ▾
✕

Instance Type
t3.micro

Number of Instances

Agent Tunnel Type
VXLAN ▾

Agent CA
uctv_ca ▾

IP Address Type

Private
 Public ⓘ
 Elastic

Additional Subnets

Add Subnet

Subnet 1
traffic1 ▾

Security Groups
test_sg ▾ ✕

Tags

Add

Key
Owner

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

Fields	Description
Controller Version(s)	<p>The UCT-V Controller version. If there are multiple versions of UCT-Vs deployed in the EC2 instances, then you must configure multiple versions of UCT-V Controllers that matches the version numbers of the UCT-Vs.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0; background-color: #e6f2ff;"> <p>NOTE: If the version of UCT-V Controllers do not match with UCT-Vs, GigaVUE-FM cannot detect the agents in the instances.</p> </div> <p>Click Add to add multiple versions of UCT-V Controllers: Under Controller Versions, select Add.</p> <ol style="list-style-type: none"> a. From the Version drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances. b. From the Instance Type drop-down list, select a size for the UCT-V Controller. c. In Number of Instances, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.
Agent Tunnel Type	<p>The type of tunnel used for sending the traffic from UCT-Vs to GigaVUE V Series Nodes. The options are GRE or VXLAN tunnels. If any Windows agents co-exist with Linux agents, you must select VXLAN.</p>
Agent CA (optional - This field is used when configuring secure tunnels)	<p>The Certificate Authority (CA) to use in the UCT-V Controller for connecting the tunnel.</p>
IP Address Type	<p>The IP address type. Select one of the following:</p> <ul style="list-style-type: none"> ■ Select Private if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the UCT-V Controller and

Fields	Description
	<p>GigaVUE-FM.</p> <ul style="list-style-type: none"> Select Public if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. Select Elastic if you want a static public IP address for your instance. Ensure to have the available elastic IP address in your VPC. <p>NOTE: The elastic IP address does not change when you stop or start the instance.</p>
Additional Subnet(s)	<p>(Optional) If there are UCT-Vs on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the UCT-V Controller can communicate with all the UCT-Vs.</p> <p>Select Add to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.</p>
Tag(s)	<p>(Optional) The key name and value that helps to identify the UCT-V Controller instances in your AWS environment. For example, you might have UCT-V Controllers deployed in a VPC. To identify the UCT-V Controllers you can provide a name that is easy to identify such as us-west-2-uctv-controllers.</p> <p>To add a tag,</p> <ol style="list-style-type: none"> Click Add tag. In the Key field, enter the key. For example, enter Name. In the Value field, enter the key value. For example, us-west-2-uctv-controllers.

Configure GigaVUE V Series Proxy

Select **Yes** for the Configure a GigaVUE V Series Proxy field. GigaVUE V Series Proxy is optional for the GigaVUE Cloud Suite for AWS. For details, refer to [GigaVUE V Series Proxy](#).

Enter or select the appropriate information as described in the following table for GigaVUE V Series Proxy Configuration.

Fields	Description
Version	GigaVUE V Series Proxy version.
Instance Type	<p>Instance type for the GigaVUE V Series Proxy. The recommended minimum instance type is t2.micro.</p> <p>You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.</p>
Number of Instances	Number of GigaVUE V Series Proxy to deploy in the monitoring domain.
Set Management Subnet	<p>Use the toggle button to select a management subnet.</p> <ul style="list-style-type: none"> Yes to use the management subnet that you selected previously. No to use another management subnet.
Set Security Groups	<p>Toggle option to Yes to set the security group that is created for the GigaVUE V Series Proxy. Refer to Security Group for more details.</p>

Fields	Description
IP Address Type	<p>Select one of the following IP address types:</p> <ul style="list-style-type: none"> ■ Select Private if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Proxy and GigaVUE-FM instances in the same network. ■ Select Public if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. ■ Select Elastic if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. <p>The elastic IP address does not change when you stop or start the instance.</p>
Additional Subnets	<p>(Optional) If GigaVUE V Series Nodes are on subnets that are not IP routable from the management subnet, must specify additional subnets so that the GigaVUE V Series Proxy can communicate with all the GigaVUE V Series Nodes.</p> <p>Select Add to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.</p>
Tags	<p>(Optional) The key name and value that helps to identify the GigaVUE V Series Proxy instances in your AWS environment.</p>

Configure GigaVUE V Series Node

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

Fields	Description
SSL Key	Select the SSL key from the drop-down.
Version	GigaVUE V Series Node version.
Instance Type	<p>The instance type for the GigaVUE V Series Node. Refer to Recommended Instance Types for AWS for more details on the recommended instance for GigaVUE V Series Node.</p> <p>You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.</p>
Volume Size	<p>The size of the storage disk. The default volume size is 8. The recommended volume size is 80.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>NOTE: When using Application Metadata Exporter, the minimum recommended Volume Size is 80GB.</p> </div>
IP Address Type	<p>Select one of the following IP address types:</p> <ul style="list-style-type: none"> ■ Select Private if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Controller and GigaVUE-FM instances in the same network. ■ Select Elastic if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. <p>The elastic IP address does not change when you stop or start the instance.</p>
Min Number of Instances	<p>The minimum number of GigaVUE V Series Nodes that must be deployed in the monitoring domain.</p> <p>The minimum number of instances must be 1. When 0 is entered, no GigaVUE V Series Node is</p>

Fields	Description
	<p>launched.</p> <p>NOTE: If the minimum number of instances is set as '0', then the nodes will be launched when a monitoring session is deployed if GigaVUE-FM discovers some targets to monitor.</p>
Max Number of Instances	The maximum number of GigaVUE V Series Nodes that can be deployed in the monitoring domain.
Data Subnets	<p>The subnet that receives the mirrored GRE or VXLAN tunnel traffic from the UCT-Vs.</p> <p>NOTE: Using the Tool Subnet checkbox you can indicate the subnets to be used by the GigaVUE V Series to egress the aggregated/manipulated traffic to the tools.</p>
Tags	<p>(Optional) The key name and value that helps to identify the GigaVUE V Series Node instances in your AWS environment. For example, you might have GigaVUE V Series Node deployed in many regions. To distinguish these GigaVUE V Series Node based on the regions, you can provide a name that is easy to identify such as us-west-2-vseries. To add a tag:</p> <ol style="list-style-type: none"> Select Add tag. In the Key field, enter the key. For example, enter Name. In the Value field, enter the key value. For example, us-west-2-vseries.

Select **Save** to save the AWS Fabric Launch Configuration.

To view the fabric launch configuration specification of a fabric component, select a GigaVUE V Series Node or Proxy, and a quick view of the Fabric Launch Configuration appears on the Monitoring Domain page.

What to do Next:

After deploying the GigaVUE Fabric Components in GigaVUE-FM, based on your chosen deployment option, perform any of the following actions:

Deployment Options	Reference Topics
Acquire traffic using UCT-V	Configure UCT-V
Acquire traffic using Traffic Mirroring or Customer Orchestrated Source	Configure Monitoring Session

Configure Role-Based Access for Third Party Orchestration

Prerequisites:

Configure the AWS credentials in GigaVUE-FM to monitor workloads across multiple AWS accounts within one Monitoring Domain. For details, refer to [Create AWS Credentials](#).

Role-Based Access for Third Party Orchestration

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

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

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

Role

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




NOTE:

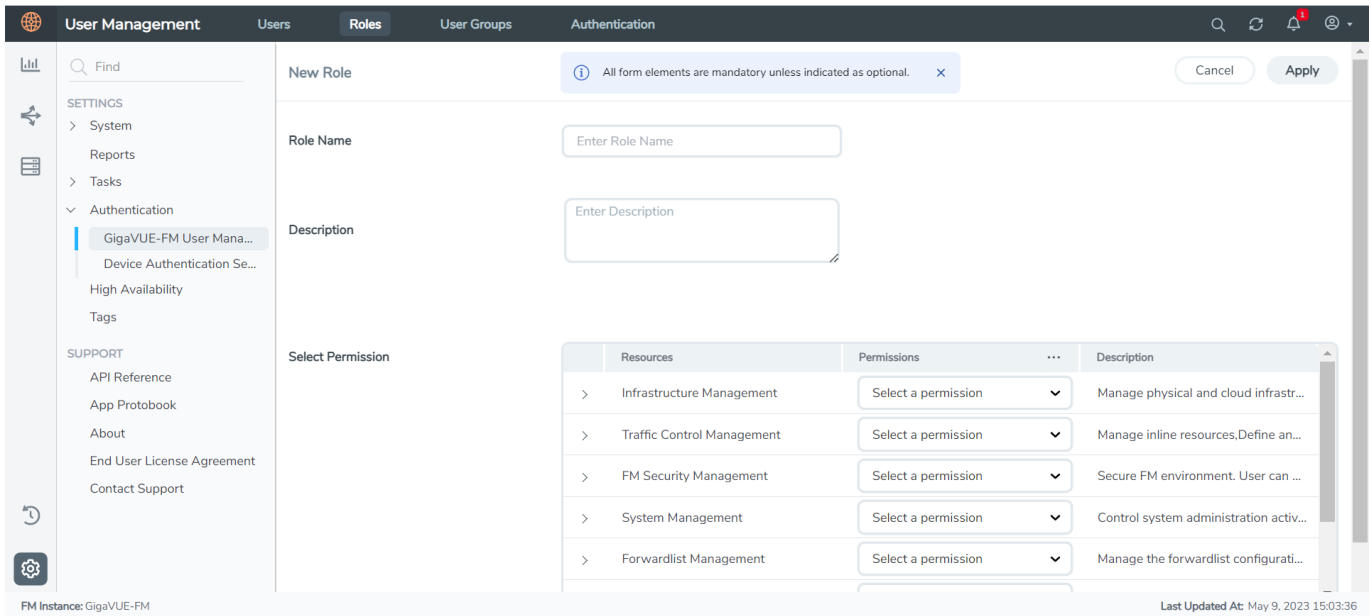
- A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.
- If you are using the default roles available in GigaVUE-FM, you must have the **fm_super_admin** role for deploying fabric components using Third Party Orchestration.

Create Custom Roles for Third Party Orchestration

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

To create a role,

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




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

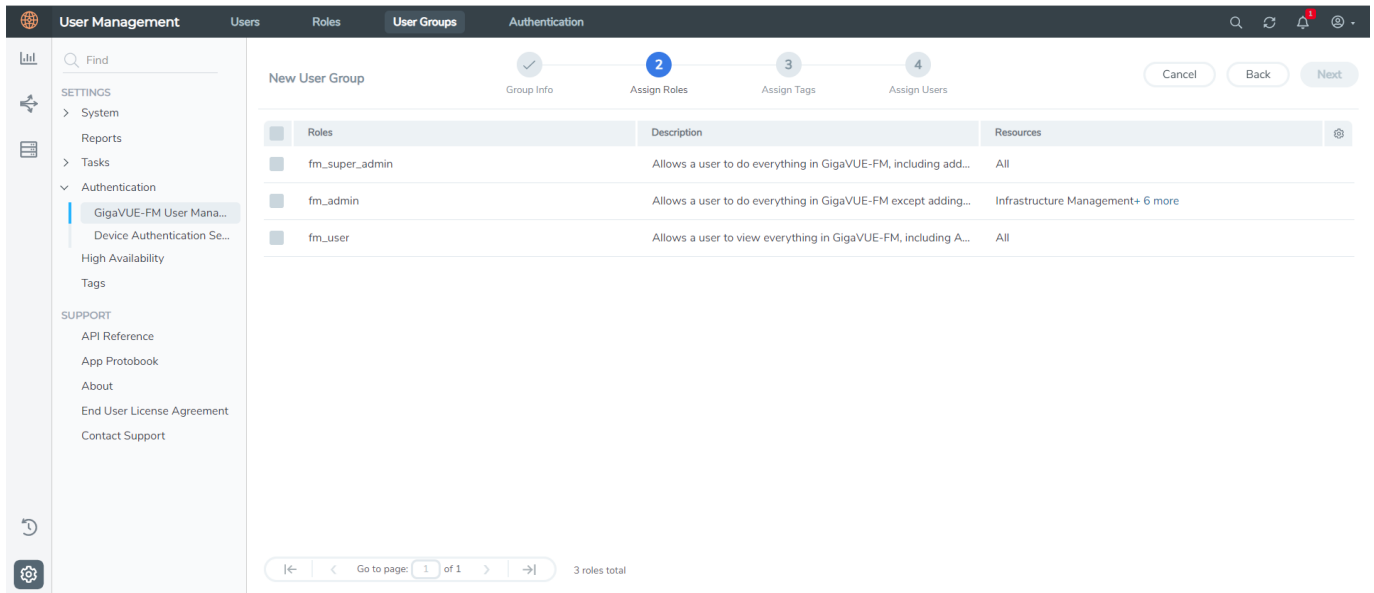
User Groups

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

Create User Groups in GigaVUE-FM for Third Party Orchestration

To create a new user group,

1. On the left navigation pane, click , and then select **Authentication > GigaVUE-FM User Management > User Groups**.
2. Select **New Group**.



3. In the Wizard, perform the following steps:
 - Select **Next** to progress forward and **Back** to navigate backward and change the details.
4. In the **Group Info** tab, enter the following details:
 - **Group Name**
 - **Description**
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration.
 - Select **Skip and Apply** to skip this step and proceed without adding users.

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

Select the ellipses to perform the following operations:

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

What to do Next:

Based on your deployment option, perform any of the following actions.

Deployment Options	Reference Topics
Deploying GigaVUE Fabric Components using GigaVUE-FM with Traffic Acquisition Method as VPC Mirroring or Customer Orchestrated Source	Create a Monitoring Domain
Deploying GigaVUE Fabric Components using GigaVUE-FM with Traffic Acquisition Method as UCT-V	Configure UCT-V

Users

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

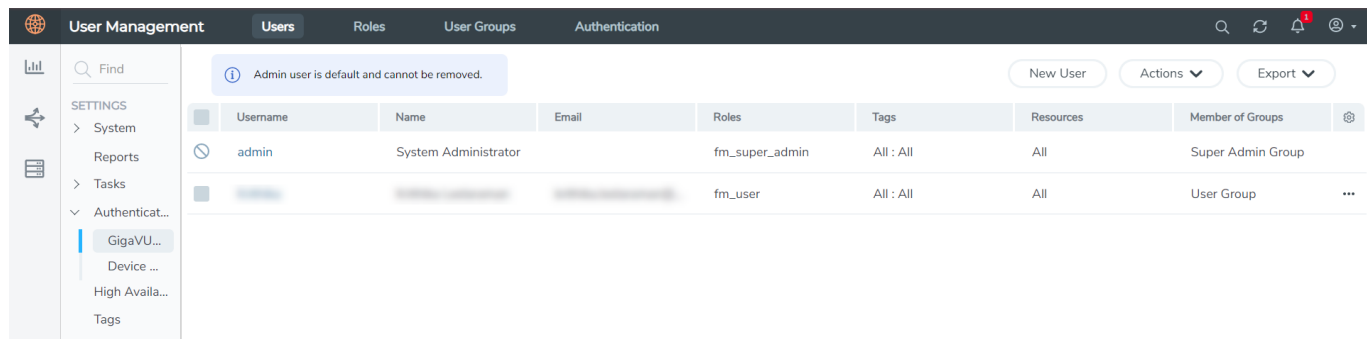
Add Users

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

To add users, perform the following steps:

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

The **User** page is displayed.



2. Select **New User**.

Add User
✕

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

Name

Username

Password

Confirm password

Email

User Group

Select User Group
▼
?

