



GigaVUE Cloud Suite for AWS - Deployment Guide

GigaVUE Cloud Suite

Product Version: 6.11

Document Version: 1.0

(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
6.11	1.0	06/17/2025	The original release of this document with 6.11.00 GA.

Contents

GigaVUE Cloud Suite for AWS - Deployment Guide	1
Change Notes	3
Contents	4
GigaVUE Cloud Suite Deployment Guide – AWS	10
Overview of GigaVUE Cloud Suite for AWS	10
Fabric Components	11
GigaVUE-FM	12
GigaVUE V Series Node	13
GigaVUE V Series Proxy	13
UCT-V	13
UCT-V Controller	15
Key Concepts	15
Monitoring Domain	16
Monitoring Session	18
GigaVUE Fabric Components Deployment Options	20
Traffic Acquisition	23
Traffic Processing	35
Traffic Forwarding	40
Egress Tunneled Traffic	40
Replicate Egress Traffic	40
Load Balance Egress Traffic	41
AWS Elastic Load Balancing	41
Inline V Series (AWS)	44
Secure Communication between GigaVUE Fabric Components	47
Architecture	49
Deployment Overview	51
Deployment Planning	52
Identify the Deployment Method	53
GigaVUE-FM Orchestration	53
Third Party Orchestration	53
Identify the AWS Regions	54
Define GigaVUE-FM Deployment Location	54
Identify the Traffic Acquisition Method	54
Identify the Deployment Model	55

Deployment Model for GigaVUE V Series Node	55
Deployment Model for UCT-V Controller	56
Identify the AWS Accounts Involved	57
Centralized vs Decentralized Account Deployment	57
Identify the Subnets Involved	57
Identify the Required IAM Roles, Policies, and Permissions	58
Identify or Create the Necessary Keypairs	59
Identify the UCT-V Deployment Details	59
Identify the UCT-C Deployment Details	59
Deployment Prerequisites	59
Subscribe to GigaVUE Products	60
Licensing for GigaVUE Cloud Suite for AWS	60
Default Trial Licenses	61
Purchase GigaVUE Cloud Suite using CPPO	62
Volume Based License (VBL)	62
AWS Security Credentials	68
AWS Key Pair	68
Subnet and Security Group for Amazon VPC	69
Subnet for VPC	69
Security Group	69
Recommended and Supported Instance Types for AWS	77
Recommended Instance Types	77
Supported Instance Types	77
Role Based Access Control	78
Configure Role-Based Access for Third Party Orchestration	79
Users	80
Role	81
User Groups	82
Configure Tokens	83
Prerequisite	84
Rules and Notes	84
Create Token	85
Revoke Tokens	85
Export Token	86
GigaVUE-FM Version Compatibility	86
Default Login Credentials for GigaVUE Fabric Components	86
Permissions and Privileges (AWS)	87
GigaVUE-FM Instance Multi Account Support Using Amazon STS	87
Minimum Permissions Required for Inline Policies and Basic Authentication	90
Minimum Permissions Required for Acquiring Traffic using the UCT-V	90
Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source	92

Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with GwLB	93
Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source with NwLB	94
Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring	96
Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring with Network Load Balancer	97
Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring and GwLB	99
Minimum Permissions Required for Acquiring Traffic using Inline V Series	100
Check for Required IAM Permissions	101
Points to Note for GigaVUE Cloud Suite for AWS	102
Deployment Options for GigaVUE Cloud Suite for AWS	103
Acquire Traffic using UCT-V - GigaVUE-FM Orchestration	104
Acquire Traffic using UCT-V - Third Party Orchestration	105
Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration	105
Acquire Traffic using Traffic Mirroring – Third Party Orchestration	106
Acquire Traffic using Traffic Mirroring with Network Load Balancer	107
Acquire Traffic using Traffic Mirroring with Gateway Load Balancing	108
Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration	109
Acquire Traffic using Customer Orchestrated Source - Third Party Orchestration	109
Acquire Traffic using Customer Orchestrated Source with Network Load Balancer	110
Acquire Traffic using Customer Orchestrated Source with Gateway Load Balancing	111
Acquire Traffic using Inline V Series Solution	112
Deploy GigaVUE Cloud Suite for AWS	113
Install GigaVUE-FM on AWS	113
Subscribe to GigaVUE-FM	113
Initial Configuration	114
Integrate Private CA	116
Rules and Notes	116
Generate CSR	116
Upload CA Certificate	116
Create AWS Credentials	117
Create a Monitoring Domain	119
Check Permissions while Creating a Monitoring Domain	122
Configure GigaVUE Fabric Components in GigaVUE-FM	125
GigaVUE Fabric Components Configuration – Field References	127

Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM	130
Configure UCT-V	131
Supported Operating Systems for UCT-V	131
Install UCT-V	132
Create Images with UCT-V	149
Uninstall UCT-V	149
Upgrade or Reinstall UCT-V	149
Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode	153
Configure UCT-V Controller in AWS	154
Configure UCT-V in AWS	157
Configure GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS	158
Upgrade GigaVUE Fabric Components using Third Party Orchestration	163
Configure AWS Elastic Load Balancing	164
Configure Network Load Balancer in AWS	164
Configure a Gateway Load Balancer in AWS	168
Create a Target Group	169
Create a Load Balancer	170
Create a Launch Template for Auto Scaling group	170
Create an Auto Scaling group using a Launch Template	171
Configure a Gateway Load Balancer in AWS for Inline V Series Solution	174
Create a Target Group	174
Create a Gateway Load Balancer	175
Create a Launch Template for Inline GigaVUE V Series Node	176
Create an Auto Scaling group using a Launch Template for Inline GigaVUE V Series Node	177
Create a Launch Template for Out of Band GigaVUE V Series Node	178
Create an Auto Scaling group using a Launch Template for Out of Band GigaVUE V Series Node	180
Managing Monitoring Domain	182
Monitoring Domain	183
VPC	184
Fabric	184
UCT-V	185
UCT-V Upgrade	186
Configure UCT-V Features	187
Configure Prefiltering	187
Rules and Notes	188
Create Prefiltering Policy Template	188
Create Precryption Template for UCT-V	189
Rules and Notes:	189

Create Precryption Template for Filtering based on Applications	190
Create Precryption Template for Filtering based on L3-L4 details	190
Configure Secure Tunnel (AWS)	192
Precryption Traffic	192
Mirrored Traffic	193
Prerequisites	193
Notes	193
Configure Secure Tunnel from UCT-V to GigaVUE V Series Node	193
Configure Secure Tunnel between GigaVUE V Series Nodes	195
Adding Certificate Authority	200
Viewing Status of Secure Tunnel for UCT-V	200
Configure Monitoring Session	201
Create a Monitoring Session (AWS)	201
Monitoring Session Page (AWS)	202
Configure Monitoring Session Options (AWS)	204
Configure a Traffic Pre-filter	208
Configure Monitoring Session for Inline V Series	209
Rules and Notes:	209
Create Ingress and Egress Tunnels (AWS)	211
Create Raw Endpoint (AWS)	219
Create a New Map (AWS)	220
Example- Create a New Map using Inclusion and Exclusion Maps	223
Map Library	224
Add Applications to Monitoring Session (AWS)	225
Deploy Monitoring Session (AWS)	225
View Monitoring Session Statistics (AWS)	227
Visualize the Network Topology (AWS)	228
Monitor Cloud Health	229
Configuration Health Monitoring	229
Traffic Health Monitoring	230
Supported Resources and Metrics	231
Create Threshold Templates	233
Apply Threshold Template	234
Clear Thresholds	235
View Health Status	236
Upgrade GigaVUE-FM in AWS	237
Upgrade GigaVUE Fabric Components in GigaVUE-FM	
for AWS	237
Prerequisite	237
Upgrade UCT-V Controller	237
Upgrade between Major Versions	238

Upgrade within the Same Major Version	239
Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy	239
Administer GigaVUE Cloud Suite for AWS	241
Configure AWS Settings	241
Interface Mapping (AWS)	244
Configure Proxy Server	245
Configure Certificate Settings	246
About Events	247
About Audit Logs	249
Migrate Application Intelligence Session to Monitoring Session	250
Post Migration Notes for Application Intelligence	252
Analytics for Virtual Resources	253
Virtual Inventory Statistics and Cloud Applications Dashboard	253
Analytics for Inline V Series Solution	258
Debuggability and Troubleshooting	260
Sysdumps	260
Sysdumps—Rules and Notes	261
Generate a Sysdump File	261
FAQs - Secure Communication between GigaVUE Fabric Components	262
Glossary	265
Additional Sources of Information	266
Documentation	266
How to Download Software and Release Notes from My Gigamon	269
Documentation Feedback	269
Contact Technical Support	270
Contact Sales	271
Premium Support	271
The VUE Community	271
Glossary	272

GigaVUE Cloud Suite Deployment Guide – AWS

This guide describes how to configure GigaVUE Cloud Suite for AWS using the GigaVUE-FM interface. This guide also describes the procedure for setting up the traffic monitoring sessions for AWS using the GigaVUE-FM.

Topics:

- [Overview of GigaVUE Cloud Suite for AWS](#)
- [Deployment Overview](#)
- [Deployment Planning](#)
- [Deployment Prerequisites](#)
- [Points to Note for GigaVUE Cloud Suite for AWS](#)
- [Deployment Options for GigaVUE Cloud Suite for AWS](#)
- [Deploy GigaVUE Cloud Suite for AWS](#)
- [Configure UCT-V Features](#)
- [Configure Monitoring Session](#)
- [Monitor Cloud Health](#)
- [Upgrade GigaVUE-FM in AWS](#)
- [Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS](#)
- [Administer GigaVUE Cloud Suite for AWS](#)
- [Migrate Application Intelligence Session to Monitoring Session](#)
- [Analytics for Virtual Resources](#)
- [Debuggability and Troubleshooting](#)
- [FAQs - Secure Communication between GigaVUE Fabric Components](#)

Overview of GigaVUE Cloud Suite for AWS

GigaVUE Cloud Suite for AWS delivers a powerful cloud-based visibility and analytics solution, ensuring comprehensive network observability whether you're migrating workloads to the cloud or optimizing an existing cloud environment. By eliminating network blind spots, it significantly reduces security and compliance risks while helping remediate performance issues.

GigaVUE Cloud Suite for AWS provides comprehensive solutions to acquire network traffic from workloads running inside the AWS platform. The acquired traffic is selectively copied and mirrored using tunnels to GigaVUE V Series Nodes for further filtering and packet processing before forwarding it to the tools. GigaVUE Cloud Suite for AWS supports multiple ways to acquire traffic from the workloads including GigaVUE Universal Cloud Tap (UCT) and Traffic Mirroring¹ technology.

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 it 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. GigaVUE Enriched Metadata (GEM) enhances network visibility by transforming raw packet data into actionable insights. It extracts, enriches, and delivers metadata to security and analytics tools, enabling faster threat detection, performance optimization, and improved decision-making across hybrid cloud environments. In addition, GEM correlates platform metadata with actual packet data.

Key Capabilities of GigaVUE Cloud Suite for AWS includes:

- Automatic discovery and deployment of visibility nodes in the platform.
- Application of advanced traffic intelligence to optimize tool performance.
- Support for both public cloud and hybrid cloud architectures.
- Integration with AWS APIs for rapid detection of changes in the workloads.
- Ability to extend on-premises security and monitoring tools to AWS environments.

Fabric Components

GigaVUE Fabric Components are the set of resources used to acquire, transport, process and distribute traffic to support your monitoring goals.

GigaVUE Cloud Suite for AWS includes the following fabric components:

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

¹Traffic Mirroring is an Amazon VPC feature that you can use to copy network traffic from an elastic network interface of type interface. You can then send the traffic to out-of-band security and monitoring appliances for content inspection, threat monitoring, and troubleshooting. The security and monitoring appliances can be deployed as individual instances, or as a fleet of instances behind either a Network Load Balancer or a Gateway Load Balancer with a UDP listener. Traffic Mirroring supports filters and packet truncation, so that you can extract only the traffic of interest, using the monitoring tools of your choice.

GigaVUE-FM

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

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

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

GigaVUE-FM can be installed on-premises as a physical or virtual appliance, or, launched from an Amazon Machine Image (AMI) from AWS Marketplace.

GigaVUE-FM manages the configuration of the following components in your Amazon Virtual Private Clouds (VPC):

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

GigaVUE-FM orchestrates the overall GigaVUE Cloud Suite for AWS which allows you to:

- define the areas of your network within which workloads to monitor can be found.
- provide adequate credentials for GigaVUE-FM to access the designated areas in order to discover the workloads to monitor and other related objects.
- define and deploy a visibility policy (Monitoring Session) to acquire traffic from the monitored workloads using the traffic acquisition method of your choice and forward the acquired traffic to available GigaVUE V Series Nodes for processing and forwarding.
- configure GigaVUE V Series Node, which processes traffic acquired from workloads and forwards to tools using specific logic defined as part of the overall visibility policy.
- continuously monitor the designated areas of your network to discover dynamically spawned workloads and automatically apply the same visibility policy to the dynamically spawned workloads if the monitoring selection criteria are met.
- gain comprehensive visibility into their AWS environments, optimize traffic sent to tools, and maintain a consistent security posture across hybrid and multi-cloud deployments.

Refer to [Install GigaVUE-FM on AWS](#) for more detailed information on how to install GigaVUE-FM in AWS.

GigaVUE V Series Node

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

For more information on installing and configuring a GigaVUE V Series Node, refer to [Deployment Options for GigaVUE Cloud Suite for AWS](#) for more detailed information on the various ways of deploying and configuring GigaVUE V Series Nodes.

GigaVUE V Series Proxy

The GigaVUE V Series Proxy is an optional component. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series Nodes.

If GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network, a Proxy can be used. It can also be used if there are a large number of nodes connected to GigaVUE-FM or if you wish to keep the IP addresses of the nodes private. A single GigaVUE V Series Proxy can be launched to provide the GigaVUE-FM network communication to hundreds of GigaVUE V Series Nodes present in private networks behind the Proxy.

Refer to [Deployment Options for GigaVUE Cloud Suite for AWS](#) for more detailed information on the various ways of deploying and configuring GigaVUE V Series Proxy.

UCT-V

UCT-V (earlier known as G-vTAP Agent) is a module that is installed in the VM instance. UCT-V modules are installed into workload VMs and grant the tenant packet-level access in any cloud environment without informing the cloud provider or requiring any assistance from the cloud provider. UCT-V can be installed on both Linux and Windows environments. Packets are mirrored from workload virtual interfaces over to GigaVUE V Series nodes where mapping actions involving filtering and packet transformation takes place.

UCT-V mirrors the selected traffic from a source interface to a destination mirror interface. The mirrored traffic is encapsulated using GRE or VXLAN tunneling and then sent to the GigaVUE Cloud Suite® V Series Node.

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

Single Network Interface Configuration

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

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

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

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

Grant permission to monitor ingress and egress traffic at iface

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

Multiple Network Interface Configuration

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

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

Example of the Linux 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

NOTE: Loop Back Interface configuration is not supported on Windows environment.

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

The UCT-V is offered as a Debian (.deb), Redhat Package Manager (.rpm) package for Linux workloads and a ZIP or MSI for Windows Server workloads. For more information on installing UCT-V on your virtual machines, refer to [Configure 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 has the same version. For example, the UCT-V Controller 6.11.00 can only manage UCT-Vs 6.11.00. If you have the previous version UCT-V still deployed in the EC2 instances, you must configure both the previous version and 6.11.00. 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.

Key Concepts

This section provides the key concepts required for understanding GigaVUE Cloud Suite for AWS.

Refer to the following section for more detailed information:

- [Monitoring Domain](#)
- [Monitoring Session](#)
- [GigaVUE Fabric Components Deployment Options](#)
- [Traffic Acquisition](#)
- [Traffic Processing](#)
- [Traffic Forwarding](#)
- [Egress Tunneled Traffic](#)
- [Replicate Egress Traffic](#)
- [Load Balance Egress Traffic](#)
- [AWS Elastic Load Balancing](#)
- [Inline V Series \(AWS\)](#)
- [Secure Communication between GigaVUE Fabric Components](#)

Monitoring Domain

Your AWS cloud infrastructure may encompass numerous resources spread across multiple AWS accounts and Virtual Private Clouds (VPCs). When implementing GigaVUE Cloud Suite for AWS to monitor specific workloads, it's crucial to limit access to only the necessary parts of your cloud environment.

To clearly define the scope of GigaVUE Cloud Suite for AWS deployment, we introduce the concept of a Monitoring Domain. This domain establishes a boundary within your AWS cloud environment where the visibility solution will be implemented.

Monitoring Domain

A Monitoring Domain in AWS is typically defined by:

- AWS accounts
- Regions
- VPCs

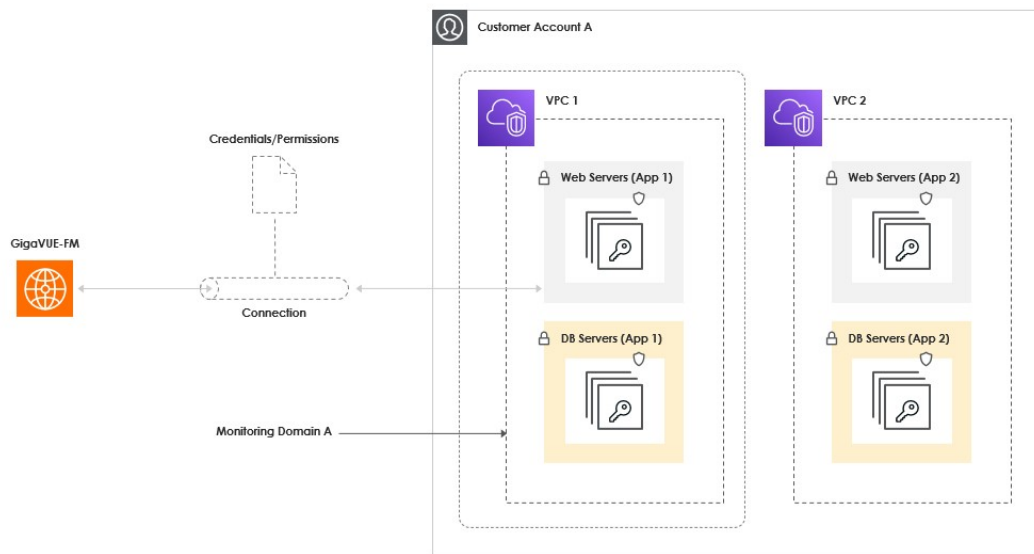
GigaVUE Cloud Suite for AWS interacts only with resources within the specified accounts and VPCs listed in a Monitoring Domain.

Connection

To further refine access control, we introduce the concept of a Connection. This is associated with a set of credentials and permissions that precisely limit what GigaVUE Cloud Suite for AWS can access. By utilizing Connections, you can deploy GigaVUE Cloud Suite for AWS to the appropriate resources with minimal credentials and permissions, enhancing security and control.

These concepts of Monitoring Domain and Connection work together to provide a granular approach to deploying and managing GigaVUE Cloud Suite for AWS within your cloud infrastructure, ensuring that you maintain control over which parts of your environment are accessible to the monitoring solution.

The following diagram provides more details about the concepts of Monitoring Domain and Connection:



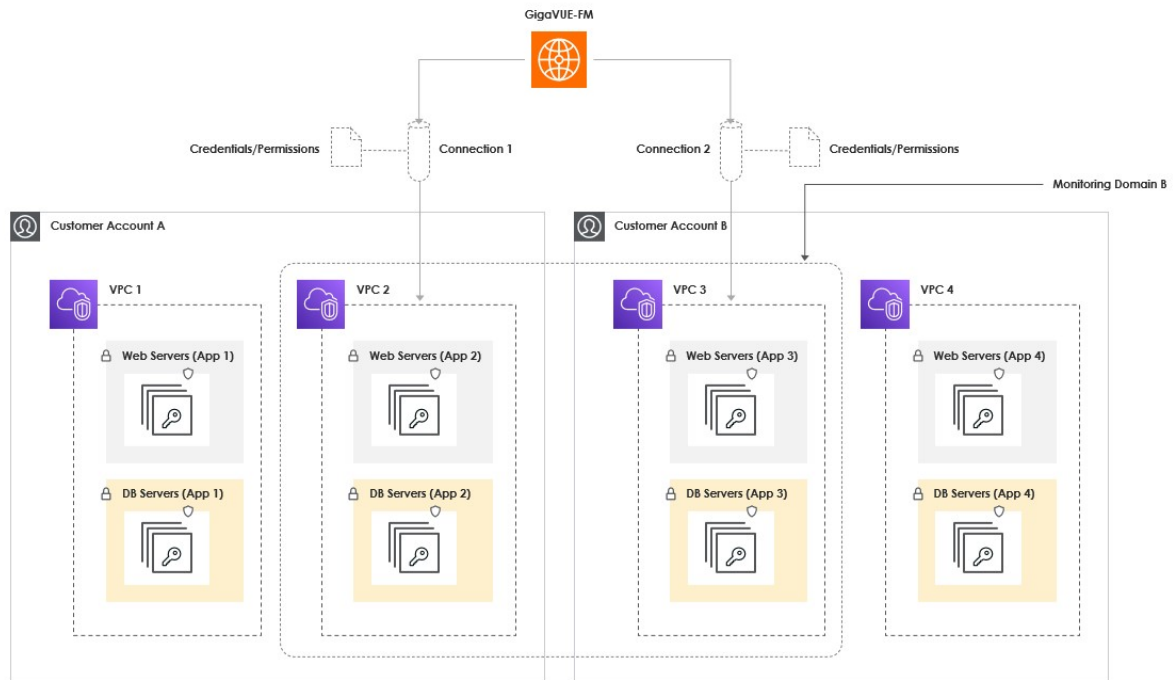
© 2017-2025 Gigamon Inc. All rights reserved.