ℹ Your new password must contain:

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

Cancel
Ok

3. In the **Add User** wizard, enter details for the following:

- **Name:** Actual name of the user
- **Username:** User name configured in GigaVUE-FM
- **Email:** Email ID of the user
- **Password/Confirm Password:** Password for the user.
- **User Group:** Select the User Group that you want to associate the user with.

NOTE: GigaVUE-FM prompts for your password.

- a. Select **Ok** to save the configuration.

The new user is added to the summary list view.

The username and password created used in the registration data is used for deploying the fabric components.

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

You can use your own AWS orchestration system to deploy GigaVUE fabric components and use GigaVUE-FMM to configure the advanced features supported by these nodes. These nodes register themselves with GigaVUE-FM using the information provided by creating the Registration files on each component (/etc/gigamon-cloud.conf) . Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM. Health status of the registered nodes are determined by the heartbeat messages sent from the respective nodes.

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. For details, refer to [Install Custom Certificate](#).

Recommended Instance Type

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

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

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

- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- When using Traffic Mirroring as the traffic acquisition method, you must add a key and value when deploying the respective fabric components in the AWS orchestrator. Set the key to **GigamonNode** and any string to the value. The string cannot contain numbers and special characters.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in AWS. For details on how to add network interfaces when launching an instance, refer to the [Launch an instance using the Launch Instance Wizard](#) topic in Amazon EC2 Documentation.

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

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

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

To configure GigaVUE V Series Nodes and Proxy in AWS platform:

1. Before configuring GigaVUE fabric components through AWS, you must create a monitoring domain in GigaVUE-FM. For details, refer to [Create a Monitoring Domain](#).
2. In the **Monitoring Domain Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you are going to configure the fabric components in AWS Orchestrator.

The screenshot shows the 'Monitoring Domain Configuration' page in the AWS console. The page has a dark header with 'AWS > Monitoring Domain' and search, refresh, and notification icons. Below the header, there's a breadcrumb 'Monitoring Domain Configuration' and 'Save' and 'Cancel' buttons. The main content area lists several configuration items:

- Use V Series 2:** Toggle set to 'Yes'.
- Configure HTTP Proxy:** Toggle set to 'No'.
- Monitoring Domain:** Text input field with placeholder 'Enter a monitoring domain name'.
- Authentication Type:** Dropdown menu with 'EC2 Instance Role' selected.
- Region Name:** Dropdown menu with 'Region Name...' selected.
- Account:** Dropdown menu with 'Select Accounts...' selected.
- VPC:** Dropdown menu with 'Select VPCs...' selected.
- Traffic Acquisition Method:** Dropdown menu with 'G-vTAP' selected.
- Traffic Acquisition Tunnel MTU:** Text input field with '8951' entered.
- Use FM to Launch Fabric:** Toggle set to 'No'.

At the bottom left, there's a 'FM Instance: GigaVUE-FM' label.

3. In your AWS environment, you can deploy GigaVUE V Series Nodes or V Series proxy using the following methods:
 - [Register GigaVUE V Series Nodes or Proxy using User Data](#)
 - [Register GigaVUE V Series Node or Proxy using a configuration file](#)

Register GigaVUE V Series Nodes or Proxy using User Data

To register GigaVUE V Series Nodes or proxy using the user data in AWS GUI:

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

2. On the **Step 3: Configure Instance Details** tab, 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. You can also install custom certificates to GigaVUE V Series Node or Proxy, 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: <VPC 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/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: <VPC Name> user: <Username> password: <Password> remoteIP: <IP address of the GigaVUE-FM> or <IP address of the Proxy> remotePort: 443</pre> <p>NOTE: The minimum value for the authentication key encryption length provided during the key generation is 2048.</p>



- You can register your GigaVUE V Series Node directly with GigaVUE-FM or you can use GigaVUE V Series Proxy to register your GigaVUE V Series Node with GigaVUE-FM. If you wish to register GigaVUE V Series Node directly, enter the `remotePort` value as 443 or if you wish to deploy GigaVUE V Series Node using V Series proxy then, enter the `remotePort` value as 8891.
- You need to configure User and Password in the **User Management** page. For details, refer to [Configure Role-Based Access for Third Party Orchestration](#). Enter the Username and Password created in the **Add Users** Section.

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

Register GigaVUE V Series Node or Proxy using a configuration file

To register GigaVUE V Series Node or Proxy using a configuration file:

1. Log in to the GigaVUE V Series Node or Proxy.
2. Edit the local configuration file (`/etc/gigamon-cloud.conf`) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node or Proxy, refer to the below table for details:

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

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

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


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


```
$ sudo service vps restart
```

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

Configure UCT-V Controller in AWS

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

To configure UCT-V Controller in AWS platform,

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

The screenshot displays the 'Monitoring Domain Configuration' page in the AWS console. The page title is 'AWS > Monitoring Domain'. The breadcrumb is 'Monitoring Domain Configuration'. There are 'Save' and 'Cancel' buttons at the top right. The configuration options are as follows:

Configuration Option	Value
Use V Series 2	Yes
Configure HTTP Proxy	No
Monitoring Domain	Enter a monitoring domain name
Authentication Type	EC2 Instance Role
Region Name	Region Name...
Account	Select Accounts...
VPC	Select VPCs...
Traffic Acquisition Method	G-vTAP
Traffic Acquisition Tunnel MTU	8951
Use FM to Launch Fabric	No

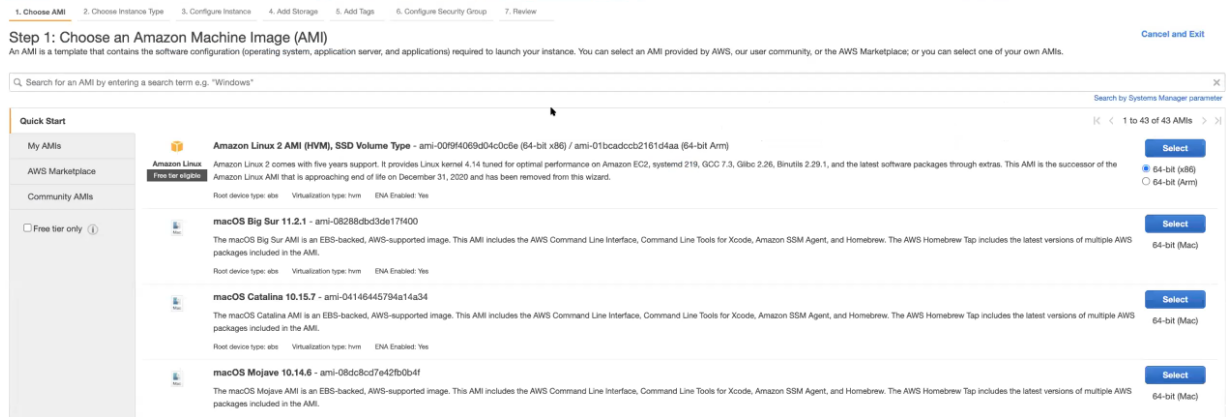
FM Instance: GigaVUE-FM

- In your AWS environment, launch the UCT-V Controller AMI instance using any of the following methods:
 - Register UCT-V Controller using User Data
 - Register UCT-V Controller using a configuration file

Register UCT-V Controller using User Data

To register UCT-V Controller using the user data in AWS GUI,


- On the Instances page of AWS EC2, select **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.



- b. 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: <VPC Name> user: <Username> password: <Password> remoteIP: <IP address of the GigaVUE-FM> sourceIP: <IP address of UCT-V Controller> (Optional Field) remotePort: 443</pre>
User data with custom certificate	<pre>#cloud-config write_files: - path: /etc/cntrl-cert.conf owner: root:root permissions: "0644" content: -----BEGIN CERTIFICATE----- <certificate content> -----END CERTIFICATE----- - path: /etc/cntrl-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> sourceIP: <IP address of UCT-V Controller> (Optional Field) remotePort: 443</pre>

Field	User Data
	<p>NOTE: The minimum value for the authentication key encryption length provided during the key generation is 2048.</p>

 • You must configure User and Password in the **User Management** page. For details, refer to [Configure Role-Based Access for Third Party Orchestration](#). Enter the Username and Password created in the **Add Users** Section.

- c. 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
<input type="checkbox"/> MD1					
	pubhraj-vpc				<input checked="" type="checkbox"/> Connected
		G-vTapController	34.219.250.141	1.7-304	<input checked="" type="checkbox"/> Ok
		Gigamon-VSeriesProxy-1	34.211.211.49	2.1.0	<input checked="" type="checkbox"/> Ok
		Gigamon-VSeriesNode-1	172.16.34.188	2.2.0	<input checked="" type="checkbox"/> Ok

Register UCT-V Controller using a configuration file

To register UCT-V Controller using a configuration file,

- Log in to the UCT-V Controller.
- Edit the local configuration file (`/etc/gigamon-cloud.conf`) and enter the following user data. You can also install custom certificates to UCT-V Controller. Refer to the below table for details.

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

- Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

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

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

```

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

```

Example netplan config:

```

network:
  version: 2
  renderer: networkd
  ethernets:
    ens3:
      addresses:
        -192.168.1.10/24
        -2001:db8:1::10/64
      nameservers:
        addresses:
          -8.8.8.8
          -2001:4860:4860::8888
      routes:
        -to: 0.0.0.0/0
          via: 192.168.1.1
            metric: 100
        -to: ::/0
          via: 2001:db8:1::1
            metric: 100

```

- d. Save the file.
- e. Restart the UCT-V Controller service.


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

The deployed UCT-V Controller registers with the GigaVUE-FM. After successful registration, the UCT-V Controller sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is

missing, the fabric component status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, tries to reach the UCT-V Controller. If that fails as well then GigaVUE-FM unregisters the UCT-V Controller and it is removed from GigaVUE-FM.

Configure UCT-V in AWS

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

NOTE: Deployment of UCT-Vs through a third-party orchestrator is supported on Linux and Windows platforms. For details, refer to [Linux UCT-V Installation](#) and [Windows UCT-V Installation](#).

To register UCT-V using a configuration file,

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



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

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



- If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:
`localInterface:<Interface to which UCT-V Controller is connected>`
- You must configure User and Password in the **User Management** page. For details, refer to [Configure Role-Based Access for Third Party Orchestration](#). 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.

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

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

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

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

Once the upgrade is complete, we recommend to change the password on the Users page. For details, refer to [Configure Role-Based Access for Third Party Orchestration](#).

Install UCT-V

You can install UCT-V on both Linux and Windows environments.

For more information on how to configure UCT-V, refer to the following topics:

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

Supported Operating Systems for UCT-V

Supported Operating System for UCT-V ¹ is 6.5.00, 6.6.00, 6.7.00, 6.8.00, 6.9.00

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

Operating System	Supported Versions
Ubuntu/Debian	Versions 16.04 through 24.04
CentOS	Versions 7.5 through 9.0
RHEL	Versions 7.5 through 9.4
Windows Server	Versions 2012 through 2022
Rocky OS	Versions 8.4 through 8.8

GigaVUE-FM version 6.9 supports UCT-V version 6.9 as well as (n-2) versions. For better compatibility, we recommend to use the latest version of UCT-V with GigaVUE-FM.

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

Linux UCT-V Installation

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

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

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

Single Network Interface Configuration

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

Example

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

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

Sample Configuration

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

Grant permission to monitor ingress and egress traffic at iface

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

Multiple Network Interface Configuration

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

Example

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

In the UCT-V configuration, you can configure:

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

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

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

Grant permission to monitor ingress and egress traffic at iface

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

Loopback Network Interface Configuration

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

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

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

Linux Network Firewall Requirements

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

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

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

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

Install Linux UCT-Vs

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

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

Prerequisites

UCT-V requires specific packages to function properly. Ensure you have the following packages installed before installing deb or rpm packages on your Linux VMs. If you have already installed UCT-V, use the `uctv-wizard pkg-install` command to install the packages.

- Python v3.x
- Python v3.x-pip
- Python modules
 - netifaces
 - urllib3
 - requests
- iproute-tc for RHEL and CentOS VMs

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

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

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

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

- [Linux UCT-V Installation](#)
- [Install Linux UCT-Vs using Manual Configuration](#)

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

Install Linux UCT-Vs using Installation Script

1. To install UCT-V from Ubuntu/Debian:

- a. Download the UCT-V6.9.00 Debian (.deb) package from the [Gigamon Customer Portal](#). For assistance, contact [Contact Technical Support](#).
- b. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue_uctv_6.9.00_amd64.deb
$ sudo dpkg -i gigamon-gigavue_uctv_6.9.00_amd64.deb
```

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

- a. Download the UCT-V6.9.00 RPM (.rpm) package from the [Gigamon Customer Portal](#). For assistance, contact [Contact Technical Support](#).
- b. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue_uctv_6.9.00_x86_64.rpm
```

```
$ sudo rpm -i gigamon-gigavue_uctv_6.9.00_x86_64.rpm
```

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

```
sudo uctv-wizard
```

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

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

Options	Use Command	Description
pre-check	sudo uctv-wizard pre-check	<p>Checks the status of the required packages and firewall requirements.</p> <ul style="list-style-type: none"> • If any package is missing, it displays an appropriate message with the missing package details. • If installation includes all the packages, it displays a success message indicating that UCT-V is ready for configuration.
pkg-install	sudo uctv-wizard pkg-install <div data-bbox="407 999 894 1241" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: The uctv-wizard install command requires access to a repository, either public (internet-based) or local, that hosts prerequisite packages for installation. If no repository is accessible, you must manually install the required packages. Refer to Install Linux UCT-Vs using Manual Configuration.</p> </div>	<p>Displays the missing package and version details. To proceed with the installation, you can choose between the following:</p> <p>If you wish to skip the prompts and proceed with the system update, enter your option as y. The console interface installs the missing packages and restarts the UCT-V service.</p> <p>Enter N if you wish to install it manually. For details, refer to Install Linux UCT-Vs using Manual Configuration</p>
configure	sudo uctv-wizard configure	<p>First, it checks for any existing configured file in the tmp directory. If available, UCT-V uses that configuration.</p> <p>If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination).</p> <p>You can add the required policy for the available port if a firewall is installed.</p> <p>If you wish to skip the prompts to add the required firewall policy, enter your option as y. The console interface will add the firewall rules automatically.</p>

Options	Use Command	Description
		Enter N if you wish to configure manually. For details, refer to Install Linux UCT-Vs using Manual Configuration .
uninstall	<code>sudo uctv-wizard uninstall</code>	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

**Notes:**

- Use the command below to view all the log messages generated from uctv-wizard. These log messages are stored at `/var/log/uctv-installation.log`
`sudo vi /var/log/uctv-installation.log`
- Use the command below to know the usage descriptions for the individual operations.
`sudo uctv-wizard help`

Linux UCT-V Installation Scenarios

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

Install Linux UCT-Vs using Manual Configuration

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

Install UCT-V from Ubuntu/Debian Package

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

```
sudo apt-get update
sudo apt install python3-netifaces
curl https://bootstrap.pypa.io/pip/3.5/get-pip.py -o get-pip.py
/usr/bin/python3.5 get-pip.py
sudo /usr/bin/python3.5 -m pip uninstall requests
sudo /usr/bin/python3.5 -m pip install requests==2.22.
```

To install from a Debian package:

1. Download the UCT-V6.9.00 Debian (.deb) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Copy this package to your instance.
3. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue_uctv_6.9.00_amd64.deb
$ sudo dpkg -i gigamon-gigavue_uctv_6.9.00_amd64.deb
```
4. Modify the file `/etc/uctv/uctv.conf` to configure and register the source and destination interfaces. The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

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

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

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

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

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

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

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

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

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

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

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

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

5. Save the file.

- Restart the UCT-V service.

```
$ sudo service uctv restart
```

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

```
$ sudo service uctv status
```

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



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

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

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

- Download the UCT-V6.9.00 RPM (.rpm) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
- Copy this package to your instance.
- Install the package with root privileges. For example:

```
$ ls gigamon-gigavue_uctv_6.9.00_x86_64.rpm
$ sudo rpm -i gigamon-gigavue_uctv_6.9.00_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: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

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

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

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

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

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

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

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

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

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

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

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

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


```
$ sudo service uctv restart
```

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

```
$ sudo service uctv status
```

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

What to do Next:

After installing UCT-V, you must create Monitoring Session. Refer to [Configure Monitoring Session](#) for detailed instructions on how to create a Monitoring Session, tunnel end points, add applications to the Monitoring Session, and deploy a Monitoring Session.

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.

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

- [Windows Network Firewall Requirements](#)
- [Install Windows UCT-Vs](#)
- [Register Windows UCT-V](#)
- [Create Images with UCT-V Installed](#)

Windows Network Firewall Requirements

If Network Firewall requirements or Security Groups are configured in your environment, you must open the following ports for the virtual machine. Refer to [Network Firewall Requirement for GigaVUE Cloud Suite](#) for more details on the firewall requirements or security groups required for your environment.



Notes:

- After installing UCT-V, manually add the following TCP ports for Windows Firewall:
 - Port 8301 (Inbound)
 - Port 8300 (Outbound)
- You can configure the ports using the following PowerShell commands. Make sure to run PowerShell as **Administrator**:
 1. `New-NetFirewallRule -DisplayName "GigaVUE UCT-V (http01_challenge_port)" -Group "Virtual Tap" -Direction "Inbound" -Program "C:\Program Files (x86)\Uctv\step.exe" -LocalPort "8301" -Protocol "TCP" -Action`
 2. `New-NetFirewallRule -DisplayName "GigaVUE UCT-V (pki_ra_port)" -Group "Virtual Tap" -Direction "Outbound" -Program "C:\Program Files (x86)\Uctv\uctvd.exe" -LocalPort "8300" -Protocol "TCP" -Action Allow`

Install Windows UCT-Vs

Rules and Notes:

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

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

- [Install Windows UCT-Vs using Installation Script](#)
- [Install Windows UCT-Vs using Manual Configuration](#)



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

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

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

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

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V 6.9.00 MSI package from the [Gigamon Customer Portal](#). For assistance, contact [Contact Technical Support](#).
2. Install the downloaded MSI package as **Administrator**, and the UCT-V service starts automatically.

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

```
uctv-wizard
```

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

Options	Use Command	Description
pre-check	uctv-wizard pre-check	<p>Checks the network adapter properties and firewall requirements. It notifies the user if the network adapter's send buffer size is smaller than the required size for the Windows UCT-V and if any firewall rules need to be added.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: It is recommended to Increase the send buffer size of network adapters to 128 MB during the UCT-V installation to optimize performance and minimize traffic disruption.</p> </div>
adapter-setup	uctv-wizard adapter-setup	<p>Checks the compatible network adapters, increases the send buffer size and restarts the service. Before changing the buffer size, the existing configuration is saved as a backup.</p> <p>You can choose between the following:</p> <ul style="list-style-type: none"> • If you wish to skip the prompts for changing the buffer size of compatible network adapters, enter the option as y. • Enter N if you wish to set it up manually. Refer to the Install Windows UCT-Vs using Manual Configuration section for more details.

Options	Use Command	Description
adapter-restore	uctv-wizard adapter-restore	<p>Using this command, you can restore the backup copy of the network adapter buffer size configuration saved in the in the uctv-wizard adapter-setup step.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>NOTE: You need to manually restart the network adapters for changes to take effect immediately.</p> </div> <p>You can choose between the following:</p> <ul style="list-style-type: none"> • If you wish to skip the prompts for restoring the buffer size of the compatible network adapters, enter the option as y. • Enter N if you wish to restore it manually. Refer to the Install Windows UCT-Vs using Manual Configuration section for more details.
configure	uctv-wizard configure	<p>First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the C:\Users\<username>\AppData\Local location). If available, UCT-V will use that configuration.</p> <p>If unavailable, UCT-V will automatically add the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination).</p> <p>You can add the required policy for the available port if a firewall is installed.</p> <ul style="list-style-type: none"> • If you wish to skip the prompts to add the required firewall policy, enter your option as y. The console interface will add the firewall rules automatically. • Enter N if you wish to configure manually. Refer to the Install Windows UCT-Vs using Manual Configuration section for more details.
uninstall	uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.



Notes:

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

```
uctv-wizard help
```

Windows UCT-V Installation Scenarios

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

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V 6.9.00 MSI package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Install the downloaded MSI package as **Administrator** and the UCT-V service starts automatically.

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

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



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

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

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

For IPv4:

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

For IPv6:

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

```
2001:db8:abcd:ef01::/64 mirror-dst
```

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

For IPv4:

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

```
192.168.2.0/24 mirror-dst
```

For IPv6:

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

```
2001:db8:abcd:ef02::/64 mirror-src-egress
```

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

- Save the file.

5. Restart the Windows UCT-V using one of the following actions:
 - Run 'sc stop uctv' and 'sc start uctv' from the command prompt.
 - Restart the UCT-V from the Windows Task Manager.

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

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

Register Windows UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. It is used once and does not need to be maintained.

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

1. **GigaVUE-FM Orchestration:** Refer to the following steps:
 - a. Log in to the UCT-V.
 - b. Create a local configuration file and enter the following user data.
C:\ProgramData\uctv\gigamon-cloud.conf is the local configuration file in Windows platform.

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

- c. Restart the UCT-V service.

Windows platform: Restart from the Task Manager Service

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

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

Create Images with UCT-V Installed

If you want to avoid downloading and installing the UCT-Vs every time there is a new VM to be monitored, you can save the UCT-V running on a VM as a private image. When a new VM is launched that contains the UCT-V, GigaVUE-FM automatically detects the new VM and updates the number of monitoring VMs in the monitoring session.

What to do Next:

After installing UCT-V, you must create Monitoring Session. For detailed instructions on how to create a Monitoring Session, tunnel end points, add applications to the Monitoring Session, and deploy a Monitoring Session, refer to [Configure Monitoring Session](#).

Uninstall UCT-V

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

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

```
sudo uctv-wizard uninstall
```

- For Windows, to uninstall the UCT-V in the MSI package, use the following command:

```
CMD uctv-wizard uninstall
```

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

Upgrade or Reinstall UCT-V

You can upgrade UCT-V in your virtual machine in two ways.

- [Upgrade UCT-V manually on Virtual Machine](#)
- [Upgrade UCT-V through GigaVUE-FM](#)

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

Upgrade UCT-V manually on Virtual Machine

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

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

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

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

Upgrade UCT-V through GigaVUE-FM

Upgrading UCT-V manually involves a series of steps to uninstall, install, and restart the service again. This method is complicated when you need to upgrade UCT-Vs for a large number of VMs.

However, you can upgrade UCT-V in the workload VM without any hands-on involvement through GigaVUE-FM. For more details and instructions, refer to the following sections:

1. [Upload the UCT-V Images](#)
2. [Upgrade the UCT-V](#)

Rules and Notes:

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

Upload the UCT-V Images

Follow these steps to upload UCT-V image files in GigaVUE-FM:

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

From the **Upload Internal Image Files** wizard, select **Choose File**, upload the UCT-V files from your local, and select **Ok**.



Notes:

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

4. Once completed, the uploaded UCT-V images is listed in the **Images** page.

In the **Images** page, select **Filter** to filter the images based on Image Name, Version, and Image Type. You can delete one or multiple images. Select the required images and click **Delete** or **Delete All** from the Actions drop-down menu. You can only delete those image files that are not associated with any tasks created for the upgrade process.

Upgrade the UCT-V

Follow these steps to upgrade UCT-V in GigaVUE-FM:

1. In the **UCT-V Upgrade** drop-down menu, select **Dashboard** to view the UCT-V upgrade landing page.
2. In the Dashboard page, verify the upgrade status of individual UCT-Vs and the stages of the upgrade process (Fetch, Install, Verify). The page also displays the overall progress of the upgrade.
3. Select the required UCT-Vs and from the **Actions** drop-down menu, select **Upgrade. UCT-V Upgrade task** page appears.
4. Enter the task name.
5. In the **Image Version** drop-down menu, select the required version you want to upgrade to from the list of available image versions.
6. Select the option to upgrade as immediately or schedule a time for the upgrade to happen.
7. Select the required option in the **Time Selection** field. If you prefer to schedule the upgrade, enter the choice of your date and time in the respective fields.

NOTE: You cannot schedule upgrade for a time in the past.

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



Note:

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



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



Notes:

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

You can view the different stages of the upgrade process in UCT-V Upgrade Dashboard page. Each stage

is marked with  if it is successful and  in case of failure. If the upgrade is successful, GigaVUE-FM updates the upgrade status as **Success** for the selected UCT-V.



Notes:

- The default wait time for the upgrade status to get updated is 15 minutes.
- In case of failure, you can upgrade the failed instance manually.

Configure Secure Tunnel (AWS)

The Secure tunnel can be configured on:

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

Preencrypted Traffic

You can send the preencrypted traffic through a secure tunnel. When secure tunnels for Preencryption is enabled, packets are framed and sent in PCAPng format.

When you enable the secure tunnel option for mirrored traffic and Preencryption traffic, two TLS secure tunnel sessions are created.

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

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

Mirrored Traffic

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

Refer to the following sections for Secure Tunnel Configuration:

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

Prerequisites

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

Notes

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

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

To configure a secure tunnel in UCT-V, you must configure one end of the tunnel to the UCT-V and the other end to GigaVUE V Series node. You must configure the CA certificates in UCT-V and the 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 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. In the Alias field, enter the CA name. 4. 5. <table border="1"> <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> 6. 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 an SSL Key	<p>You must add an SSL key to GigaVUE V Series node. To add an SSL Key, follow the steps in the section Upload SSL Keys.</p>						

S. No	Task	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. Go to Traffic > Virtual > Orchestrated Flows > Select your cloud platform. 2. Select a Monitoring Session from the Monitoring Sessions list view on the left side of the screen and click the TRAFFIC ACQUISITION tab. 3. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and precrypted traffic. <p>NOTE: When GigaVUE V Series Node is upgraded or deployed to 6.5, all the existing Monitoring Sessions will be redeployed, and individual TLS Tunnel End Points are created for each UCT-V.</p>
4.	Select the SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM.	<p>You must select the added SSL Key in GigaVUE V Series Node Key while creating a Monitoring Domain configuring the fabric components in GigaVUE-FM. To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM</p> <p>If the existing Monitoring Domain does not have an SSL key, you can add it by following the given steps:</p> <ol style="list-style-type: none"> 1. Select the Monitoring Domain for which you want to add the SSL key. 2. Click the Actions drop down list and select Edit SSL Configuration. An Edit SSL Configuration window appears. 3. Select the CA in the UCT-V Agent Tunnel CA drop down list. 4. Select the SSL key in the V Series Node SSL key drop down list. 5. Click Save.
5.	Select the CA certificate while creating the monitoring domain configuring the fabric components in GigaVUE-FM.	<p>You should select the added Certificate Authority (CA) in UCT-V Controller. To select the CA certificate, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM</p>

Configure Secure Tunnel between GigaVUE V Series Nodes

You can create secure tunnel:


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

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


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

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

S. No	Task	Refer to						
1.	Upload a Certificate Authority (CA) Certificate	<p>You must upload a Custom Certificate to UCT-V Controller to establish a connection between the GigaVUE V Series node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> Go to Inventory > Resources > Security > CA List. Click Add, to add a new Certificate Authority. The Add Certificate Authority page appears. Enter or select the following information. <table border="1" data-bbox="862 663 1474 861"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>Alias name of the CA.</td> </tr> <tr> <td>File Upload</td> <td>Choose the certificate from the desired location.</td> </tr> </tbody> </table> Click Save. 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 an SSL Key	<p>You must add an SSL key to GigaVUE V Series Node. To add an SSL Key, follow the steps in the section Upload SSL Keys.</p>						
3.	Creating a secure tunnel between UCT-V and the first GigaVUE V Series Node.	<p>You should enable the secure tunnel feature to establish a connection between the UCT-V and the first GigaVUE V Series Node. To enable the secure tunnel feature follow these steps:</p> <ol style="list-style-type: none"> Go to Traffic > Virtual > Orchestrated Flows > Select your cloud platform. Select a Monitoring Session from the Monitoring Sessions list view on the left side of the screen and click the TRAFFIC ACQUISITION tab. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and preencrypted traffic. 						
4.	Select the added SSL Key while creating a Monitoring Domain	<p>Select the SSL Key added in the Step 2 while creating a Monitoring Domain and configuring the fabric components in GigaVUE-FM for the first GigaVUE V Series Node.</p> <p>You must select the SSL Key added in the first GigaVUE V Series Node.</p> <p>To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM.</p>						
5.	Select the added CA certificate while creating the monitoring domain	<p>You should select the added Certificate Authority (CA) in UCT-V Controller. To select the CA certificate, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM.</p>						

S. No	Task	Refer to						
6	Create an Egress tunnel from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session.	<p>You must create a tunnel for traffic to flow out from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to Configure Monitoring Session to know about monitoring session.</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 on an existing Monitoring Session, navigate to the TRAFFIC PROCESSING tab. The GigaVUE-FM Monitoring Session canvas page appears. 2. In the canvas, click the  icon on the left side of the page to view the traffic processing elements. Select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears. 3. On the New Tunnel quick view, enter or select the required information as described in the following table: <table border="1" data-bbox="784 905 1471 1073"> <thead> <tr> <th data-bbox="784 905 954 982">Field</th> <th data-bbox="954 905 1471 982">Action</th> </tr> </thead> <tbody> <tr> <td data-bbox="784 982 954 1026">Alias</td> <td data-bbox="954 982 1471 1026">The name of the tunnel endpoint.</td> </tr> <tr> <td data-bbox="784 1026 954 1073">Description</td> <td data-bbox="954 1026 1471 1073">The description of the tunnel endpoint.</td> </tr> </tbody> </table>	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.
Field	Action							
Alias	The name of the tunnel endpoint.							
Description	The description of the tunnel endpoint.							

S. No	Task	Refer to								
		<table border="1"> <thead> <tr> <th data-bbox="781 262 954 338">Field</th> <th data-bbox="954 262 1471 338">Action</th> </tr> </thead> <tbody> <tr> <td data-bbox="781 338 954 413">Type</td> <td data-bbox="954 338 1471 413">Select TLS-PCAPNG for creating egress secure tunnel</td> </tr> <tr> <td data-bbox="781 413 954 1423">Traffic Direction</td> <td data-bbox="954 413 1471 1423"> Choose Out (Encapsulation) for creating an egress tunnel from the GigaVUE 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 Version 1.3. 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="781 1423 954 1499">Remote Tunnel IP</td> <td data-bbox="954 1423 1471 1499">Enter the interface IP address of the second GigaVUE V Series Node (Destination IP).</td> </tr> </tbody> </table> <p data-bbox="781 1514 954 1543">4. Click Save.</p>	Field	Action	Type	Select TLS-PCAPNG for creating egress secure tunnel	Traffic Direction	Choose Out (Encapsulation) for creating an egress tunnel from the GigaVUE 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 Version 1.3. o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments. o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments. 	Remote Tunnel IP	Enter the interface IP address of the second GigaVUE V Series Node (Destination IP).
Field	Action									
Type	Select TLS-PCAPNG for creating egress secure tunnel									
Traffic Direction	Choose Out (Encapsulation) for creating an egress tunnel from the GigaVUE 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 Version 1.3. o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments. o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments. 									
Remote Tunnel IP	Enter the interface IP address of the second GigaVUE V Series Node (Destination IP).									
7.	Select the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in the second GigaVUE V Series Node.	You must select the added SSL Key in GigaVUE V Series Node. To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM .								
8	Create an ingress tunnel in the second GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session for the second GigaVUE V Series Node.	You must create a ingress tunnel for traffic to flow in from GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to Configure Monitoring Session to know about monitoring session.								