In the above diagram, you are defining Monitoring Domain A and associating it with a connection object to it to provide the necessary credentials and permissions to access VPC 1 in your account A. GigaVUE-FM uses this connection to access VPC 1 in order to discover the required resources, such as workload VMs, subnets, security groups, key pairs, and more. GigaVUE-FM helps you easily deploy and configure GigaVUE Fabric Components and platform features to acquire traffic from the VMs you select, process it using GigaVUE V Series Nodes, and forward it to your analysis tools.

The Monitoring Domain defines a clear boundary within which GigaVUE-FM operates. This ensures both security and performance goals are achieved. In this case, you do not want GigaVUE-FM to access any VPCs other than VPC 1, GigaVUE-FM complies with your intent by restricting its operations strictly to the boundary defined by the Monitoring Domain. Additionally, the actions of GigaVUE-FM are further restricted by the credentials and permissions you provide through the connection associated with the Monitoring Domain.

The Monitoring Domain is a logical concept. Its definition is based on concepts defined by the underlying cloud platform. On AWS, you can define any boundary using accounts and VPCs.

The following diagram illustrates a Monitoring Domain encompassing resources in VPCs in two different AWS accounts:



© 2017-2025 Gigamon Inc. All rights reserved.

In the above diagram, Monitoring Domain B is created to monitor the resources in VPC 2 and VPC 3, which are from two different accounts. GigaVUE-FM uses Connection 1 to access the resources in VPC 2 and Connection 2 to access the resources in VPC 3. In this case, GigaVUE-FM will not have access to the resources in VPC 1 and VPC 4.

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

Monitoring Session

GigaVUE Cloud Suite for AWS offers a sophisticated approach to network visibility through customizable Monitoring Sessions. These sessions allow you to tailor your visibility strategy with precision, focusing on specific aspects of your AWS environment:

Workload Selection

You can define the scope of your monitoring by selecting target workloads by:

- Choose VMs or pods based on various criteria
- Utilize filters such as VPC name, subnet, IP address, VM tags, or pod labels
- Align selections with your predefined Monitoring Domain boundaries

Traffic Acquisition

You can specify the types of traffic to capture from selected sources:

- Options vary depending on the chosen acquisition technology
- Customize traffic selection to match your monitoring requirements

Traffic Processing

You can leverage a comprehensive suite of traffic processing features:

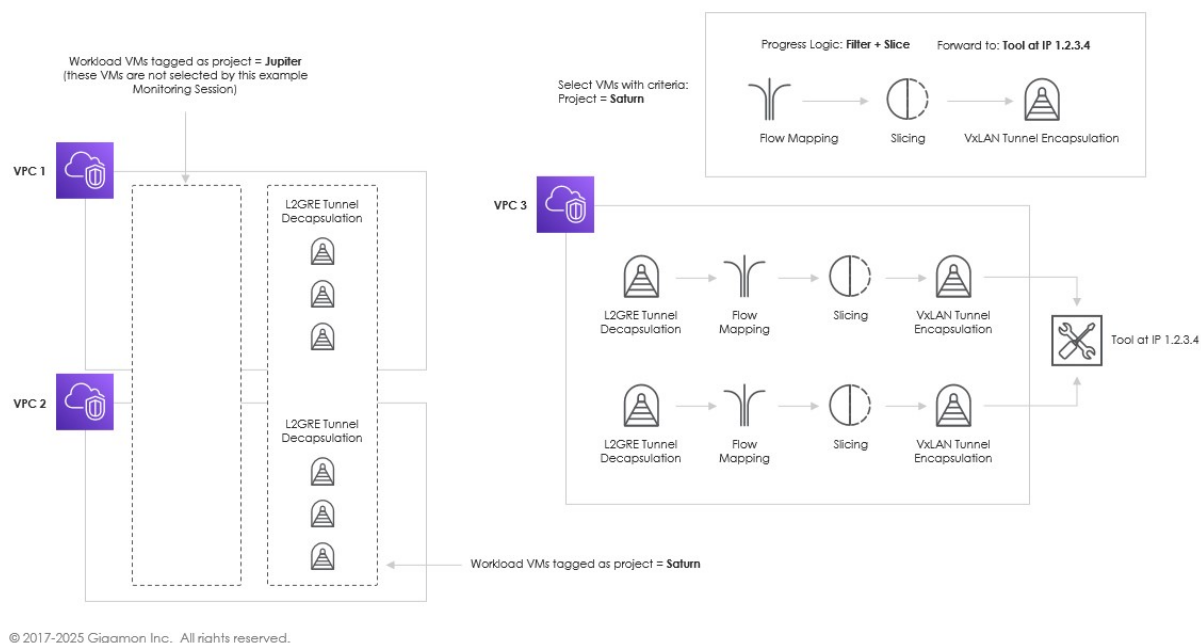
- Apply various GigaSMART Applications to refine and optimize captured traffic.
- Enhance security and efficiency of your monitoring solutions
- Tailor the data sent to analysis tools for maximum relevance

Configuring these elements within a Monitoring Session allows you to create a finely-tuned visibility policy that aligns perfectly with your specific monitoring objectives in AWS environments.

Once you define a Monitoring Session, it automatically configures the required traffic acquisition points, processing, and forwarding logic. This ensures that traffic collected from the workloads you want to monitor is pre-filtered and processed by GigaVUE V Series Nodes and then forwarded to your analysis tools.

The following diagram provides a high-level overview of an example Monitoring Session:

Example: Visibility Policy Defined as Monitoring Session A



The above diagram shows a Monitoring Session is defined to monitor (select) VMs for project Saturn. These VMs are tagged as project = "Saturn". Traffic from these selected VMs is filtered first by the GigaVUE V Series Nodes, where each packet is then sliced to reduce traffic volume before being forwarded to your analysis tool at IP 1.2.3.4. These details are configured in a monitoring session using GigaVUE-FM, representing your intent to monitor specific workload VMs.

Once you define this monitoring session, you deploy it into a Monitoring Domain to establish actual traffic flows as per your intent. In this case, GigaVUE-FM discovers all the VMs in the given Monitoring Domain, select the VMs matching your defined criteria (project = "Saturn"), and configure the necessary settings to acquire traffic using your chosen method (e.g., UCT-V, traffic mirroring). The acquired traffic is then sent to the available GigaVUE V Series Nodes for processing based on your defined logic (e.g., filtering and packet slicing) before being tunneled to your analysis tool.

After the Monitoring Session is deployed into your Monitoring Domain, GigaVUE-FM continue to monitor the changes in your environment. If new VMs are launched in Project Saturn, they will be automatically tapped, traffic processed, and forwarded to the tool based on your defined visibility policy (Monitoring Session).

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

GigaVUE Fabric Components Deployment Options

GigaVUE Fabric Components are deployed in your AWS cloud environment and can be configured to support the visibility policies you have configured.

There are two different approaches to deploying GigaVUE Fabric Components:

- [GigaVUE-FM Orchestrated Fabric Deployment](#)
- [Third Party Orchestrated Fabric Deployment](#)

GigaVUE-FM Orchestrated Fabric Deployment

In GigaVUE-FM Orchestrated Fabric Deployment approach you can define Monitoring Domains and then deploy the fabric components like UCT-V Controllers, GigaVUE V Series Nodes, and GigaVUE V Series Proxy using the GigaVUE-FM GUI.

Third Party Orchestrated Fabric Deployment

GigaVUE fabric components support flexible deployment options beyond the standard GigaVUE-FM deployment method. You can use third-party orchestration tools, such as Terraform or custom scripts, to deploy these components, enabling seamless integration with existing infrastructure management workflows.

When deploying fabric components through an external orchestration system, you can provide the necessary parameters for self-registration with GigaVUE-FM. Once registered, GigaVUE-FM serves as the central point for configuring Monitoring Sessions and associated services, ensuring unified management and control of the deployed fabric.

This approach allows organizations to:

- Leverage existing orchestration workflows for automated deployment.
- Ensure seamless integration with infrastructure management tools.
- Maintain centralized monitoring and service configuration through GigaVUE-FM.

By combining customized deployment processes with centralized visibility management, this method enhances flexibility while maintaining control over network monitoring infrastructure.

Refer to the following section for more information on the different ways of deploying the fabric components using Third Party Orchestration:

- [User Driven Fabric Deployment](#)
- [Automated Fabric Deployment](#)

User Driven Fabric Deployment

With a user-driven fabric deployment approach, you can deploy the fabric components using a combination of the cloud platform's UI or CLI. To use user-driven fabric deployment method, follow these high-level steps:

1. Deploy GigaVUE-FM

Deploy the GigaVUE-FM in your AWS cloud environment using the AWS Marketplace or AWS EC2 console.

2. Create a Monitoring Domain

Log into GigaVUE-FM and create a Monitoring domain to define the boundaries for your fabric components.

3. Deploy the Fabric Components

Use AWS UI to deploy the following components into a VPC within the Monitoring Domain:

- a. UCT-V Controller: Deploy this if you are using UCT-V to acquire traffic.
- b. GigaVUE V Series Nodes: Deploy these for traffic processing.
- c. GigaVUE V Series Proxy: Deploy this if required for your environment.

4. Monitor Workloads in EKS Clusters (if applicable)

For monitoring workloads in EKS clusters, launch the UCT-C and UCT-C Controller services using the EKS console or AWS CLI.

5. Configure AWS Load Balancers (if applicable)

If you are using AWS load balancers, launch these resources from the AWS console along with any associated resources, such as an auto-scaling group.

By following these steps, you can efficiently deploy and configure the fabric components in your AWS environment.

Automated Fabric Deployment

When using Infrastructure as Code (IaC) methodology, deploying a fabric component can be fully automated using scripts written in tools such as Terraform, Ansible, or CloudFormation. To use the automated fabric deployment method, follow these high-level steps:

1. Deploy GigaVUE-FM

Launch GigaVUE-FM in your chosen environment, such as an AWS cloud environment or your private cloud.