S. No	Task	Refer to														
		<p>To create the ingress tunnel, follow these steps:</p> <ol style="list-style-type: none"> After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the TRAFFIC PROCESSING tab. The GigaVUE-FM Monitoring Session canvas page appears. In the canvas, click the  icon on the left side of the page to view the traffic processing elements. Select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears. On the New Tunnel quick view, enter or select the required information as described in the following table: <table border="1" data-bbox="784 724 1471 1482"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Alias</td> <td>The name of the tunnel endpoint.</td> </tr> <tr> <td>Description</td> <td>The description of the tunnel endpoint.</td> </tr> <tr> <td>Type</td> <td>Select TLS-PCAPNG for creating egress secure tunnel. NOTE: If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.</td> </tr> <tr> <td>Traffic Direction</td> <td>Choose in (Decapsulation) for creating an ingress tunnel that receives traffic from the first GigaVUE V Series Node. Select or enter the values as described in Step 6:</td> </tr> <tr> <td>IP Version</td> <td>The version of the Internet Protocol. IPv4 and IPv6 are supported.</td> </tr> <tr> <td>Remote Tunnel IP</td> <td>Enter the interface IP address of the first GigaVUE V Series Node (Destination IP).</td> </tr> </tbody> </table> Click Save. 	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.	Type	Select TLS-PCAPNG for creating egress secure tunnel. NOTE: If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.	Traffic Direction	Choose in (Decapsulation) for creating an ingress tunnel that receives traffic from the first GigaVUE V Series Node. Select or enter the values as described in Step 6:	IP Version	The version of the Internet Protocol. IPv4 and IPv6 are supported.	Remote Tunnel IP	Enter the interface IP address of the first GigaVUE V Series Node (Destination IP).
Field	Action															
Alias	The name of the tunnel endpoint.															
Description	The description of the tunnel endpoint.															
Type	Select TLS-PCAPNG for creating egress secure tunnel. NOTE: If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.															
Traffic Direction	Choose in (Decapsulation) for creating an ingress tunnel that receives traffic from the first GigaVUE V Series Node. Select or enter the values as described in Step 6:															
IP Version	The version of the Internet Protocol. IPv4 and IPv6 are supported.															
Remote Tunnel IP	Enter the interface IP address of the first GigaVUE V Series Node (Destination IP).															

For more information, refer to [Secure Tunnels](#).

Viewing Status of Secure Tunnel

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

To verify the status of secure tunnel:

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

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

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

Create Prefiltering Policy Template

To create a prefiltering policy template,

1. Go to **Traffic > Resources > Prefiltering** and select **UCT-V**.
2. Select **New**.
3. In the **Template Name** field, enter the name of the template,
4. In the **Rule Name** field, enter the name of a rule.
5. Select one of the following options:
 - **Pass:** Allows the traffic.
 - **Drop:** Blocks the traffic..

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

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

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

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

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

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

- L3
- L4

9. Select one of the following options **Filter Name**:

- ip4Src
- ip4Dst
- ip6Src
- ip6Dst
- Proto: Applies to both ipv4 and ipv6.

10. Select one of the following options for **Filter Relation**:

- Not Equal to
- Equal to

11. In the **Value** field, enter the source or destination port.

12. Select **Save**.

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

To enable prefiltering, refer to [Monitoring Session Options](#).

Create Precryption Template for UCT-V

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

Rules and Notes:

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

For details, refer to the section:

- [Create Precryption Template for Filtering based on Applications](#)
- [Create Precryption Template for Filtering based on L3-L4 details](#)

Create Precryption Template for Filtering based on Applications

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

To create,

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

The added applications are displayed in the **APPLICATION** tab.

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

Create Precryption Template for Filtering based on L3-L4 details

To create,

1. Go to **Traffic > Resources > Precryption**. The **Precryption Policies** page appears.
2. Select the **L3-L4** tab.
3. Select **Add**.
4. In the **Template** field, enter the name of the precryption template.

5. From the **Priority** drop-down list, select the value of the priority based on which you prioritize the rules for filtering.
 - 1: Select the value as 1 to pass or drop a rule in top priority.
 - 2-8: Similarly, you can select the value as 2, 3, 4 upto 8, where 8 is for setting a rule with the least priority.
 - Drop rules are added based on the priority and, then pass rules are added.
6. In the **Rule Name** field, enter the name of the rule.
7. From the **Traffic Action** drop-down list, select how the traffic is handled.
 - Pass: Passes the traffic.
 - Drop: Drops the traffic.

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

8. From the **Direction** drop-down list, select the direction of traffic.
 - Bi-Directional: Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
 - Ingress: Filters the traffic that flows in.
 - Egress: Filters the traffic that flows out.
9. From the **L3/L4 Layer** drop-down list, select **L3** or **L4**.

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

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

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

13. Select **Save**.

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

The template is successfully created. To enable Precryption, refer to [Configure Monitoring Session Options \(AWS\)](#) section.

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

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

Configure Monitoring Session

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

Refer to the following sections for details:

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

Create a Monitoring Session (AWS)

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

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

Target Instance

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

You can create multiple Monitoring Sessions within one Monitoring Domain.

To create a new Monitoring Session:

1. Go to Traffic > Virtual > Orchestrated Flows and select your cloud platform.
The **Monitoring Session** page appears.
2. Select New Monitoring Session to open the New Monitoring Session configuration page.
3. In the configuration page, perform the following:
 - In the **Alias** field, enter the name of the Monitoring Session.
 - From the **Monitoring Domain** drop-down list, select the desired Monitoring Domain or select **Create New** to create a Monitoring Domain.

For details, refer to the Create a Monitoring Domain section in the respective cloud guides.

- From the **Connections** drop-down list, select the required connections to include as part of the Monitoring Domain.
4. Select **Save**.
The Monitoring Session Overview page appears.



Monitoring Session Page (AWS)

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

Tab	Description
Overview	You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can also view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can filter the statistics based on the elements associated with the Monitoring Session. For more information, refer to View Monitoring Session Statistics (AWS)
Sources	Displays the sources and target details monitored by the Monitoring Session. You can view and edit the connection details of the Monitoring Session. You can view the deployment status, number of targets, and targets source health. NOTE: In the case of OVS Mirroring, the Sources tab also displays the Hypervisor details along with the Instances.
Traffic Acquisition	You can enable or disable Prefiltering, Precryption, and Secure Tunnel here. You can also create a prefiltering template and apply it to the Monitoring Session. Refer to Configure Monitoring Session Options (AWS) for more detailed information. NOTE: Traffic Acquisition is only applicable for Monitoring Domain created with UCT-V as Acquisition method.
Traffic Processing	You can view, add, and configure applications, tunnel endpoints, raw endpoints, and maps. You can view the statistical data for individual applications and also apply threshold template, enable user defined applications, and enable or disable distributed De-duplication. Refer to Configure Monitoring Session Options (AWS) for more detailed information.
V Series Nodes	You can view the V Series nodes associated with the Monitoring Session. In the split view, you can view details such as name of the V Series Node, health status, deployment status, Host VPC, version, and Management IP. You can also change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping (AWS) section for details.

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

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

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

- Delete
- Deploy
- Undeploy

Configure Monitoring Session Options (AWS)

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

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

Traffic Acquisition

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

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

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

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

Enable Prefiltering

To enable Prefiltering, follow the steps given below:

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

Enable Precryption

Rules and Notes

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

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

To enable Precryption, follow the steps given below:

1. In the Monitoring Session **TRAFFIC ACQUISITION** page, click **Precription** tab.
2. Enable the **Precription** toggle button. Refer to [Precription™](#) topic for more details on Precription.
3. You can apply Precription to a few selective components based on the traffic:

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

Applications:

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

L3-L4

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

Validate Precription connection

To validate the Precription connection, follow these steps:

- Navigate to the **Monitoring Session** dashboard and select the Precription option that should show **yes**,
- Select **Status**, to view the rules configured.

Limitations

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

Traffic processing

To navigate to **TRAFFIC PROCESSING** tab, follow these steps:

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

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

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

Apply Threshold Template

To apply threshold, follow these steps:

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

Enable User Defined Applications

To enable user defined application, follow these steps:

1. In the Monitoring Session **TRAFFIC PROCESSING** page, select **User Defined Applications** under **Options** menu.
2. Enable the **User-defined Applications** toggle button. For details, refer to [User Defined Application](#) section in the GigaVUE V Series Applications Guide.

Enable Distributed De-duplication

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



Notes:

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

Create Ingress and Egress Tunnels (AWS)

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

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


Create a new tunnel endpoint

To create,

1. Perform one of the following and navigate to the **TRAFFIC PROCESSING** tab:

- Create a new monitoring session
- Select **Actions > Edit** on an existing monitoring session.

The GigaVUE-FM canvas appears.

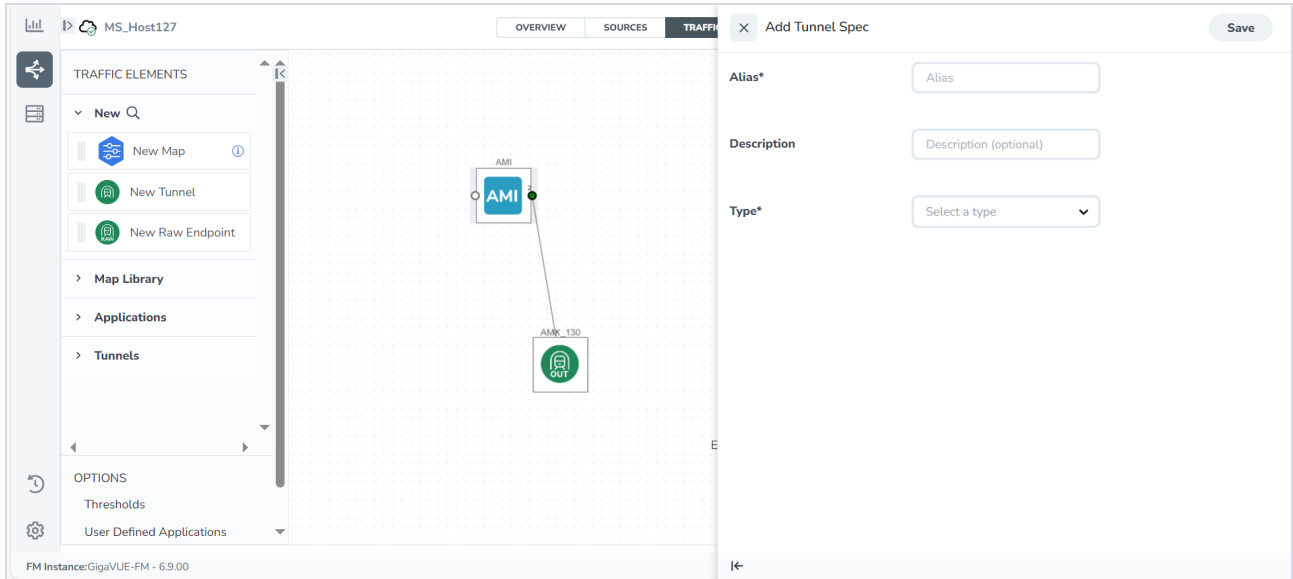
2. On the left pane of the canvas, select the  icon to view the traffic processing elements.
3. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace.

The **Add Tunnel Spec** quick view appears.

4. Enter the **Alias**, **Description**, and **Type** details.

For details, refer to [Details - Add Tunnel Specifications](#) table.

5. Select **Save**.



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

Apply a threshold template to Tunnel End Points

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

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

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

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

Details - Add Tunnel Specifications

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

Field	Description	
Alias	The name of the tunnel endpoint.	
Description	The description of the tunnel endpoint.	
Admin State This option appears only after the Monitoring session deployment.	Use this option to send or stop the traffic from GigaVUE-FM to the egress tunnel endpoint. Admin State is enabled by default. You can use this option to stop sending traffic to unreachable or down tools. Each egress tunnel configured on the GigaVUE V Series Node has an administrative state that enables GigaVUE-FM to halt the tunnel's traffic flow. GigaVUE-FM only disable the tunnels when it receives a notification via REST API indicating that a tool or group of tools is down. This option is not supported for TLS-PCAPNG tunnels.	
Type	The type of the tunnel. Select from the options below to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE.	
VXLAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. In the scenario where secure tunnels need to be established between a GigaVUE V Series Node and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to configure secure tunnels on your physical device conveniently. For details, refer to Secure Tunnels section.		
In	Choose In (Decapsulation) for creating an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value that is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	The port used to establish the connection to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port used to establish the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose Out (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node to the destination endpoint.	
	Remote Tunnel IP	For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63

Field	Description	
		being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
UDPGRE		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose In (Decapsulation) for creating an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UDPGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . Refer to the Secure Tunnels section.		
In	Choose In (Decapsulation) to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UDPGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.

Field	Description	
Out	Choose Out (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint.	
	Remote Tunnel IP	For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value helps to identify packets that belong to the same flow. A flow is a sequence of packets treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
ERSPAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device. Refer to the Secure Tunnels section.		

Field	Description	
In	IP Version	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

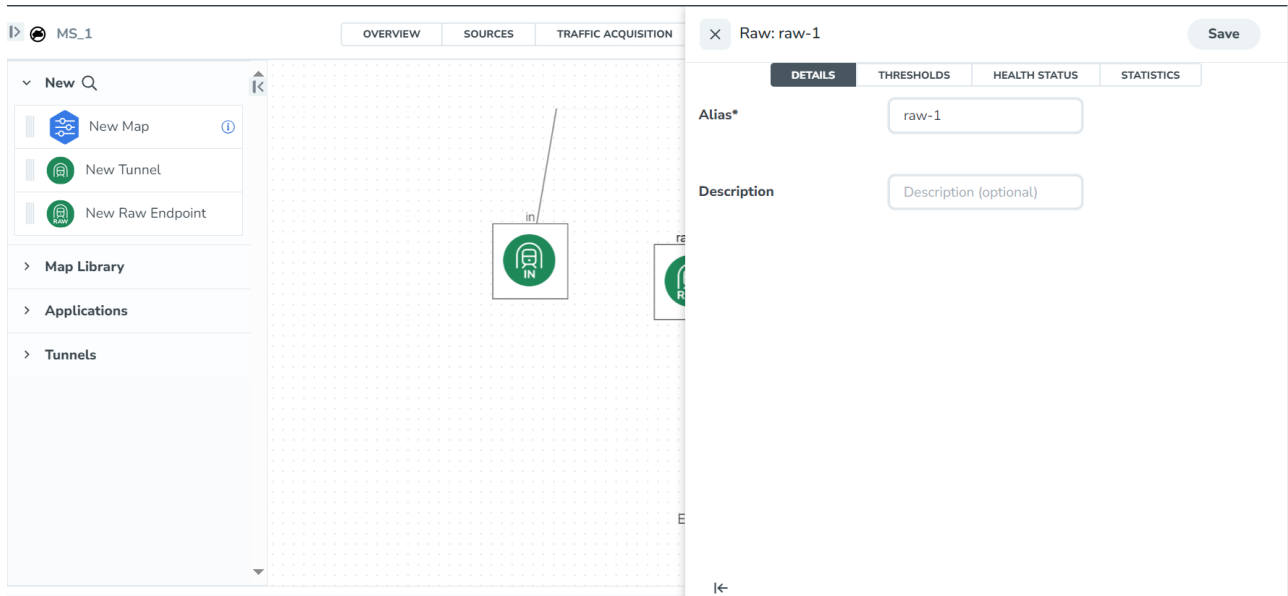
Field	Description	
Out	IP Version	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that helps network devices identify the higher or lower priority to handle traffic. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the number of times you can try the sync. The value ranges from 1 to 6.
Delay Acknowledgments	Enable to receive the acknowledgments for a delay.	
UDP:		
Out	L4 Destination IP Address	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. For details, refer to Application Metadata Exporter .
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.

Create Raw Endpoint (AWS)

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

To add Raw Endpoint to the monitoring session:

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



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

Create a New Map (AWS)


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

For new users, the free trial bundle expires 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.

Terms to know before creating a map:

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

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	<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> <p>For any rule type as Source - the traffic direction is egress.</p> <p>For Destination rule type - the traffic direction is ingress.</p> <p>For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress.</p> <div data-bbox="683 1199 1468 1539" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Notes:</p> <ul style="list-style-type: none"> For OpenStack environment, Subnet Name Source and Subnet Name Destination are the exclusion filters available as part of Exclusion Maps with Traffic Acquisition method as OVS Mirroring in the Monitoring Domain. If no ATS rule filters listed above are used, all VMs and vNICs are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC. </div>
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

Rules and Notes:

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


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

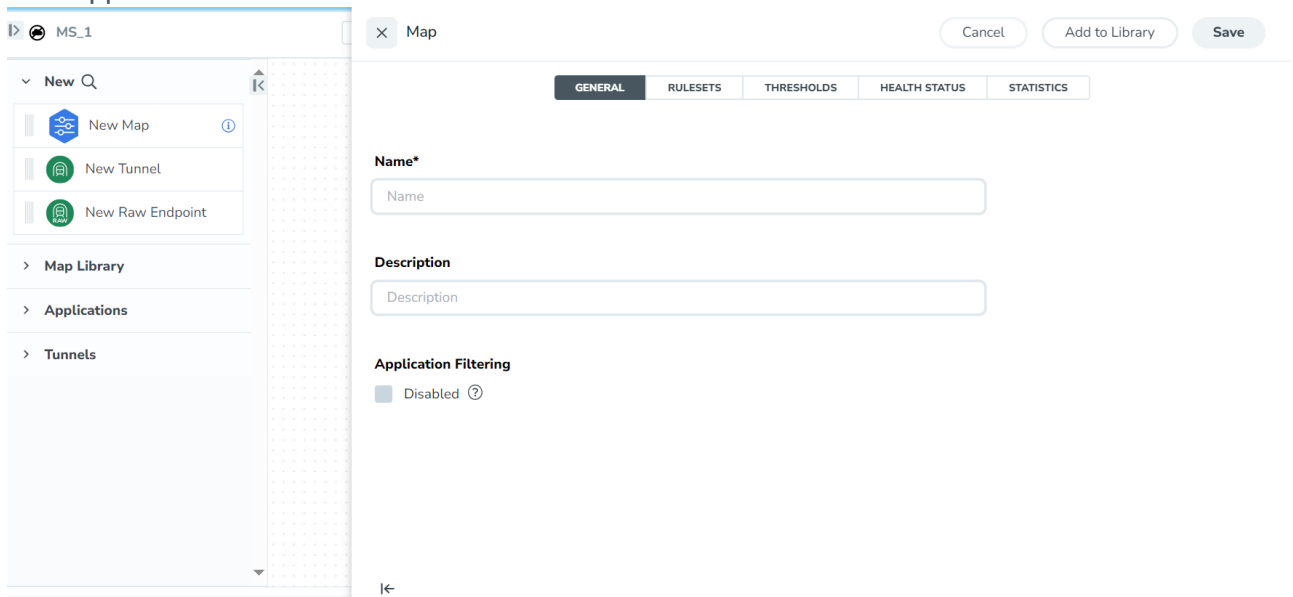
To create a new map:

1. Perform one of the following:


- Create a new Monitoring Session.
- On an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab.

The GigaVUE-FM Monitoring Session canvas appears.

2. On the left pane of the canvas, select the  icon expand icon to view the traffic processing elements.
3. Select **New > New Map**, drag and drop a new map template to the workspace. The New Map quick view appears.



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

 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

5. Select the **Rule Sets** tab. Through the map, you can drop or pass packets based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. For details, refer to [Example- Create a New Map using Inclusion and Exclusion Maps](#).

a. **To create a new rule set:**

- i. Select **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. Select **Actions > New Rule**.
- ii. Select a required condition from the drop-down list. Click  and select **Add Condition** to add more conditions.
- iii. Select the rule to **Pass** or **Drop** through the map.

6. Select **Save**.

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

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

Example- Create a New Map using Inclusion and Exclusion Maps

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

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

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

Map Library

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

To add a map,

1. From the Monitoring Session screen, select **TRAFFIC PROCESSING**.
The GigaVUE-FMCanvas page appears.
2. From the page,, select the desired map and save it as a template.
3. Select **Details**.

The Application quick view appears.

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

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

Reusing a map

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

Add Applications to Monitoring Session (AWS)

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

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

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

Interface Mapping (AWS)

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

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

To perform interface mapping:

1. Go to Traffic > Virtual > Orchestrated Flows and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Navigate to the **V SERIES NODES** tab and select **Interface Mapping**. The **Deploy Monitoring Session** dialog box appears.
3. Select the GigaVUE V Series Nodes to which you wish to map the interface.
4. From the drop-down menu of the GigaVUE V Series Node, select the interfaces for the following deployed in the Monitoring Session:
 - REPs (Raw Endpoints)
 - TEPs (Tunnel Endpoints)
5. Select **Deploy**.

The updated mappings take effect when deployed.

Deploy Monitoring Session (AWS)

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

To deploy the Monitoring Session,

1. **Add components to the canvas**
Drag and drop the following items to the canvas as required:
 - **Ingress tunnel** (as a source): From the New section.
 - **Maps**: From the Map Library section.
 - **Inclusion and Exclusion maps**: From the Map Library to their respective section at the bottom of the workspace.
 - **GigaSMART apps**: From the **Applications** section.
 - **Egress tunnels**: From the **Tunnels** section.
2. **Connect components**
Perform the following steps after placing the required items in the canvas.
 - a. Hover your mouse on the map
 - b. Select the dotted lines
 - c. Drag the arrow over to another item (map, application, or tunnel).

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

3. (Optional) Review Sources

Select the **SOURCES** tab to view details about the subnets and monitored instances.

The monitored instances and the subnets are visible in orange.

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

4. Deploy the Monitoring Session

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

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

View the Deployment Report

You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab.

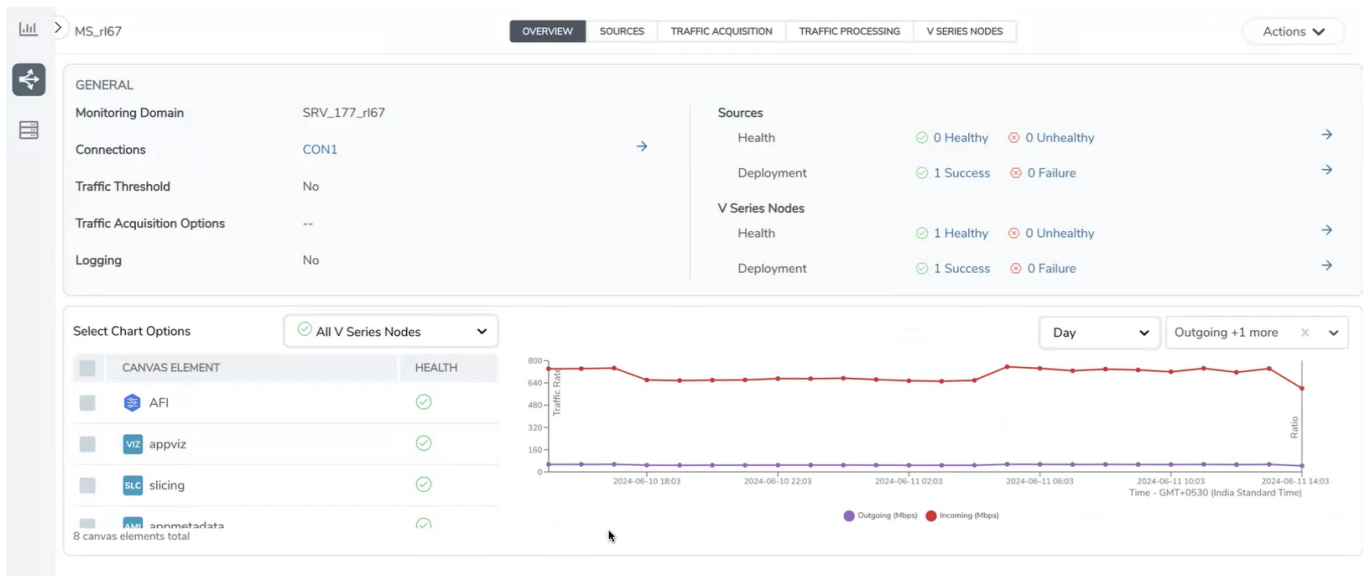
- When you select the **Status** link, the Deployment Report is displayed.
- When the deployment is incorrect, the Status column displays one of the following errors:
 - **Success:** Not deployed on one or more instances due to V Series Node failure.
 - **Failure:** Not deployed on all V Series Nodes or Instances.

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

View Monitoring Session Statistics (AWS)

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

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



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

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

Visualize the Network Topology (AWS)

You can have multiple connections in GigaVUE-FM. Each connection can have multiple Monitoring Sessions configured within it. The Topology tab provides a visual representation of the monitored elements within a selected connection and Monitoring Session.

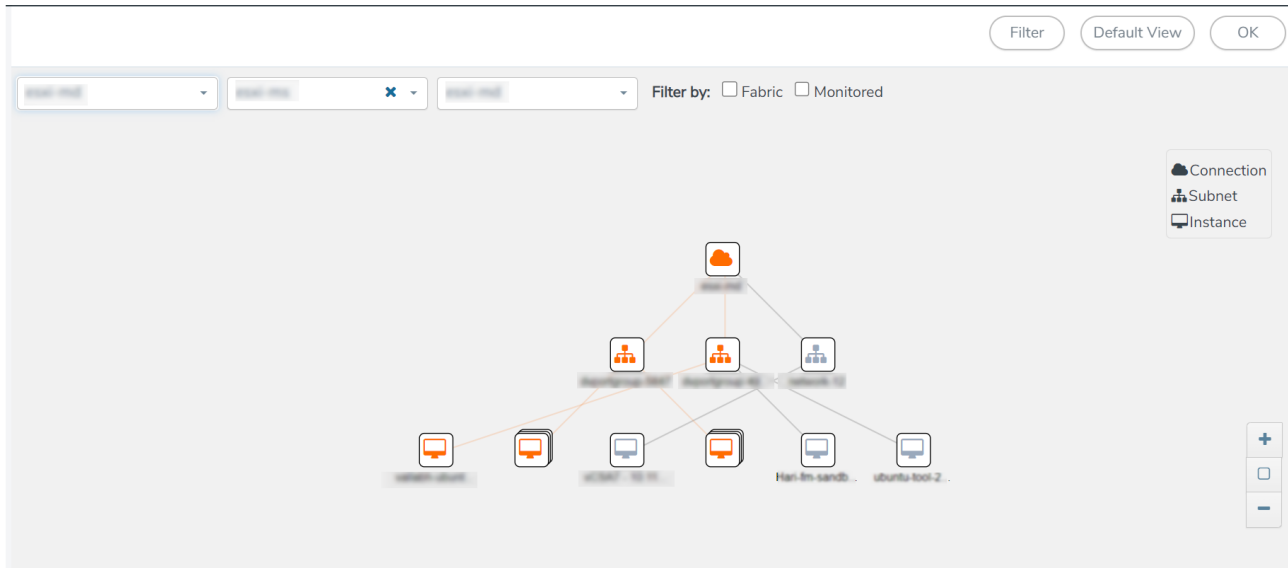
To view the topology in GigaVUE-FM:

1. Go to Traffic > Virtual > Orchestrated Flows and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Create a Monitoring Session or select an existing Monitoring Session,
3. Open the **TOPOLOGY** tab.
4. From the **Connection** list on the Topology page, select a connection.

The topology view of the monitored subnets and instances in the selected session is displayed.

5. From **View**, select one of the following instance types:

- Fabric
- Monitored



6. (Optional) Hover over or select the subnet or VM Group icons to view the subnets or instances in the group.

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

- Use the **Filter** button to filter the instances based on the VM name, VM IP, OS Type, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitored instances.
- Apply Navigation controls, such as:
 - Use the arrows at the bottom-right corner to move the topology page up, down, left, or right.
 - Use + or - icons to zoom in and zoom out of the topology view.
 - Select the **Fit View** icon to fit the topology diagram according to the width of the page.

Migrate Application Intelligence Session to Monitoring Session

Starting from Software version 6.5.00, you must configure the Application Intelligence solution from Monitoring Session Page. After upgrading to 6.5.00, you cannot create a new Application Intelligence Session or edit an existing Application Intelligence Session for a virtual environment from the

Application Intelligence page.

The following actions are available only when using the existing Application Intelligence Session:

- View Details
- Delete
- Forced Delete

We recommend to migrate the existing sessions to Monitoring Session for full functionality. GigaVUE-FM seamlessly migrates all your virtual Application Intelligence sessions and their connections. If migration fails, all sessions return to their original states.

Points to Note:

- You must have write access for the **Traffic Control Management** Resource in GigaVUE-FM to perform this migration. For details, refer to Create Roles section In GigaVUE Administration Guide
- The migration does not proceed:
 - If any of the existing Application Intelligence Session is in PENDING or SUSPENDED. Resolve the issue and start the migration process.
 - If any of the existing Application Intelligence Session is in FAILED state due to incorrect configuration. Resolve the issue and start the migration process.
 - If an existing Monitoring Session has the same name as the Application Intelligence Session. Change the existing Monitoring Session name to continue with the migration process.
- You cannot continue the session if any of the existing Application Intelligence Session has Application Filtering configured with Advanced Rules as Drop Rule and No Rule Match Pass All in the 5th rule set. In the Monitoring Session, the fifth Rule Set supports either Pass All or Advanced Rules as Drop. Delete this session and start the migration.
- When migrating the Application Intelligence Session, in rare scenarios, the migration process might fail after the pre-validation. In such cases, all the Application Intelligence Session roll back to the Application Intelligence page. Contact Technical Support for assistance.

Migrate your existing Application Intelligence Session to Monitoring Session Page

Follow these steps:

1. In the left navigation pane, select **Traffic > Solutions > Application Intelligence**. You cannot create a new Application Intelligence Session from this page. When you have an existing virtual Application Intelligence Session in the above page, the **Migrate Virtual** Application Intelligence dialog box appears.
2. Review the message and select **Migrate**. The **Confirm Migration** dialog box appears with the list of Application Intelligence Session that you need to migrate.
3. Review the list and select **Migrate**. GigaVUE-FM verifies the requirements and then migrates the Application Intelligence Sessions to the Monitoring Session Page.
4. Select **Go to Monitoring Session Page**.

You can view that all the virtual Application Intelligence Sessions in the Application Intelligence page are migrated to the Monitoring Session Page.

Post Migration Notes for Application Intelligence

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

1. **Secure Tunnels in the Options page** If you wish to enable Secure tunnels after migrating the Application Intelligence Session, follow these steps.

- a. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.