2. Deploy Workload VMs with UCT-V

- Launch workload VMs with the UCT-V pre-installed. Alternatively, configure your scripts to install UCT-V dynamically after the workload VMs are successfully launched.
- Configure each UCT-V with the IP address of FM. Once initialized, each UCT-V sends a REST API call to GigaVUE-FM to register itself.

3. Deploy UCT-V Controller and GigaVUE V Series Nodes

- Launch UCT-V Controller and GigaVUE V Series Nodes as dedicated VMs in your AWS environment.
- Configure each controller and node with the IP address of GigaVUE-FM and any other relevant information needed to register with FM after initialization.

4. Deploy UCT-C and UCT-C Controllers (if applicable)

- For monitoring workloads in EKS clusters, deploy UCT-C and UCT-C Controllers in the required clusters.
- Configure these components so they automatically register with GigaVUE-FM once initialized.

By following these steps, you can efficiently deploy and configure the fabric components

Traffic Acquisition

You can acquire traffic from multiple virtual machines and container pod instances using UCT-V, UCT-C(for containers), 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.

Refer to the following topics for more detailed information:

- [Virtual Machine Based Workloads](#)
- [Container Based Workloads](#)
- [Packet Mirroring](#)
- [Precryption](#)
- [Secure Tunneling to GigaVUE V Series Nodes](#)

Virtual Machine Based Workloads

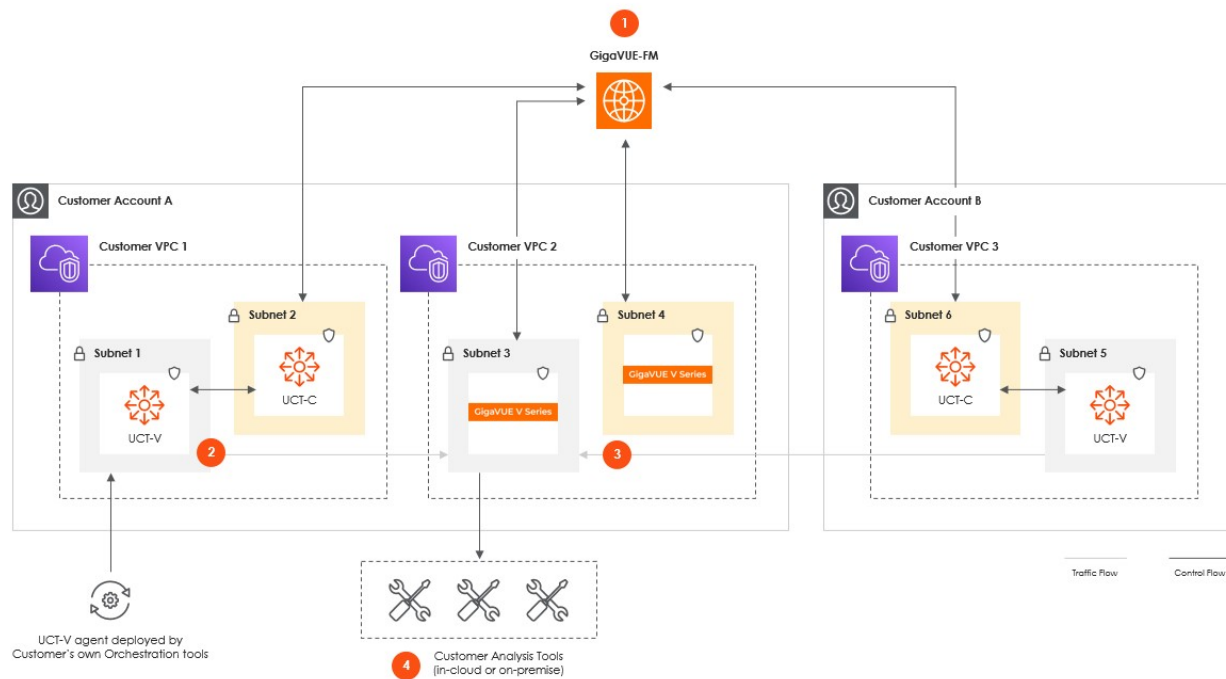
You can acquire traffic for Virtual Machines using the following ways:

- [Traffic Acquisition Method using UCT-V](#)
- [Traffic Acquisition Method using Traffic Mirroring](#)
- [Traffic Acquisition Method using Customer Orchestrated Source](#)

Traffic Acquisition Method using UCT-V

UCT-V can be deployed in various compute instances to mirror production traffic and send to GigaVUE V Series Nodes for further processing and distribution to monitoring and observability tools.

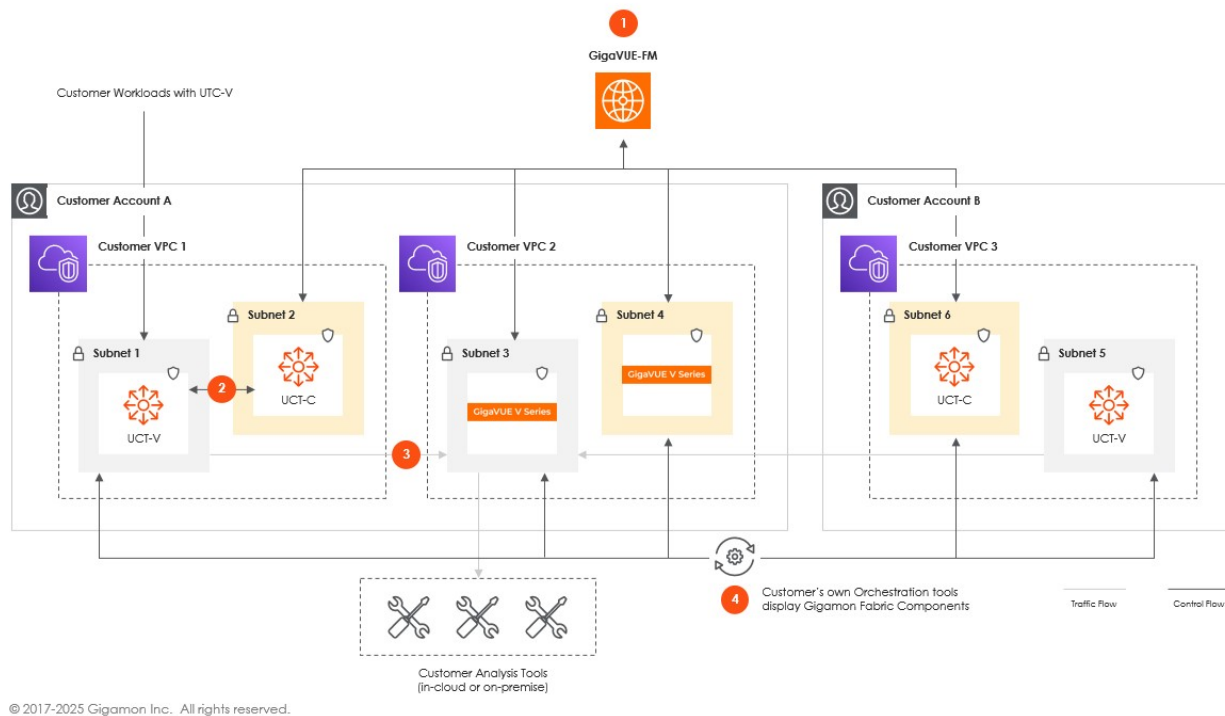
Deploying Fabric Components using GigaVUE-FM



This diagram illustrates the deployment of fabric components across multiple AWS accounts, enabling traffic acquisition, processing, and forwarding to your analysis tools. GigaVUE-FM establishes control flows across accounts and VPCs, ensuring seamless integration and centralized management. GigaVUE-FM orchestrates traffic acquisition and processing by communicating with deployed components, including UCT-Vs, UCT-V Controllers, GigaVUE V Series Nodes, and Proxies.

UCT-V Controller orchestrates the communication between installed on workload VMs, captures the traffic, and forwards the traffic to GigaVUE V Series Nodes. This traffic is processed by GigaVUE V Series Nodes before being forwarded to analysis tools in the cloud or on-premises.

Deploy Fabric Components using Third Party Orchestration



Traffic Acquisition Method using Traffic Mirroring

With VPC Traffic Mirroring, 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 Controller.

VPC Peering is required to send mirrored traffic from other VPCs into a centralized GigaVUE V Series deployment.

- UCT-V Controller configuration is not applicable for VPC Traffic Mirroring.
- Traffic Mirroring does not support cross-account solutions without a load balancer.
- For VPC Traffic Mirroring option, additional permissions are required. Refer to the [Permissions and Privileges \(AWS\)](#) topic for details.
- 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.

Refer to the following Gigamon Validated Design for more detailed information on how to use Application Filtering Intelligence and Slicing with Traffic Mirroring:

- [AWS Traffic Mirroring with Application Filter Intelligence and Slicing \(6.3\)](#)

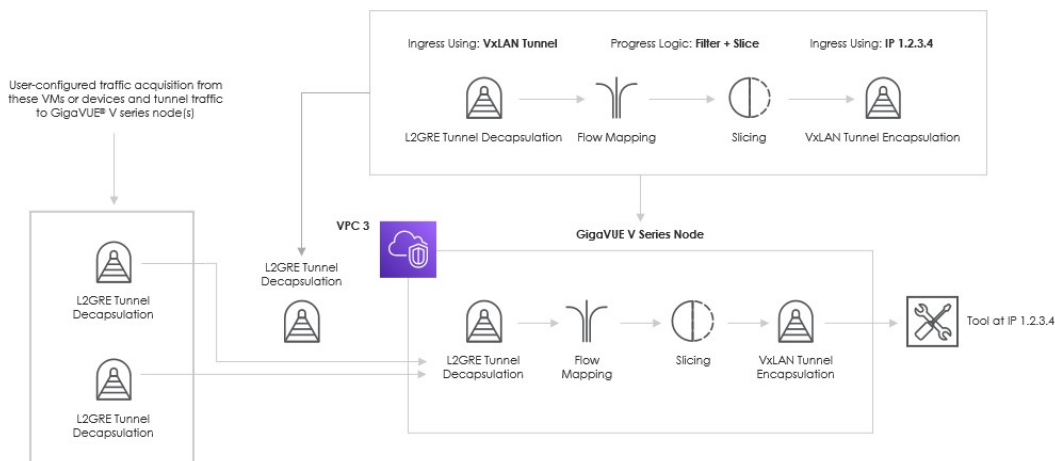
Traffic Acquisition Method using Customer Orchestrated Source

Customer Orchestrated Source is a traffic acquisition method that allows you to tunnel traffic directly to the GigaVUE V Series Nodes. In cases where UCT-V or Traffic Mirroring cannot be configured due to firewall or other restrictions, you can still leverage GigaVUE Cloud Suite features to efficiently process and distribute acquired traffic to the tools.