The **Monitoring Sessions** page appears.

- b. Select the Monitoring Session for which you enabled Secure Tunnels.

- c. Select **Actions > Undeploy**.

The monitoring session is undeployed.

- d. Select the Monitoring Session for which you enabled Secure Tunnels.

- e. Select **Actions > Edit**.

The **Edit Monitoring Session Canvas** page appears.

- f. Add the Application Intelligence applications.

- g. Modify the Number of Flows as per the below table.

Cloud Platform	Instance Size	Maximum Number of Flows
VMware	Large (8 vCPU and 16GB RAM)	200k
AWS	AMD - Large (c5n.2xlarge)	300k
	AMD - Medium (t3a.xlarge)	100k
	ARM - Large (c7gn.2xlarge)	100k
	ARM - Medium (m7g.xlarge)	200k
Azure	Large (Standard_D8s_v4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16GB RAM)	200k

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

- h. Select **Deploy**. For details, refer to Application Intelligence section in the GigaVUE V Series Applications Guide.

2. Temporary Loss of Statistics with Version Mismatch

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

3. Configuration Changes Post-Migration

To make configuration changes post-migration, make sure that the GigaVUE V Series Node version is greater than or equal to 6.3.00.

Configure AWS Elastic Load Balancing

You can use a load balancer to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series Nodes. The load balancer distributes the traffic to the GigaVUE V Series Nodes and the GigaVUE-FM auto-scales the GigaVUE V Series Nodes based on the traffic.

The following load balancers are supported:

- [AWS Network Load Balancer](#)
- [Gateway Load Balancer](#)

AWS Network Load Balancer

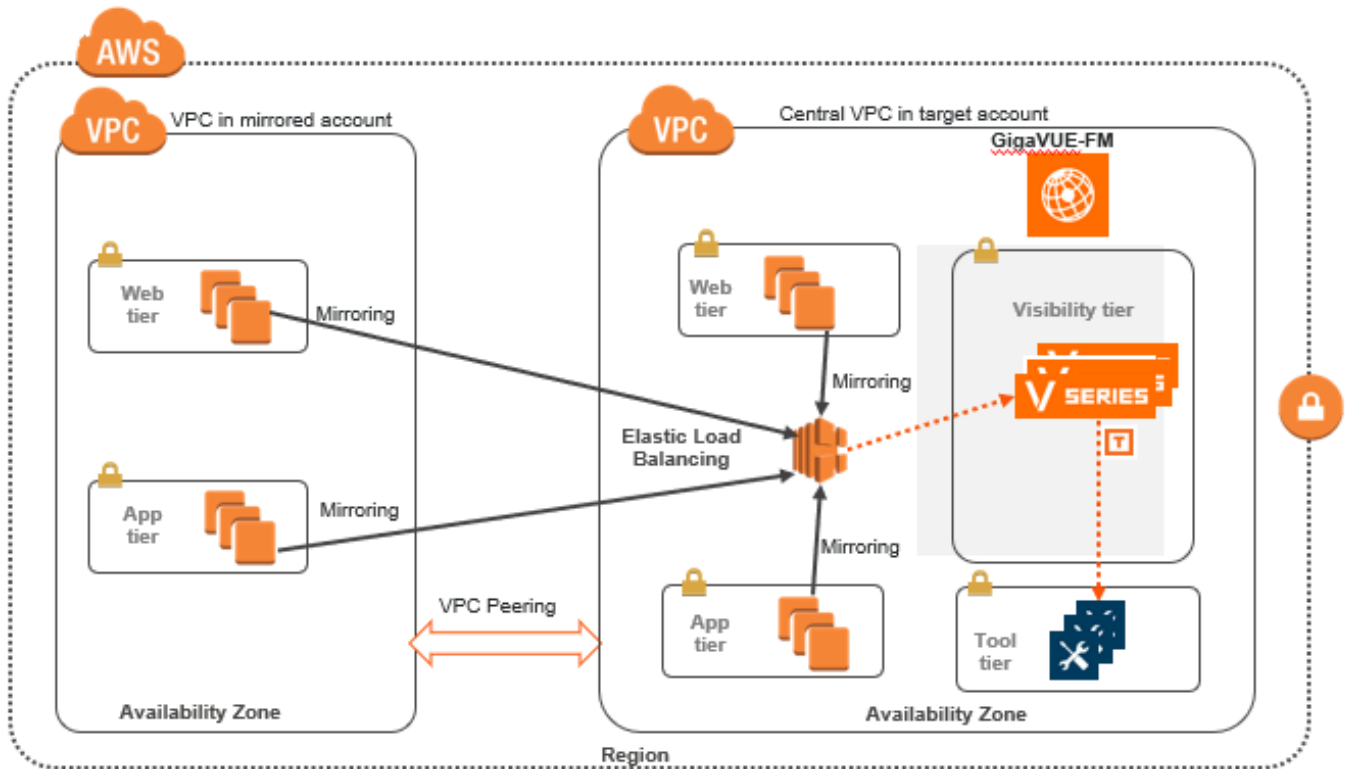
You can use a load balancer to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series Nodes. The load balancer distributes the traffic to the GigaVUE V Series Nodes and the AWS platform auto-scales the GigaVUE V Series Nodes based on the traffic by using the AWS autoscaling group.

GigaVUE-FM creates a traffic mirror from the target VMs to the load balancer that all the targets must have the same traffic load balancer destination. Load balancer forwards the traffic to the GigaVUE V Series nodes and the AWS Auto Scaling group monitors the load of all GigaVUE V Series nodes. AWS Auto Scaling group can add or remove nodes if the traffic load is heavy or low.

Refer to the following topics for detailed information.

- [Architecture](#)
- [Configure Network Load Balancer](#)
- [Deploy Visibility Fabric with Network Load Balancer](#)

Architecture



The design shows how to deploy GigaVUE Cloud Suite fabric components in a centralized VPC where the target VMs of multiple AWS accounts are deployed behind an external AWS network load balancer. GigaVUE-FM creates Traffic Mirroring on the target VMs to mirror and forward the traffic to the load balancer. The load balancer then deploys or deletes additional GigaVUE V Series Nodes and distributes the traffic among them to aggregate, filter, and forward the traffic to the tools over the tunnel endpoint. In AWS, the Auto Scaling group monitors the load among all the GigaVUE V Series Nodes and adds or removes them via RESTful API integration with the GigaVUE-FM when the traffic load crosses or drops below a pre-defined threshold.

A typical AWS deployment to support the external load balancer requires the following components:

- GigaVUE-FM (GigaVUE-FM fabric manager)
- GigaVUE V Series Node
- AWS Network Load Balancer (uniformly distributes traffic from AWS target VMs to GigaVUE V Series nodes)

Configure Network Load Balancer

Prerequisites

- Create or update Security Group polices of GigaVUE Cloud Suite components. For details, refer to [Security Group](#) .
- Create or update routes in various VPCs across participating mirrored AWS accounts so that all mirrored account VPCs can connect to the target account VPC where the AWS Network Load Balancer is deployed. For details, refer to [Amazon VPC](#).

NOTE: The target account VPC is considered as the centralized VPC by GigaVUE-FM and the connections towards all other mirrored account VPCs either through 1 : 1 VPC peering or via 1 : M transit gateway (that connects all participating VPCs across mirrored AWS accounts). VPC peering has no bandwidth limitation and no additional cost within the same region (recommended). Transit gateway costs more and it also has a limitation of 50 Gbps burst per VPC.

- Create or update existing IAM role for GigaVUE-FM in the centralized VPC. Additionally trust relationship needs to be created between the mirrored and the target account for GigaVUE-FM to execute the above permissions at the IAM role level. Refer to AML and Permissions section for detailed information.
- User and Password provided in the registration data must be configured in the **User Management** page for deploying GigaVUE V Series Node using Third Party Orchestration. For details, refer to [Configure Role-Based Access for Third Party Orchestration](#).

Points to Note:

When configuring Network Load Balancer, the GigaVUE V Series Nodes must be deployed using Third Party Orchestration.

Perform the following steps to configure an external load balancer in AWS:

1. In the **Target Groups** page, click **Create target group** and the Create target group wizard appears. Enter or select the following values and create the target group.
 - a. Select **IP addresses** as the target type.
 - b. Enter a name for the target group.
 - c. Select the **UDP** as the Protocol and **4789** as the port number.
 - d. Select the VPC of your target group where the targets are registered.
 - e. Select **TCP** as the Health check protocol in port number **8889** with **10 seconds** health check interval.

NOTE: For detailed instructions, refer to [Create a target group for your Network Load Balancer](#) topic in the AWS Elastic Load Balancing document.

2. Navigate to the **Load Balancer** page and click **Create Load Balancer** the Create elastic load balancer wizard appears. Enter or select the following values and create the load balancer.
 - a. Select **Network Load Balancer** as the load balancer type and click **Create**.
 - b. Enter a name for the Network Load Balancer.
 - c. Select **Internal** load balancer as the Scheme.
 - d. Select the **VPC** for your targets (GigaVUE V Series Nodes).
 - e. Select the regions/zones and the corresponding subnets.
 - f. Select **UDP** as the Listener Protocol with Port number **4789**.

NOTE: For detailed instructions, refer to [Create a Network Load Balancer](#) topic in the AWS Elastic Load Balancing document.

3. Navigate to the **Launch Templates** page and click **Create launch template** the Create launch template wizard appears. Enter or select the following values and create the launch template.
 - a. Enter a name for the launch template.
 - b. Select the AMI of the GigaVUE V Series node.
 - c. Select **t3a.xlarge** as the instance type.
 - d. Select a Key pair for the instance.
 - e. Select **VPC** as the Networking platform and don't specify the security group.
 - f. Add 2 Network Interfaces for the GigaVUE V Series Node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces, select the appropriate security group.
 - g. In the **Advanced details** section, enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM using Third Party Orchestration.

```
#cloud-config
write_files:
- 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
```

NOTE: Enter the Username and Password created in the **Add Users** Section of the **User Management** page.

4. Navigate to the **Auto Scaling groups** page, and click **Create an Auto Scaling group** the Create Auto Scaling group wizard appears. Enter or select the following values and create the Auto Scaling group.
 - a. Enter a name for the Auto Scaling group.
 - b. Select an existing launch template.
 - c. Select the VPC and subnet.
 - d. In the Group size section, enter the Desired capacity as 0. The Desired capacity value must be less than the Maximum Capacity value.

NOTE: Once the monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node that needs to be deployed in this Monitoring Domain.

- e. In the Scaling policies section, select **Target tracking scaling policy** and choose Average network in (bytes) for the Metric type with **1000000000 (bytes)** as target value and **300** seconds warm up value.
- f. (optional) Add **Tags** to the instances.

NOTE: For detailed instructions, refer to [Creating an Auto Scaling group using a launch template](#) topic in the AWS EC2 Auto Scaling document. Once the monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node that needs to be deployed in this Monitoring Domain.

In the Instances page, you can view the GigaVUE V Series Node instance deployed by the load balancer.

Deploy Visibility Fabric with Network Load Balancer

To deploy GigaVUE V Series Node across the AWS accounts with Network Load Balancer in GigaVUE-FM:

1. In the **Monitoring Domain Configuration** page, select **VPC Traffic Mirroring** or **Customer Orchestrated Source** as the Traffic Acquisition method. Refer to [Create a Monitoring Domain](#) for detailed information.
2. Enter the Monitoring Domain name and the Connection name as mentioned in the user data provided during the template launch in AWS. Refer to [Configure Network Load Balancer](#) section for more detailed information.
3. For the **Use Load Balancer** field, select **Yes**.
4. Select **No** for the **Use FM to Launch Fabric** option. This allows you to deploy the fabric components using Third Party Orchestration.

The screenshot displays the 'Monitoring Domain Configuration' interface. At the top, there are navigation tabs for 'AWS', 'Monitoring Domains', 'Connections', 'Fabric', 'UCT-V', and 'Settings'. The main configuration area includes the following fields:

- Monitoring Domain***: md1
- Traffic Acquisition Method***: VPC Traffic Mirroring
- Traffic Acquisition Tunnel MTU***: 8951
- Use FM to launch V Series Proxy**: No (toggle)
- Use Load Balancer**: Yes (toggle)

Below these fields is a 'Connections' section with a table for adding connections:

Name*	Credential*	Region*	Accounts*	VPCs*
Enter a connection name	Credential Name...	Region Name...	Select Accounts...	Select VPCs...

At the top right of the configuration area, there are buttons for 'Check Permissions', 'Save', and 'Cancel'. A blue notification banner at the top right reads: 'We have changed the G-vTAP product name to UCT-V. No functionality will be affected by this name change.'

5. Click **Save**. The Monitoring Domain is created successfully.
6. In the AWS Fabric Launch Configuration page, select the following for the load balancer.
 - Select the **VPC** from the drop down list.
 - Select the **Load Balancer** configured in AWS.
 - Select the **Auto Scaling Group** configured in AWS.
7. Click **Save** to save the configuration.

Once the Monitoring Domain is successfully configured, edit the **Desired capacity** value for the Auto Scaling Group in AWS. Refer to [Create an Auto Scaling group using a launch template](#) section in AWS for more detailed information.

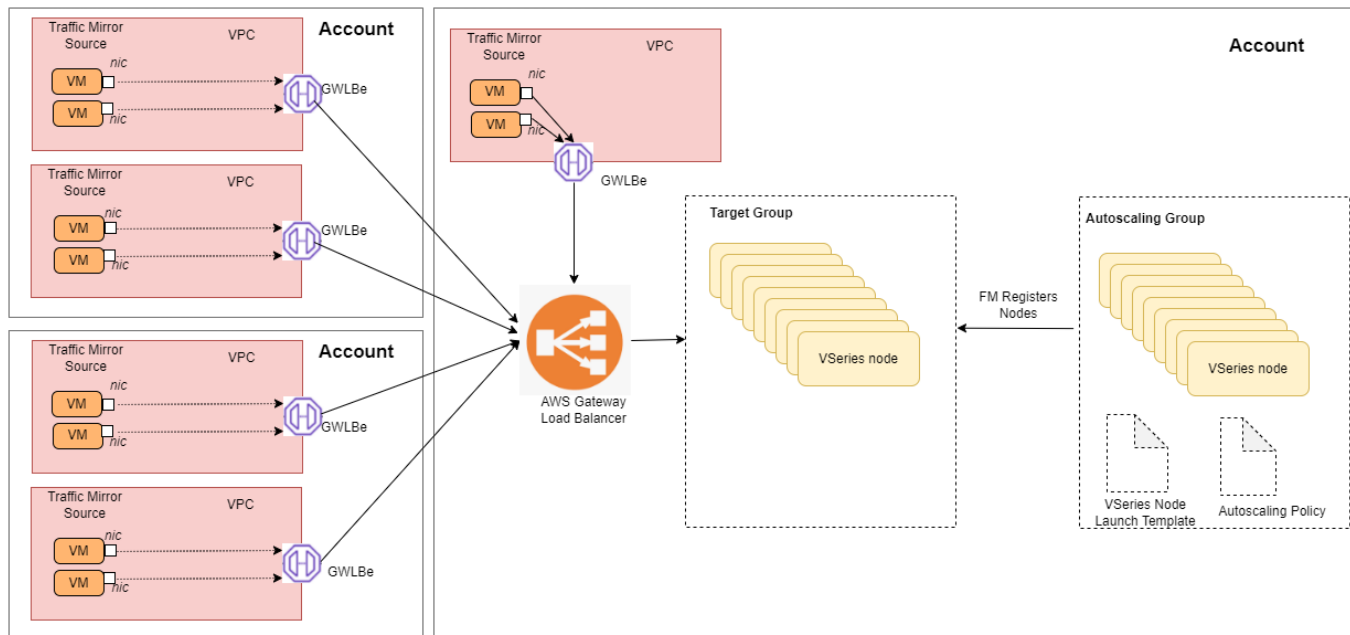
What to do Next:

To monitor the traffic, you must create a Monitoring Session. For more information on creating a Monitoring Session, see [Configure Monitoring Session](#).

AWS Gateway Load Balancer

The gateway load balancer (GWLB) uses the gateway load balancer end points to distribute the traffic across the end points. It is a VPC endpoint that provides connectivity in between virtual machines. With GWLB Endpoint as a target, mirrored traffic can be forwarded from any subnet. You can monitor network traffic across multiple VPCs and accounts, with centralized traffic inspection in a single VPC across the entire organization.

Architecture



In the architecture, you can see the deployment of GigaVUE Cloud Suite for AWS environments that have GWLB implementation for the security appliances, such as firewalls. In such deployments, the applications and your appliances are in different VPCs.

The workload VPC is configured with the Gateway load balancer endpoint while the service VPC is configured with the Gateway load balancer. Gigamon deployed VPC has the solution components, such as GigaVUE-FM, GigaVUE V Series Nodes, and the OOB tools that consume the mirrored and decapsulated data.

Configure a Gateway Load Balancer

Prerequisites

- Create or update Security Group policies of GigaVUE Cloud Suite components. For details, refer to [Security Group](#).
- Create or update routes in various VPCs across participating mirrored AWS accounts so that all mirrored account VPCs can connect to the target account VPC where the AWS Gateway Load Balancer is deployed. For details, refer to [Amazon VPC](#).
- Create or update existing IAM role for GigaVUE-FM in the centralized VPC. Additionally trust relationship needs to be created between the mirrored and the target account for GigaVUE-FM to execute the above permissions at the IAM role level. For details, refer to AMI and Permissions.
- For more information on AWS recommended design for Gateway Load Balancer implementation with inline services, such as firewall, see [Getting started with Gateway Load Balancers - Elastic Load Balancing \(amazon.com\)](#)
- You must create a VPC endpoint and endpoint service. For more information, see [Create endpoint service](#)
- Create a routing table. For more information, see [Amazon documentation](#).
- User and Password provided in the registration data must be configured in the **User Management** page for deploying GigaVUE V Series Node using Third Party Orchestration. For details, refer to [Configure Role-Based Access for Third Party Orchestration](#).

Points to Note:

When configuring Gateway Load Balancer, the GigaVUE V Series Nodes must be deployed using Third Party Orchestration.

Perform the following steps to configure an external load balancer in AWS:

1. In the **Target Groups** page, click **Create target group** and the Create target group wizard appears. Enter or select the following values and create the target group.
 - a. Select **IP addresses** as the target type.
 - b. Enter a name for the target group..
 - c. Select the VPC of your target group where the targets are registered.
 - d. Select **TCP** as the Health check protocol in port number **8889** with **10 seconds** health check interval.

NOTE: You must select GENEVE protocol and port 6081 while creating the targets groups. For detailed instructions, refer to [Target groups for your Gateway Load Balancers](#).

2. Navigate to the **Load Balancer** page and click **Create Load Balancer** the Create elastic load balancer wizard appears. Enter or select the following values and create the load balancer.
 - a. Select **Gateway Load Balancer** as the load balancer type and click **Create**.
 - b. Enter a name for the Gateway Load Balancer.
 - c. Select the **VPC** for your targets (GigaVUE V Series Nodes).
 - d. Select the regions/zones and the corresponding subnets.
 - e. Associate the load balancer to the target group.
 - f. By default, **GENEVE** as the Listener Protocol with Port number **6081** is selected.

NOTE: For detailed instructions, refer to [Create a Gateway Load Balancer](#) topic in the AWS Elastic Load Balancing document

3. Navigate to the **Launch Templates** page and click **Create launch template** the Create launch template wizard appears. Enter or select the following values and create the launch template.
 - a. Enter a name for the launch template.
 - b. Select the AMI of the GigaVUE V Series node.
 - c. Select **c5n.xlarge** as the instance type.
 - d. Select a Key pair for the instance.
 - e. Select **VPC** as the Networking platform and don't specify the security group.
 - f. Add 2 Network Interfaces for the GigaVUE V Series Node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces, select the appropriate security group.
 - g. In the **Advanced details** section, enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM using Third Party Orchestration.

```
#cloud-config
write_files:
- 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
```

NOTE: Enter the Username and Password created in the **Add Users** Section of the **User Management** page.

NOTE: For detailed instructions, refer to [Creating a launch template for an Auto Scaling group](#) topic in the AWS EC2 Auto Scaling document.

4. Navigate to the **Auto Scaling groups** page, and select **Create an Auto Scaling group**. The Create Auto Scaling group wizard appears. Enter or select the following values and create the Auto Scaling group.
 - a. Enter a name for the Auto Scaling group.
 - b. Select an existing launch template.
 - c. Select the VPC and subnet.
 - d. In the Group size section, enter the Desired capacity as 0. The Desired capacity value must be less than the Maximum Capacity value.

NOTE: Once the monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node that needs to be deployed in this Monitoring Domain.

- e. In the Scaling policies section, select **Target tracking scaling policy** and choose Average network in (bytes) for the Metric type with **1000000000 (bytes)** as target value and **300** seconds warm up value.
- f. (optional) Add **Tags** to the instances.

NOTE: For detailed instructions, refer to [Creating an Auto Scaling group using a launch template](#) topic in the AWS EC2 Auto Scaling document.

In the Instances page, you can view the GigaVUE V Series Node instance launched by the auto scaling group.

Deploy Visibility Fabric with Gateway Load Balancer

To deploy GigaVUE V Series Node across the AWS accounts with Gateway Load Balancing in GigaVUE-FM:

1. In the **Monitoring Domain Configuration** page, select **VPC Traffic Mirroring** or **Customer Orchestrated Source** as the Traffic Acquisition method. Refer to [Create a Monitoring Domain](#) for detailed information.
2. Enter the Monitoring Domain Name and the Connection Name as mentioned in the user data provided during the template launch in AWS. Refer to [Configure a Gateway Load Balancer](#) section for more detailed information.
3. For the **Use Load Balancer** field, select **Yes**.
4. Select **No** for the **Use FM to Launch Fabric** option. This allows you to deploy the fabric components using Third Party Orchestration.

The screenshot displays the 'Monitoring Domain Configuration' interface. The 'Monitoring Domain' is set to 'md1'. The 'Traffic Acquisition Method' is 'VPC Traffic Mirroring'. The 'Traffic Acquisition Tunnel MTU' is '8951'. The 'Use FM to launch V Series Proxy' toggle is 'No', and the 'Use Load Balancer' toggle is 'Yes'. Below these are fields for 'Connections', including 'Name', 'Credential', 'Region', 'Accounts', and 'VPCs'. A notification banner at the top right indicates a product name change from G-vTAP to UCT-V.

5. Click **Save**. The Monitoring Domain is created successfully.
6. In the AWS Fabric Launch Configuration page, select the following for the load balancer.
 - Select the VPC from the drop down menu.
 - Select the Load Balancer configured in AWS
 - Select the Auto Scaling Group configured in AWS
7. Click **Save** to save the configuration.

Once the monitoring domain is successfully configured, edit the Desire capacity value for the Auto Scaling Group in AWS. Refer to [Configure a Gateway Load Balancer](#) section for more detailed information.

To monitor the traffic, you must create a monitoring session. For more information on creating a Monitoring Session, see [Configure Monitoring Session](#).

For more information on the best practices and architectures, see the following links:

- [Getting started with Gateway Load Balancers](#)
- [Scaling network traffic inspection using AWS Gateway Load Balancer](#)

Check for Required IAM Permissions

GigaVUE-FM allows you to validate whether policy attached to the GigaVUE-FM using **EC2 Instance Role="** or **Access Credential** has the required IAM permissions and notifies the users about the missing permissions.

You can check permissions while creating Monitoring Domain and deploying GigaVUE Fabric Components using GigaVUE-FM, by clicking the **Check Permissions** button on the **Monitoring Domain Configuration** page and **AWS Fabric Launch Configuration** page. The GigaVUE-FM displays the minimum required IAM permissions.

Prerequisites to deploy GigaVUE Cloud Suite for AWS:

- **IAM permissions:** Checks whether the minimum required permissions are granted for the instance where the GigaVUE-FM is deployed. For details on how to configure the required permissions in AWS, refer to [Permissions and Privileges \(AWS\)](#).
- **Access to public cloud end points:** Check for access to the AWS cloud end point APIs.
- **Subscription to the GigaVUE Cloud Suite for AWS:** Before deploying the solution, you must subscribe to the GigaVUE Cloud Suite components from the AWS marketplace. It checks whether the required components are subscribed in the marketplace. For details, refer to [Subscribe to GigaVUE Products](#).
- **Security Group:** Checks whether the required ports are configured in the security group. For more information on the security groups, see [Security Group](#) .

NOTE: Security group rules validation does not validate prefix List and user groups. For a successful validation, the ports and CIDR range should be updated in the Security Group.

After you press the **Check Permissions** button, GigaVUE-FM verifies the minimum required permissions. Any missing permissions are highlighted with the respective message against the permission in a dialog box. You can use the displayed IAM Policy JSON as a reference and update the policy that is attached to the GigaVUE-FM.

Refer to the following sections for more detailed information:

- [Check Permissions while Creating a Monitoring Domain](#)
- [Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM](#)

Upgrade GigaVUE-FM in AWS

This chapter describes how to upgrade the GigaVUE-FM instance deployed in AWS.

Refer to the following sections for details:

- [Upgrade GigaVUE-FM using Snapshot in AWS](#)
- Upgrade from UI. For more information on upgrading from UI, refer to the Upgrade from UI topic in GigaVUE-FM Installation and Upgrade Guide.

At a Glance

To upgrade the GigaVUE-FM instance successfully, you must perform the following steps:

1. Stop the existing version of the GigaVUE-FM instance.
2. Create a snapshot of the second disk (dev/sdb) of the GigaVUE-FM instance.
3. Make a note of the snapshot ID.
4. Launch the latest version of the GigaVUE-FM instance. While launching the latest version, enter the snapshot ID of the old version of the GigaVUE-FM instance in **Add Storage > Add New Volume**.
5. Complete the launch.
6. Verify if the data from the previous GigaVUE-FM instance is restored in the new instance.
7. Terminate the old GigaVUE-FM instance.

Stop GigaVUE-FM Instance

Before upgrading the GigaVUE-FM instance, stop the existing version of the GigaVUE-FM instance.

NOTE: Do not terminate the GigaVUE-FM instance.

To stop the GigaVUE-FM instance,

1. Log in to the AWS account and select **Services > EC2**.
2. In the left pane, select **Instances**.
3. In the search field, enter the name of the existing GigaVUE-FM instance and select the Instance ID.

NOTE: If the instance ID is the password for logging in to the existing GigaVUE-FM, make note of this instance ID. This instance ID is used as the password for logging in to the upgraded GigaVUE-FM as well. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

4. Go to **Actions > Instance State > Stop**.

Create Snapshot of the GigaVUE-FM Instance

You must create a snapshot of the volume of the existing version (dev/sdb) of the GigaVUE-FM instance. Snapshots capture data that are written to your Amazon EBS volume at the time the snapshot is taken. This excludes any data that are cached by any applications or the operating system.

To create a snapshot,

1. Select the GigaVUE-FM instance and select the **Description** tab.
2. Scroll down and locate Block Devices.
3. Select the **/dev/sdb** link. The Block Device dialog box is displayed with the volume ID link.
4. In the Block Device dialog box, click the volume ID link. The Volumes page is displayed.
5. Select **Actions > Create Snapshot**.

The Create Snapshot dialog box is displayed.

6. In the Create Snapshot dialog box, enter the following information:

Table 1: Fields for Creating a Snapshot

Field	Description
Name	The name of the snapshot.
Description	The description of the snapshot.

7. Select **Create**. After several minutes the snapshot is created.

NOTE: Make a note of the snapshot ID. This snapshot ID is used to find the snapshot and add the volume while upgrading the GigaVUE-FM instance.

Upgrade GigaVUE-FM Instance

While upgrading the GigaVUE-FM instance, the Amazon EBS volume must be restored with the data from the snapshot that is created in [Create Snapshot of the GigaVUE-FM Instance](#).

To upgrade the GigaVUE-FM instance:

1. Select **Services > EC2**.
2. Select **Launch Instance** and go to **AWS Marketplace** or **Community AMIs**.
3. Search for **Gigamon**, locate the latest version of the GigaVUE-FM AMI, and click **Select**.
4. Select the Instance Type. The recommended instance type is **m4.xlarge**.

NOTE: Do not select the t2 instance types as they are not supported.

5. Select **Next:> Configure Instance Details**.
6. Enter the following information.
 - o **Network**– Select the VPC where you want to launch the AMI.
 - o **Subnet**– Select the management subnet that the instance will use after launch. (Required)
 - o **Auto-assign Public IP**– Select **Enable**.
 - o **IAM role**–Select an existing IAM role to associate with the instance. Refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide*.
7. Select **Configure storage > Advanced**.
8. Select **Volume 2** and then select the Snapshot that you created in [Create Snapshot of the GigaVUE-FM Instance](#).
9. Click **Next: Tag Instance**, and then add a key-value pair to identify the instance.
10. Select **Next: Add Security Group**.
11. Select the **Select an existing security group** check box if the security group is already created. Otherwise, select the **Create a new security group** check box and select **Add Rule**. For more information on creating a security group, refer to the *Security Group* section in GigaVUE Cloud Suite Deployment Guide - AWS.
12. Select **Review and Launch**.
13. Review the instance launch details and select **Launch**.
14. Select the SSH key pair, check the acknowledgment check box, and select **Launch Instances**.
15. Verify the initialized instance through the Web interface as follows:
 - a. Find the instance and expand the page in the **Descriptions** tab to view the instance information, if necessary.
 - b. Copy the Public DNS value and paste the value into a new browser window or tab.

- c. Copy the Instance ID of the previous version of the GigaVUE-FM. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

NOTE: Do not have multiple versions of GigaVUE-FM instances monitoring the same AWS connection.

Launch the new version of the GigaVUE-FM instance. Verify if the data from the previous GigaVUE-FM instance is restored in the new instance. Once the data is verified, terminate the old version of the GigaVUE-FM instance.

Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS

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

Refer to the following topic for more information:

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

Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series Nodes, you must upgrade GigaVUE-FM to software version 5.13 or above.

Upgrade UCT-V Controller

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

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

To change UCT-V Controller version between different major versions

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

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

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

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

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

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

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

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

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



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

Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

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

There are two ways to upgrade the GigaVUE V Series Proxy and Nodes. You can:

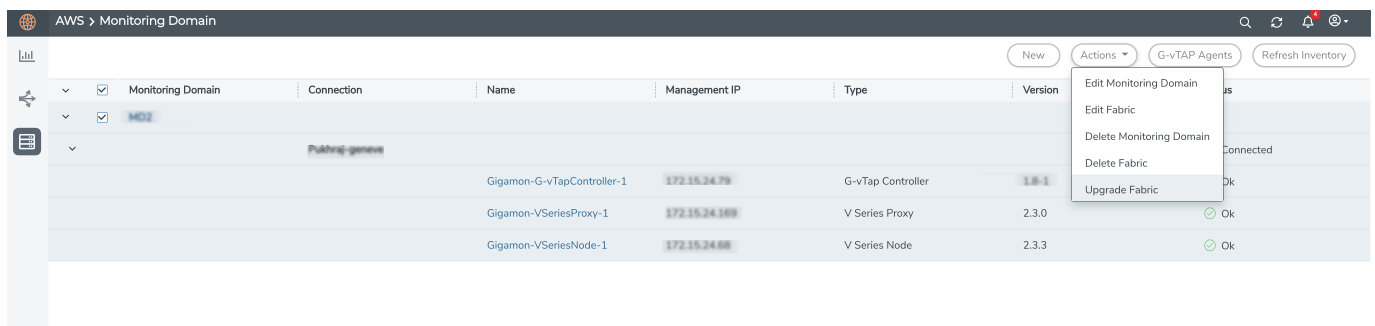
- Launch and replace the complete set of nodes and proxy at a time.
For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VPC, you can upgrade all of them at once. First, the new version of GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes are launched. Then, the old version of V Series Proxy and Nodes are deleted from the VPC.