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

The following diagram provides more details on how customer orchestrated source works:

Example: Monitoring Session for User-Configured Sources



© 2017-2025 Gigamon Inc. All rights reserved.

Ingress Tunneled Traffic

With user configured traffic acquisition, several tunnel types are available for user to ingress traffic into V Series nodes for processing: VxLAN, L2GRE or ERSPAN. User chooses the type and detailed configuration of ingress tunnel endpoint that works best in their environment.

If you 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 Controller. You must create this tunnel feed and point it to the GigaVUE V Series Node(s).

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.

Refer to [Create a Monitoring Domain](#) for more detailed information on how to select **Traffic Acquisition Method** as **Customer Orchestrated Source**.

Container Based Workloads

GigaVUE V Series Nodes can be used to process traffic from a container environment. For container based work loads UCT-C deployed within the Kubernetes environment captures traffic and forwards it to the GigaVUE V Series Nodes which is deployed in VMs, for advanced processing, such as filtering or slicing, before forwarding it to analysis tools. Refer to Universal Cloud TAP - Container Deployment Guide for instructions on UCT-C deployment.

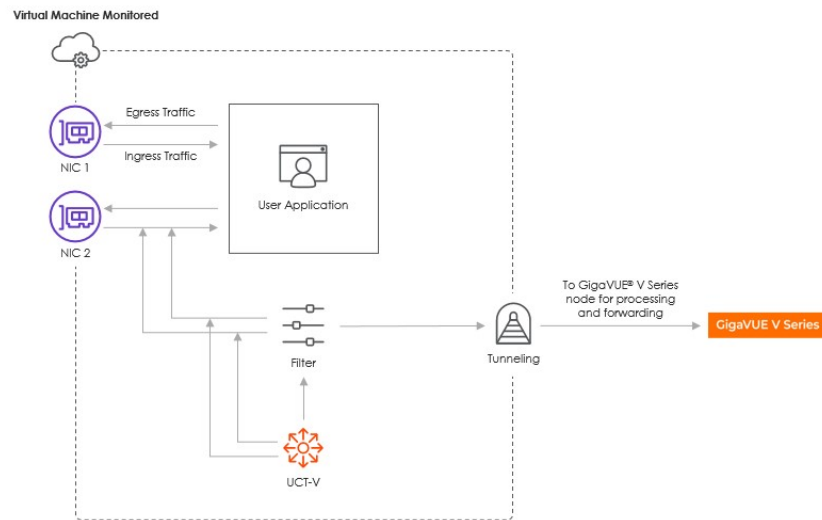
Packet Mirroring

Packet Mirroring is one of the fundamental ways to acquire traffic from the workloads (VMs or pods) for monitoring. Packet mirroring clones the network packets directly from network interfaces of selected workloads and sends them to a destination for processing and analysis. Packets can be selectively mirrored from some or all the network interfaces of the workloads. Packet mirroring can also be configured to mirror packets only for ingress traffic, or only for egress traffic or both.

GigaVUE Cloud Suite for AWS also supports UCT-V based packet mirroring as well as cloud platform native packet mirroring capabilities such as Traffic Mirroring.

How Packet Mirroring Works

The following diagram illustrates how packet mirroring works using UCT-V.



© 2017-2025 Gigamon Inc. All rights reserved.

To acquire traffic from a Virtual Machine using UCT-V, install UCT-V into the VMs that need to be monitored. Refer to [Configure UCT-V](#) for more detailed information on how to install UCT-Vs. After creating and deploying a Monitoring Session in a Monitoring Domain using UCT-V as traffic acquisition method, GigaVUE-FM sends proper configuration details to all UCT-Vs running inside the VMs selected to mirror packets from network interfaces configured for mirroring. Mirrored packets can be filtered by defined criteria and tunneled out to GigaVUE V Series Nodes for processing and forwarding.

Prefilter Mirrored Traffic

NOTE: Prefiltering is supported on UCT-V for Windows systems and Linux systems running Kernel version 4.18 or later.

The mirrored traffic from the packet mirroring can be filtered before tunneling it to the GigaVUE V Series Nodes using a filtering criteria in the Monitoring Session. This helps reduce the volume of mirrored traffic sent to the analysis tool. UCT-V supports a range of criteria to acquire and forward the traffic most relevant to your monitoring needs:

- Layer 3 filters: IPv4 source IP, IPv4 destination IP, IPv6 source IP, IPv6 destination IP and protocol
- Layer 4 filters: source port, destination port

Refer to [Configure Prefiltering](#) for more detailed information and step-by-step instructions on how to configure Prefiltering.

Precryption

License: Requires **SecureVUE Plus** license.

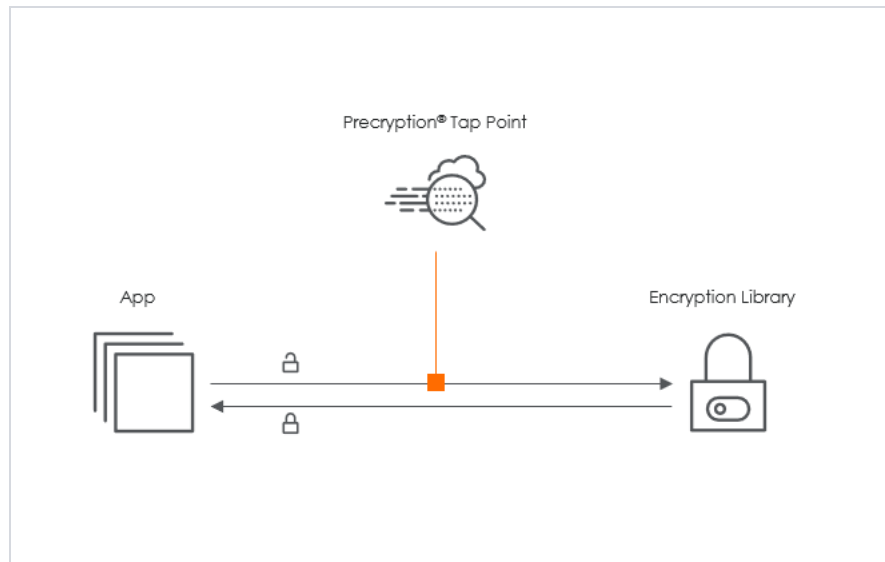
Gigamon Precryption™ technology¹ redefines security for virtual, cloud, and containerized applications, delivering plain text visibility of encrypted communications to the full security stack without the traditional cost and complexity of decryption.s

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](#)

How Gigamon Precryption Technology Works

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



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

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

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

Why Gigamon Precryption

GigaVUE Universal Cloud Tap with Precryption technology is a lightweight, friction-free solution that eliminates blind spots present in modern hybrid cloud infrastructure. It provides East-West visibility into virtual, cloud, and container platforms. It delivers unobscured visibility into all encryption types, including TLS 1.3, without managing and maintaining decryption keys. IT organizations can now manage compliance, keep private communications private, architect the necessary foundation for Zero Trust, and boost security tool effectiveness by a factor of 5x or more.

Key Features

The following are the key features of this technology:

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

Key Benefits

The following are the key benefits of this technology:

- Eliminate blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.

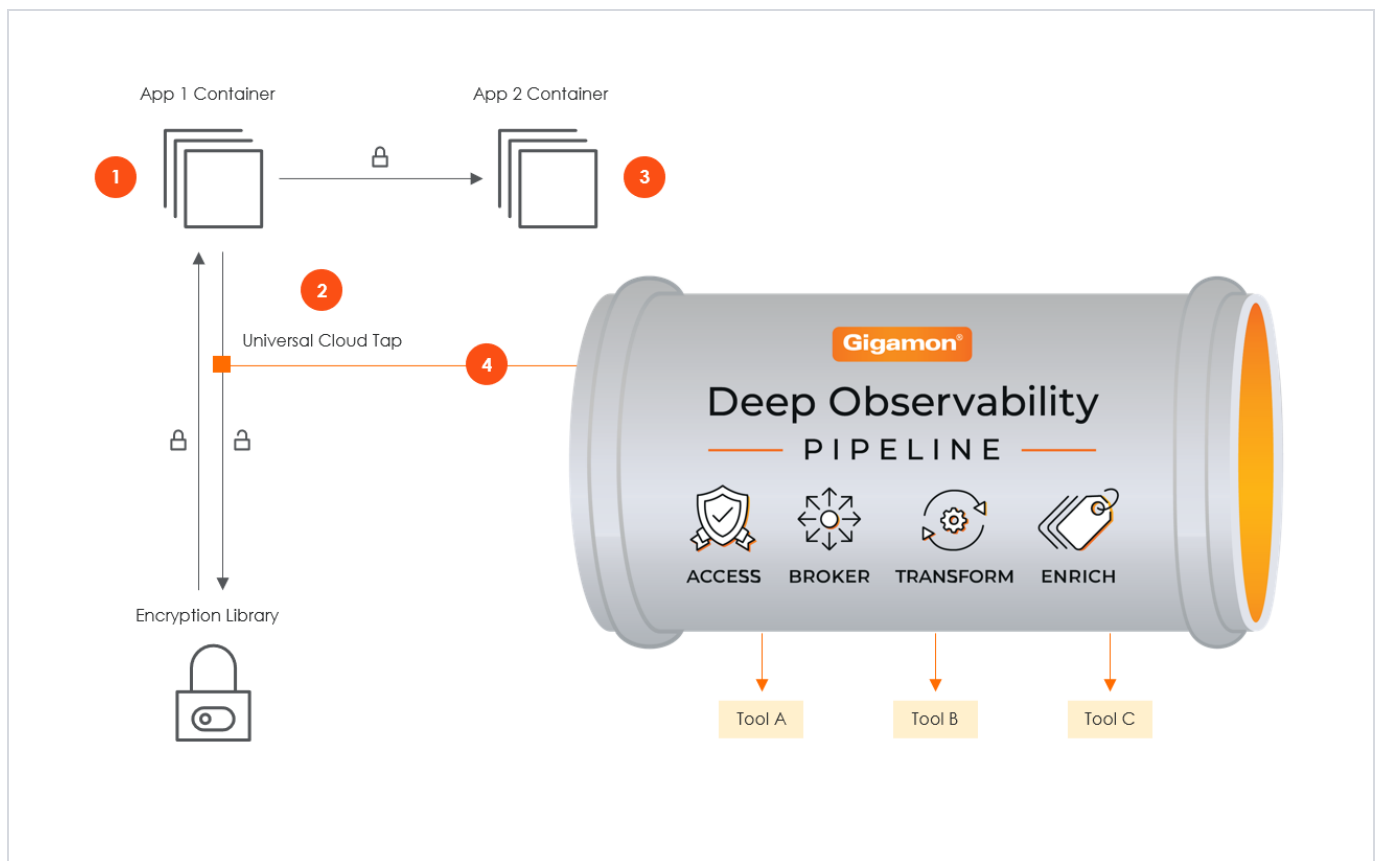
- Monitor application communications with an independent approach that enhances development team velocity.
- Extend security tools' visibility to all communications, regardless of encryption type.
- Achieve maximum traffic tapping efficiency across virtual environments.
- Leverage a 5–7x performance boost for security tools by consuming unencrypted data.
- Support a Zero Trust architecture founded on deep observability.
- Maintain privacy and compliance adherence associated with decrypted traffic management.