NOTES:

- When the new version of nodes and proxy are launched, the old version is not deleted by GigaVUE-FM until the new version of node and proxy is launched and the status is changed to **Ok**. Make sure that the instance type of the node and proxy selected during the configuration can accommodate the total number of new and old fabric components present in the VPC. If the instance type cannot support so many Virtual Machines, you can choose to upgrade the fabric components in multiple batches.
- If there is an error while upgrading the complete set of proxy and nodes present in the VPC, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
- Prior to upgrading the GigaVUE V Series Proxy and Nodes, you must ensure that the required number of free addresses are available in the respective subnets. Otherwise, the upgrade will fail.
- Launch and replace the nodes and proxy in multiple batches.
For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

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

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



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

Fabric Nodes Upgrade

V Series Proxy

Upgrade	<input checked="" type="checkbox"/>
Current Version	2.3.0
Image	<input type="text" value="Select an image..."/>
Change Instance Type	<input type="checkbox"/>
Batch Size	<input type="text" value="1"/>

V Series Node

Upgrade	<input checked="" type="checkbox"/>
Current Version	2.3.1
Image	<input type="text" value="Select an image..."/>
Change Instance Type	<input type="checkbox"/>
Batch Size	<input type="text" value="1"/>

4. Select the **Upgrade** checkbox to upgrade the GigaVUE V Series Nodes/Proxy,
5. From the **Image** drop-down list, select the latest version of the GigaVUE V Series Proxy/Nodes.
6. Select the **Change Instance Type** checkbox to change the instance type of the nodes/proxy, only if required.
7. Specify the batch size in the **Batch Size** box to upgrade the GigaVUE V Series Nodes/Proxy.

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

8. Select **Upgrade**.

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

Once the nodes are upgraded successfully, the monitoring session is re-deployed automatically.

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:

- [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.

It supports specific fabric components and features on the respective cloud platforms.

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

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

Traffic Health Monitoring

GigaVUE-FM monitors the traffic health of the entire Monitoring Session and each individual GigaVUE V Series Node in that session. It checks for issues like packet drops or traffic overflows.

When it detects a problem, GigaVUE-FM updates the health status of the related Monitoring Session. It monitors traffic health in near real-time.

The GigaVUE V Series Node tracks traffic levels. If traffic goes above or below the configured threshold, it alerts GigaVUE-FM. Then, GigaVUE-FM uses this data to calculate traffic health.

If you deploy GigaVUE-FM and GigaVUE V Series Nodes in different cloud platforms, you must add the GigaVUE-FM public IP address as the Target Address in the Data Notification Interface on the Event Notifications page.

For details, refer to the section in the *GigaVUE Administration Guide*.

This feature supports GigaVUE V Series Nodes on the respective cloud platforms.

For V Series Nodes:

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

For instructions on creating and applying threshold templates across a Monitoring Session or an application, and viewing the traffic health status, refer to the following topics:

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

Consideration to configure a threshold template

- By default, Threshold Template is not configured to any Monitoring Session. If you wish to monitor the traffic health status, then create and apply threshold template to the Monitoring Session.
- Editing or redeploying the Monitoring Session reapplies all the threshold policies associated with that Monitoring Session.
- Deleting the Monitoring Session clears all the threshold policies associated with that Monitoring Session.
- Threshold configuration is applied before deploying a Monitoring Session and remains even if the session is undeployed.
- After applying threshold template to a particular application, you need not deploy the Monitoring Session again.

Supported Resources and Metrics

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

Resource	Metrics	Threshold types	TriggerCondition
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 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
LoadBalancing	<ol style="list-style-type: none"> 1. Tx Packets 2. Rx Packets 	<ol style="list-style-type: none"> 1. Difference 2. Derivative 	<ol style="list-style-type: none"> 1. Over 2. Under

	3. Packets Dropped		
SSLDecryption	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Application Metadata	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
AMI Exporter	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
5G-SBI	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SBIPOE	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
PCAPNG	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

Create Threshold Templates

To create threshold templates:

1. Go to **Inventory > Resources > Threshold Templates**.

The **Threshold Templates** page appears.

2. Select **Create** to open the New Threshold Template page.

3. Enter the appropriate information for the threshold template as described in the following table:

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

4. Select **Save**. The newly created threshold template is saved. It appears on the **Threshold** templates page.

Apply Threshold Template

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

Apply Threshold Template to Monitoring Session

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

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

Apply Threshold Template to Applications

Applying threshold template across Monitoring Session does not overwrite the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it overwrites the existing threshold value for that particular application.

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

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

Clear Thresholds

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

Clear Thresholds for Applications

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

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

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a Monitoring Session, follow these steps:

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

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

View Health Status

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

View Health Status of an Application

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

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

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

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

View Health Status for Individual GigaVUE V Series Nodes

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

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

Administer GigaVUE Cloud Suite for AWS

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

- [Configure AWS Settings](#)
- [Configure Proxy Server](#)
- [About Events](#)
- [About Audit Logs](#)

Configure AWS Settings

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

1. Go to **Inventory > VIRTUAL > AWS**.
2. Click **Settings > Advanced Setting**.

Refresh interval for instance target selection inventory (secs)	120
Refresh interval for fabric deployment inventory (secs)	900
Number of UCT-Vs per V Series Node	100
Refresh interval for UCT-V inventory (secs)	900
Traffic distribution tunnel range start	8000
Traffic distribution tunnel range end	8512
Traffic distribution tunnel MTU	9001
Permission status purge interval in days	30
Reboot threshold limit for UCT-V Controller down ⓘ	2

3. In the **Advanced Setting** page, you can edit the following details:

Settings	Description
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of EC2 instances in AWS.
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. You can modify the number of instances for the nitro-based instance types
Refresh interval for UCT-V inventory (secs)	Specifies the frequency for discovering the UCT-Vs available in the VPC.
Traffic distribution tunnel range start	Specifies the start range value of the tunnel ID.
Traffic distribution tunnel range end	Specifies the closing range value of the tunnel ID.
Traffic distribution tunnel MTU	Specifies the MTU value for the traffic distribution tunnel.
Permissions status purge interval in days	Specifies the number of days at which the permissions report must be auto purged,
Reboot threshold limit for UCT-V Controller down	Specifies the number of times GigaVUE-FM tries to reach UCT-V Controller, when the UCT-V Controller moves to down state. GigaVUE-FM retries every 60 seconds.

4. Click **Save**.

Configure Proxy Server

Sometimes, the VPC in which the GigaVUE-FM is launched may not have access to the Internet. Without Internet access, GigaVUE-FM cannot connect to the AWS API endpoints. For GigaVUE-FM to connect to AWS, a proxy server must be configured to communicate with the public AWS API endpoints.

NOTE: To configure the proxy server, you must be a user with **fm_super_admin** role or a user with write access to the **Infrastructure Management** category.

To create a proxy server,

1. Go to **Inventory > VIRTUAL > AWS** and select **Settings**.
2. From the Settings drop-down list, select **Proxy Server Configuration**.
3. Select **Add**.
The **Configure Proxy Server** page is displayed.

Configure Proxy Server

Save

Cancel

Alias	Alias
Host	IP Address
Port	0 - 65535
Username	Username
Password	Password
	<input type="checkbox"/> NTLM

4. Select or enter the appropriate information as shown in the following table.

Field	Description
Alias	The name of the proxy server.
Host	The host name or the IP address of the proxy server.
Port	The port number used by the proxy server for connecting to the Internet.
Username	(Optional) The username of the proxy server.
Password	The password of the proxy server.
NTLM	(Optional) The type of the proxy server used to connect to the VPC. On enabling NTLM, enter the following information: <ul style="list-style-type: none"> • Domain—domain name of the client accessing the proxy server. • Workstation—name of the workstation or the computer accessing the proxy server.

5. Select **Save**.

The new proxy server configuration is added to the **Proxy Server Configuration** page. The proxy server is also listed in the AWS Connection page.

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 work on the same principles of access privileges in GigaVUE-FM in which the access rights of a user depend 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>Infrastructure Management: This includes the following cloud infrastructure resources:</p> <ul style="list-style-type: none"> • Cloud Connections • Cloud Proxy Server • Cloud Fabric Deployment • Cloud Configurations • Sys Dump • Syslog • Cloud licenses • Cloud Inventory 	<ul style="list-style-type: none"> • Configure GigaVUE Cloud Components • Create a Monitoring Domain and Launch Visibility Fabric • Configure Proxy Server
<p>Traffic Control Management: This includes the following traffic control resources:</p> <ul style="list-style-type: none"> • Monitoring session • Threshold Template • Stats • Map Library • Tunnel library • Tools library • Inclusion/exclusion Maps 	<ul style="list-style-type: none"> • Create, Clone, and Deploy Monitoring Session • Create and Apply Threshold Template • Add Applications to Monitoring Session • Create Maps • View Statistics • Create Tunnel Endpoints
<p>Third Party Orchestration: This includes the following resource:</p> <ul style="list-style-type: none"> • Cloud Orchestration 	<ul style="list-style-type: none"> • Deploy the fabric components using Third Party Orchestration. Refer to Configure Role-Based Access for Third Party Orchestration for more details on how to create users, roles, and user groups for Third Party Orchestration.

NOTE: Cloud APIs are also RBAC enabled.

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

About Events

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

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

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

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

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

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

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

Controls/ Parameters	Description
Source	The source from where the events are generated. The criteria can be as follows: <ul style="list-style-type: none"> ■ FM - indicates the event was flagged by the GigaVUE-FM fabric manager. ■ VMM - indicates the event was flagged by the Virtual Machine Manager. ■ FM Health - indicates the event was flagged due to the health status change of GigaVUE-FM.
Duration	The timestamp when the event occurred or the duration in which the event occurred. IMPORTANT: Timestamps or the duration are shown in the time zone of the client browser's computer and not the time zone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured time zone.
Scope	The category to which the events belong. Events can belong to the following category: Domain, Node, Card, Port, Stack, Cluster, Chassis, GigaVUE-FM, GigaVUE-VM, and so on. For

Controls/ Parameters	Description
	example, if there is a notification generated for port utilization low threshold, the scope is displayed as Physical Node.
Alarm Type	The type of events that generate the alarms. The types of alarms can be Abnormal Fan Operation, Card Unhealthy, Circuit Tunnel Unhealthy, CPU Over Loaded, Device Upgrade Failed.
Event Severity	The severity is one of Critical, Major, Minor, Warning or Info. Info is informational messages. For example, when power status change notification is displayed, then the message is displayed as Info.
Event Status	The status of the event. The status can be Acknowledged or Unacknowledged.
Event Type	The type of event that generated the events. The type of events can be CPU utilization high, cluster updated, device discovery failed, fan tray changed, netflow generation statistics, and so on.
Affected Entity Type	The resource type associated with the event. For example, when low disk space notification is generated, 'Chassis' is displayed as the affected entity type.
Cluster ID	Enter the Cluster ID.
Affected Entity	The resource ID of the affected entity type. For example, when low disk space notification is generated, the IP address of the node with the low disk space is displayed as the affected entity.
Device IP	The IP address of the device.
Host Name	The host name of the device.
Alias	Event Alias
Monitoring Domain	The name of the Monitoring Domain.
Connection	The name of the Connection.
Show Non-taggable Entities	Enable to display the events for entities that cannot be tagged. For example, Policies, GigaVUE-FM instance and other such entities.
Tags	Select the Key and the Value from the drop-down list.

To filter the alarms and event:

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

About Audit Logs

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

Access Audit Logs

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

All Audit Logs Filter Manage

Filter : none

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

Go to page: 1 of 16 Total Records: 106

The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: <ul style="list-style-type: none"> Log in and Log out based on users. Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details on whether the user was in GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

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

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

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

To filter the audit logs, do the following:

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

Glossary

This appendix lists the AWS terminologies used in this document. To find a brief definition of these terms, refer to [AWS Glossary](#).

- Access Key
- Access key ID
- Amazon API Gateway
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon VPC
- AMI
- AWS
- AWS Identity and Access Management (IAM)
- CIDR block
- EC2 Instances
- Elastic IP address
- Endpoint
- Instance
- Instance type
- Internet gateway
- Key pair
- Secret access key
- Subnet
- Tag
- Target Instance
- Tunnel

Additional Sources of Information

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

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

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.9 Hardware and Software Guides
<p>DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing Edit > Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p>
<p>Hardware</p> <p>how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices</p>
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide

GigaVUE Cloud Suite 6.9 Hardware and Software Guides	
GigaVUE-OS Installation Guide for DELL S4112F-ON	
G-TAP A Series 2 Installation Guide	
GigaVUE M Series Hardware Installation Guide	
GigaVUE-FM Hardware Appliances Guide	
Software Installation and Upgrade Guides	
GigaVUE-FM Installation, Migration, and Upgrade Guide	
GigaVUE-OS Upgrade Guide	
GigaVUE V Series Migration Guide	
Fabric Management and Administration Guides	
GigaVUE Administration Guide	covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide	how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides	
how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms	
GigaVUE V Series Applications Guide	
GigaVUE Cloud Suite Deployment Guide - AWS	
GigaVUE Cloud Suite Deployment Guide - Azure	
GigaVUE Cloud Suite Deployment Guide - OpenStack	
GigaVUE Cloud Suite Deployment Guide - Nutanix	
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)	
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)	
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration	
Universal Cloud TAP - Container Deployment Guide	
Gigamon Containerized Broker Deployment Guide	
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions	
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions	
Reference Guides	
GigaVUE-OS CLI Reference Guide	

GigaVUE Cloud Suite 6.9 Hardware and Software Guides

library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices

GigaVUE-OS Security Hardening Guide

GigaVUE Firewall and Security Guide

GigaVUE Licensing Guide

GigaVUE-OS Cabling Quick Reference Guide

guidelines for the different types of cables used to connect Gigamon devices

GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide

samples uses of the GigaVUE-FM Application Program Interfaces (APIs)

Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices

Sanitization guidelines for GigaVUE Fabric Management Guide and GigaVUE-OS devices.

Release Notes

GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes

new features, resolved issues, and known issues in this release ;
important notes regarding installing and upgrading to this release

NOTE: Release Notes are not included in the online documentation.

NOTE: Registered Customers can log in to [My Gigamon](#) to download the Software and Release Notes from the Software and Docs page on to [My Gigamon](#). Refer to [How to Download Software and Release Notes from My Gigamon](#).

In-Product Help

GigaVUE-FM Online Help

how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

1. Log in to [My Gigamon](#).
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to: documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	
For Online Topics	Online doc link	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>
For PDF Topics	Document Title	<i>(shown on the cover page or in page header)</i>
	Product Version	<i>(shown on the cover page)</i>
	Document Version	<i>(shown on the cover page)</i>
	Chapter Heading	<i>(shown in footer)</i>
	PDF page #	<i>(shown in footer)</i>

How can we improve?	Describe the issue	Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The VÜE Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)