How Gigamon Precryption Technology Works

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

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

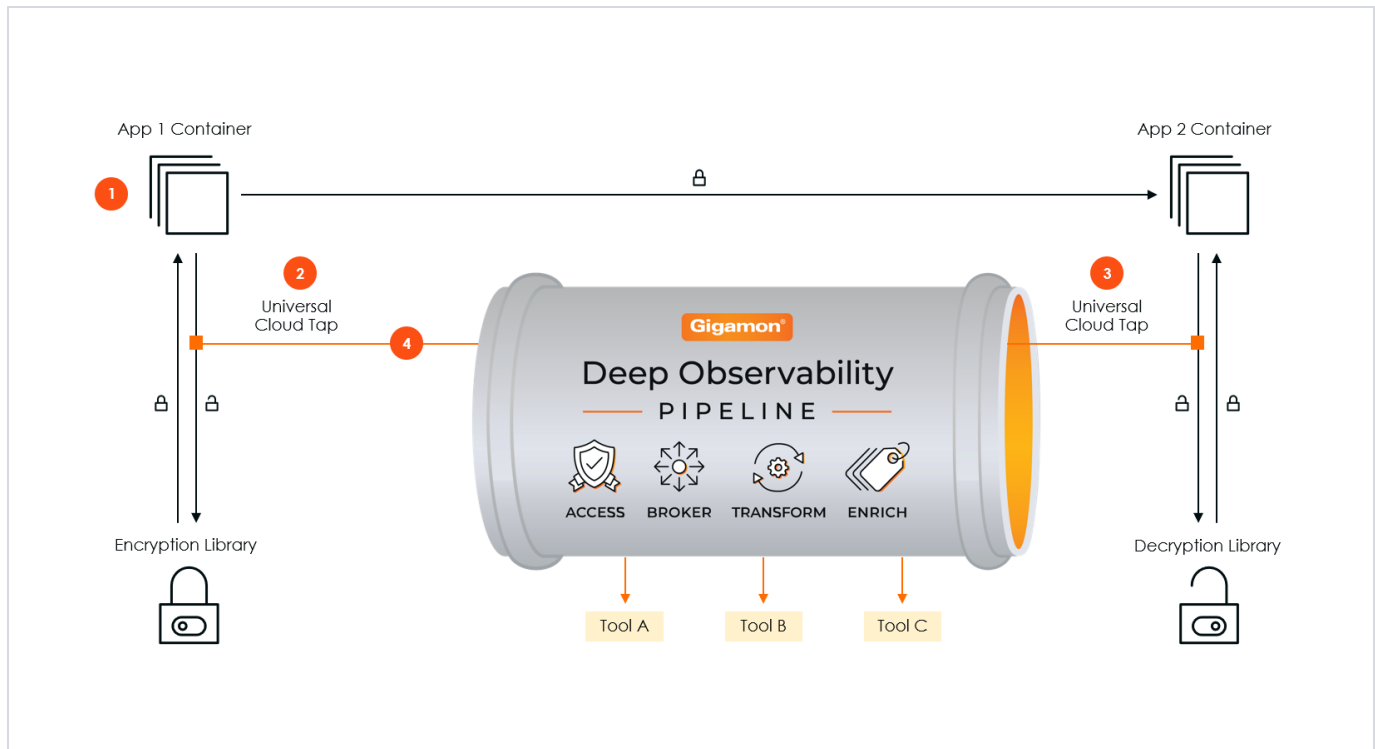
Precryption Technology on Single Node



1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.

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

Precryption Technology on Multi-Node



1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption, gets a copy of this message before it's encrypted on the network.
3. Optionally, GigaVUE UCT enabled with Precryption can also acquire a copy of the message from the server end after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates them in a tunnel, and forwards them to V Series in the deep observability pipeline. There, they are further enriched, transformed, and delivered to tools without further decryption.

Supported Platforms

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

Platform Type	Platform
Public Cloud	<ul style="list-style-type: none"> • AWS • Azure • GCP (via Third Party Orchestration)
Private Cloud	<ul style="list-style-type: none"> • OpenStack • VMware ESXi (via Third Party Orchestration only) • VMware NSX-T (via Third Party Orchestration only)

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

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

Prerequisites

Points to Note

- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x.
- For UCT-C, worker pods should always have libssl installed to ensure that UCT-C Tap can tap the Precryption packets from the worker pods whenever libssl calls are made from the worker pods.
- For GigaVUE-FM, 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.
- Precryption is supported only on Linux systems running Kernel version 4.18 or later.

License Prerequisite

- Precryption™ requires a SecureVUE Plus license.

Supported Kernel Version

Precryption is supported for Kernel Version 4.18 and above for all Linux and Ubuntu Operating Systems. For the Kernel versions below 4.18, refer to the following table:

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

For more details, refer to [Gigamon TV](#).

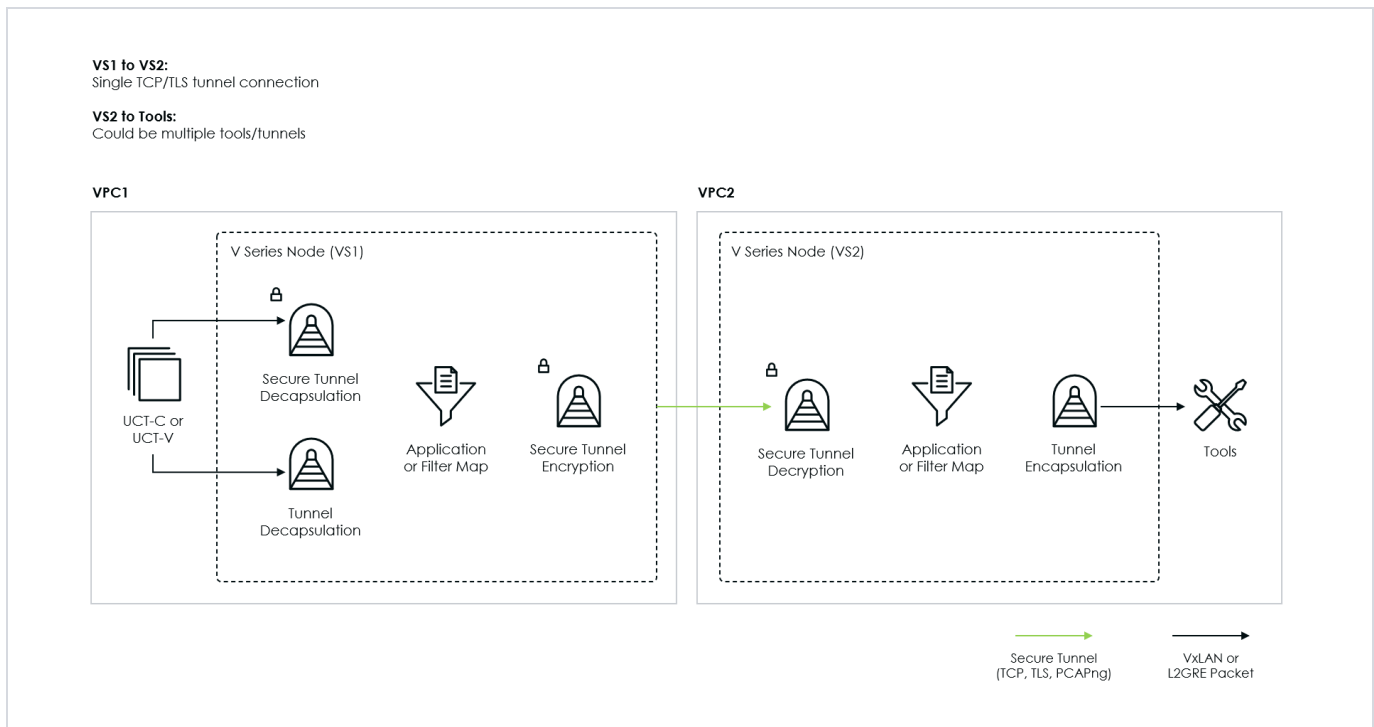
Secure Tunneling to GigaVUE V Series Nodes

Secure Tunnels securely transfer the cloud-captured packets on UCT-V and UCT-C to a GigaVUE V Series Node . The data from UCT-V and UCT-C are encapsulated in PCAPng format, and the encrypted data is sent over a TLS connection to a GigaVUE V Series Node.

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

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

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



Supported Platforms

Secure Tunnels are supported on:

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

Refer to [Configure Secure Tunnel \(AWS\)](#) for instructions on how to configure Secure tunnels.

Traffic Processing

GigaVUE Cloud Suite for AWS provides a comprehensive set of applications that allows you to build efficient and effective visibility solutions. These applications:

- Reduce the traffic volume by applying user-defined filtering criteria, removing duplicate copies of packets, or removing a significant portion of each packet. This helps in increasing the efficiency of analysis tools by focusing on the “right” information carried in network packets.
- Mask sensitive information to meet regulatory compliance requirements.

- Extract metadata information such as NetFlow Generation and a vast array of other types of metadata.
- Remove different layers of headers in nested packets so that analysis tools can easily access the real payload.

This section provides detailed information on the following topics:

- [Supported Applications](#)
- [Flexible Application Chaining](#)

Supported Applications

The following table provides an overview of the applications included in GigaVUE Cloud Suite for AWS:

Parameter	Description
Application Filtering Intelligence	Application Filtering Intelligence allows you to filter traffic based on the application (such as YouTube, Netflix, Sophos, or Facebook) or application family (such as antivirus, web, erp, or instant-messaging). Application Filtering Intelligence enables advanced traffic filtering based on Layer 7 applications, providing the ability to fine-tune your network visibility. With this capability, you can optimize tool performance by excluding high-volume, low-risk traffic from being sent to your monitoring tools. At the same time, you can prioritize and route high-risk or critical traffic of interest to the appropriate tools for detailed analysis, ensuring efficient resource utilization and timely response to potential threats or incidents.
Adaptive Packet Filtering (Part of Application Filtering Intelligence)	Adaptive Packet Filtering (APF) delivers advanced capabilities to analyze and manage traffic flows with precision. APF enables you to inspect any part of a packet, including its payload, and take intelligent actions such as forwarding, dropping, or masking the flow. This feature supports filtering across complex encapsulation headers, such as VXLAN, ERSPAN, GRE, Nested VLANs, MPLS, VN-Tag, and more. Additionally, it allows traffic to be filtered based on inner packet contents within these encapsulated flows, offering unparalleled granularity in traffic control. APF is also session-aware, allowing you to define search patterns using regular expressions (RegEx) or strings. Once a match is detected, APF can apply actions to the entire session, such as forwarding it to specific tools or completely dropping it from the monitoring pipeline.
Application Session Filtering (Part of Application Filtering Intelligence)	Application Session Filtering (ASF) provides advanced capabilities to identify and filter network flows based on flexible user-defined criteria. By leveraging powerful regular expressions (RegEx), ASF allows you to define precise patterns to match specific flow characteristics. ASF examines one or more packets within a flow session to determine if the flow aligns with your defined criteria. Once a match is identified, all packets within that session are forwarded for analysis, ensuring that only relevant traffic reaches your tools.
Application Metadata Intelligence	Application Metadata Intelligence allows you to export metadata from applications that are detected in the network traffic. The records can be

Parameter	Description
	exported to a collector either in IPFIX or CEF format
Application Metadata Exporter	Application Metadata Exporter (AMX) application converts the output from the Application Metadata Intelligence (AMI) in CEF format into JSON format and sends it to the cloud tools and Kafka.
Application Visualization	Application Visualization identifies and monitors all applications contributing to the network traffic and reports on the total applications and the total bandwidth they consume over a select period. Application Visualization allows you to identify more than 3,500 applications.
De-Duplication	De-duplication application targets, identifies, and eliminates duplicate packets, blocking unnecessary duplication and sending optimized flows to your security and network monitoring tools. De-duplication lets you detect and choose the duplicate packets to count or drop in a network analysis environment.
ERSPAN Tunnel Decapsulation	ERSPAN Tunnel Decapsulation application removes the protocol header added by ERSPAN tunnel to extract the original user data packet.
Map	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.
GENEVE Decapsulation	The GENEVE Decapsulation application removes the protocol header added by the GENEVE tunnel to extract the original user data packet.
Header Stripping	Header Stripping application efficiently examines packets for specified headers, such as MPLS, VLAN, VXLAN, VN-TAG, and GRE, and removes them before sending the packets to the appropriate security and analysis tools.
L2GRE Tunnel Decapsulation	The L2GRE Tunnel Decapsulation application removes the protocol header added by the L2GRE tunnel to extract the original user data packet.
L2GRE Tunnel Encapsulation	The L2GRE Tunnel Encapsulation application wraps a user packet within an L2GRE protocol-compliant packet for transport to the next hop for processing or analysis.
Load Balancing	A Load-Balancing application allows you to distribute traffic to multiple tools for analysis. The application not only load-balances the traffic among the tools; it can also handle the distribution in a stateful manner to ensure packets of the same flow are always distributed to the same tool.
Masking	Masking application allows you to overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis.
Packet Slicing	Packet Slicing allows you to truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. Slicing operations are typically configured to preserve specific packet header information, allowing effective network analysis without the overhead of storing full packet data.
Out of Band SSL/TLS Decryption	SSL/TLS decryption application delivers decrypted traffic to out-of-band tools that can then detect threats entering the network.

Parameter	Description
UDPGRE Tunnel Decapsulation	UDPGRE Tunnel Decapsulation application removes the protocol header added by the UDPGRE tunnel to extract the original user data packet.
VXLAN Tunnel Decapsulation	VXLAN Tunnel Decapsulation application removes the protocol header added by the VxLAN tunnel to extract the original user data packet.
VXLAN Tunnel Encapsulation	VxLAN Tunnel Encapsulation application wraps a user packet within a VXLAN protocol-compliant packet for transport to the next hop for processing or analysis.

For more detailed information on how to configure these applications in the Monitoring Session canvas, refer to GigaVUE V Series Applications Guide.

Flexible Application Chaining

When creating a Monitoring Session, you can use more than one application to receive, process, and forward the traffic. You can define an application chain to indicate how the traffic should be received by the GigaVUE V Series Node, how the traffic should be processed, and how or where the traffic should be forwarded.

The following diagram explains application chaining with two applications, Map and Slicing between Ingress and Egress Tunnels.



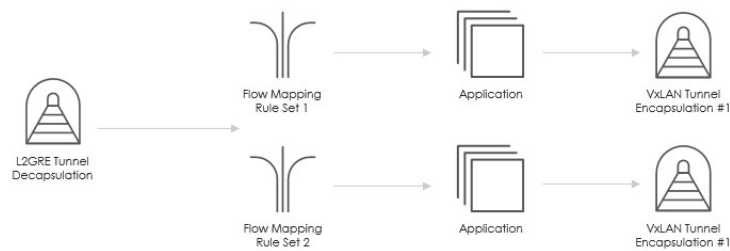
© 2017-2025 Gigamon Inc. All rights reserved.

The application chain in this example specifies the following:

- **Traffic Reception:** Acquired traffic is received by V Series nodes through an L2GRE tunnel. The L2GRE protocol header is removed before sending packets to the FlowMap for filtering.
- **Traffic Filtering:** Packets are filtered based on user-defined rules in the FlowMap. Only packets matching the criteria are forwarded to the Slicing application; non-matching packets are dropped.
- **Traffic Slicing:** The Slicing application removes specific parts of each packet as per user-defined parameters.
- **Traffic Forwarding:** Processed packets are encapsulated in a VXLAN header and sent to the specified tools based on the VXLAN Tunnel Encap configuration.

This Directed Acyclic Graph (DAG) model used in Monitoring Sessions provides you with the flexibility to customize how traffic is processed and forwarded.

Here's another simple example of an application chain defined as part of a Monitoring Session:



© 2017-2025 Gigamon Inc. All rights reserved.

In this example, traffic is received via an L2GRE tunnel, with the L2GRE header removed before being sent to the FlowMap for filtering. The FlowMap application applies two sets of user-defined filtering rules:

- Packets matching the first set of rules are sent to App1 for further processing.
- Packets matching the second set of rules are sent to App2 for separate processing.

This flexible application chaining allows you to process different traffic streams using distinct applications and forward the resulting traffic to different tools. By enabling complex processing and forwarding logic, this approach helps you efficiently achieve your monitoring goals while optimizing costs.

Traffic Forwarding

GigaVUE Cloud Suite for AWS provides useful features that allow you to forward processed traffic in the following efficient manners:

- Forward traffic using tunnel encapsulation, best suited for forwarding traffic to your tools.
- Easily replicate traffic, to efficiently forward traffic to multiple tools simultaneously.
- Load balances the traffic forwarded to multiple tools.
- Secure tunneling for added security.

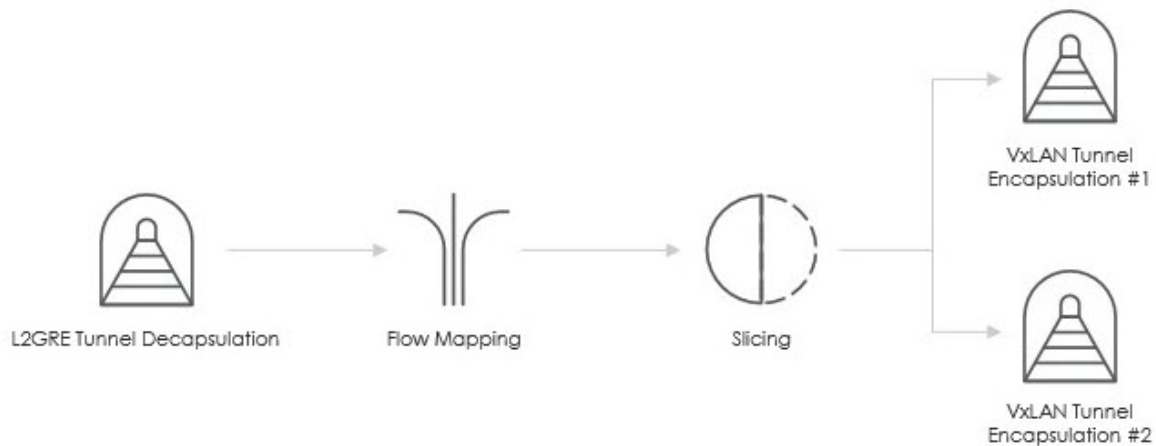
Egress Tunneled Traffic

To route processed traffic, add tunnel endpoints to the Monitoring Session canvas. Configure each endpoint with a destination IP address, tunnel type, and other protocol-specific details. GigaVUE Cloud Suite for AWS supports four protocols for sending traffic to tools:

- L2GRE
- VXLAN
- TLS-PCAPNG (For secure tunnels)
- UDP

Replicate Egress Traffic

The processed traffic can be easily replicated in the Monitoring Session canvas page. You can analyze the same traffic using different types of tools to catch different types of problems (ex: network performance versus cyber security). The following example of a Monitoring Session configuration shows how the traffic is replicated and sent to different tools:



In the above diagram, all packets coming out from the Slicing application is replicated and tunneled to two different tools using VXLAN protocol.

Load Balance Egress Traffic

In scenarios where the processed traffic volume exceeds the capacity of a single tool, you can deploy multiple tool instances to share the load. GigaVUE Cloud Suite for AWS simplifies this by providing a load balancer application that runs directly on GigaVUE V Series Nodes to distribute and balance traffic across multiple tools. To use this feature, simply add the load balancer application to your Monitoring Session canvas and connect its egress endpoint to all the egress tunnel endpoints. This ensures efficient traffic distribution and optimal tool utilization.

AWS Elastic Load Balancing

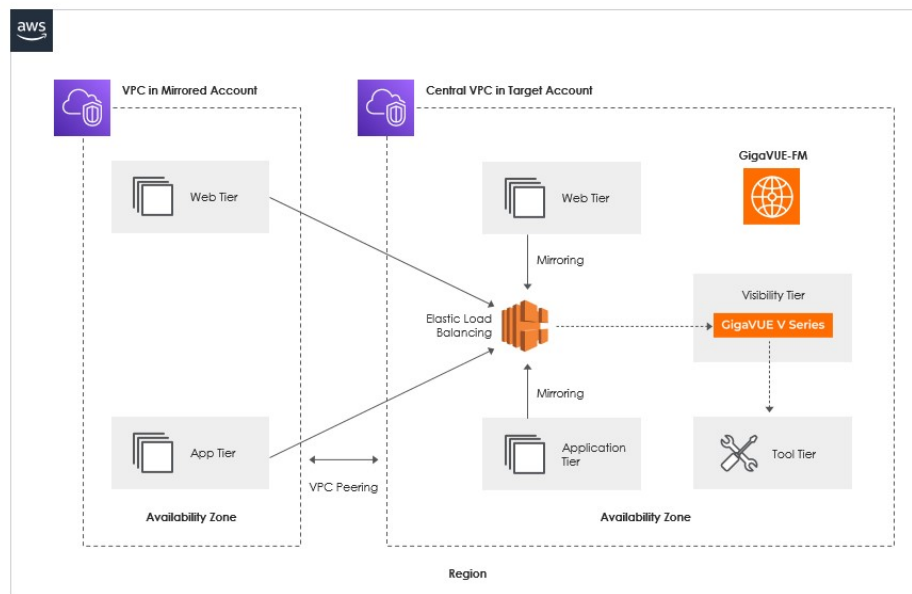
You can use a load balancer to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series Nodes. The load balancer distributes the traffic to the GigaVUE V Series Nodes and the auto-scaling group deploys the GigaVUE V Series Nodes based on the traffic.

The following load balancers are supported:

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

Network Load Balancer

The AWS Network Load Balancer (NLB) uses NLB targets to distribute traffic across multiple resources such as EC2 instances, containers, or IP addresses within a VPC. It operates at the transport layer (Layer 4) and supports protocols like TCP, UDP, and TLS for low-latency, high-throughput applications. With the NLB, traffic can be forwarded from any subnet to targets across multiple Availability Zones for better fault tolerance and scalability. It allows you to monitor and manage network traffic across your VPC, ensuring high availability and performance.



© 2017-2025 Gigamon Inc. All rights reserved.

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.

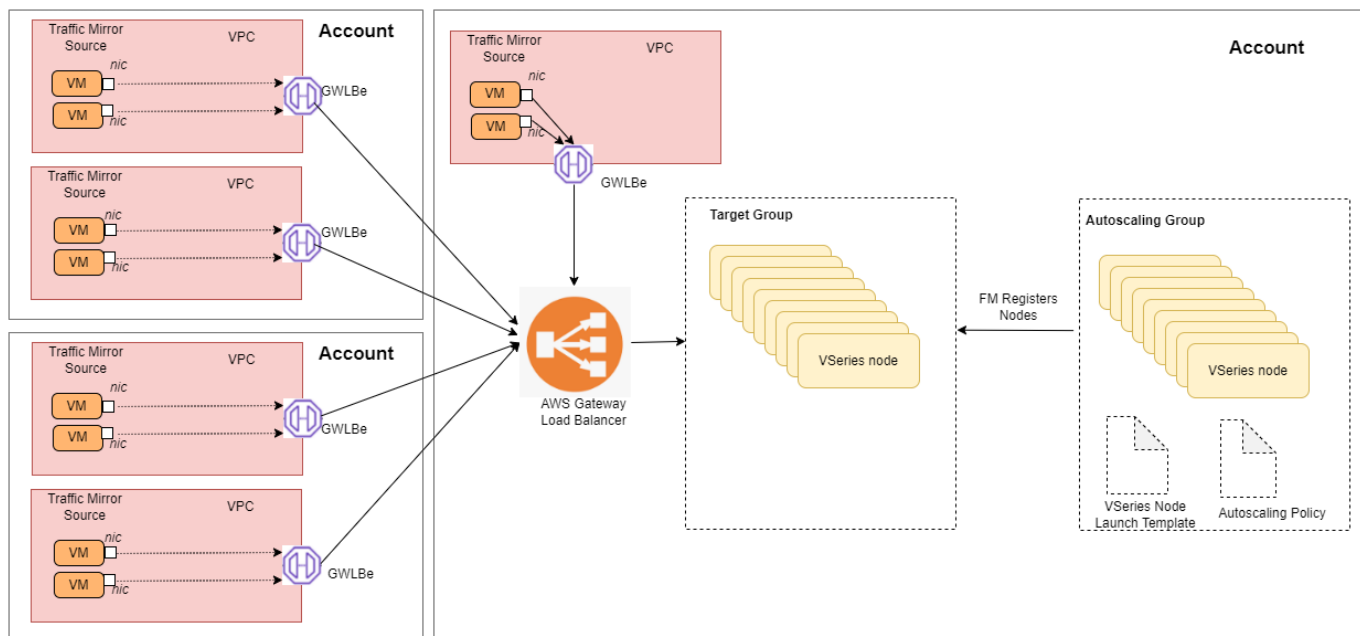
A typical AWS deployment to support the external load balancer requires the following components:

- 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)

Refer [Configure Network Load Balancer in AWS](#) section for more details on how to configure a Network Load Balancer.

Gateway Load Balancer

The gateway load balancer (GWLB) uses the gateway load balancer endpoints to distribute the traffic across the endpoints. It is a VPC endpoint that provides connectivity 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.



In the architecture, you can see the deployment of GigaVUE Cloud Suite for AWS environments that have GWLB implementation for 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, which consume the mirrored and decapsulated data.

Refer [Configure a Gateway Load Balancer in AWS](#) section for more details on how to configure Gateway Load Balancer.

Inline V Series (AWS)

NOTE: Inline V Series is now available as an Early Access feature, giving you the opportunity to explore its capabilities before the general availability (GA).

The Inline V Series solution provides an advanced, scalable, agentless traffic acquisition mechanism that integrates seamlessly into your network. By deploying V Series Nodes in inline mode, you can mirror and process traffic efficiently while ensuring the reinjection of production traffic without disruption.

In AWS and Azure environments, the Inline V Series solution leverages Gateway Load Balancers (GWLB) to enable efficient traffic handling and visibility. This feature ensures low-latency performance, making it ideal for continuous traffic inspection and monitoring. Designed for simplicity and operational efficiency, the Inline V Series allows you to gain deep insights into network activity while maintaining high performance in demanding network environments.

This solution can be used for forwarding inline traffic and traffic processing. When traffic reaches the Inline V Series Node, a copy of the packet is taken as out-of-band traffic. The copied traffic can be forwarded to a GigaVUE V Series Node for additional processing or directly to monitoring tools. During boot-up, the Inline V Series Node initializes with the default Inline application. A Monitoring Session is required to tap the inline traffic, create a copy for out-of-band forwarding, and send the traffic to the desired tools.

Deployment Use Cases for Inline V Series Solution

Single Tier Deployment

This deployment model can be used when traffic has to be tapped, filtered, and directly sent to tools without any processing.

Multi-Tier Deployment

This deployment model can be used if you wish to process the traffic using GigaVUE V Series Applications before sending it to the tools. The first tier acquires the traffic and sends it to the GigaVUE V Series Nodes in the second tier, where the processing occurs in the GigaVUE V Series Applications.

Architecture of Inline V Series Solution in AWS

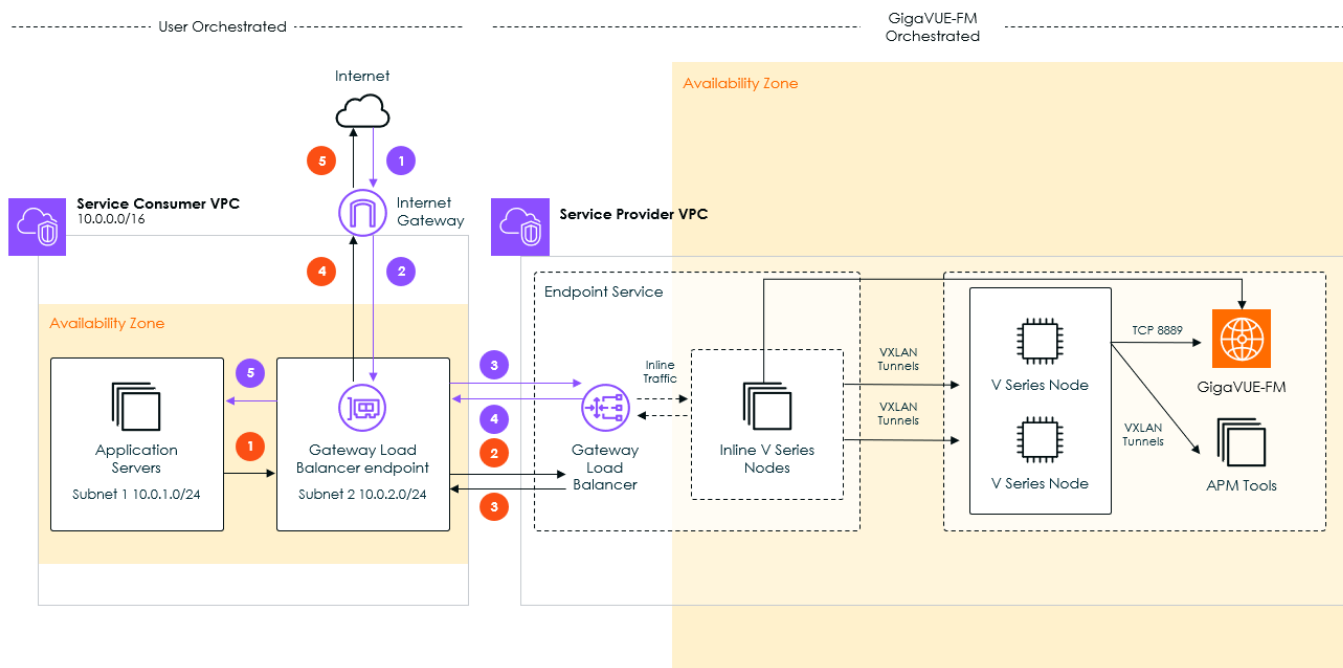
Components required for configuring Inline V Series Solution in AWS:

- Application VPC
- Appliance VPC
- Internet Gateway

- Gateway Load Balancer endpoint
- Gateway Load balancer
- Inline V Series Node

Application VPC consists of multiple workload VMs, Gateway Load Balancer endpoint, Internet Gateway, availability zone, and Application Server with the availability zone. The appliance VPC consists of Gateway Load Balancer, Gateway Load Balancer service, Inline V Series Node (Target Listeners). Any traffic reaching the Gateway Load Balancer will be routed to the Target Listeners.

The below architecture diagram explains how the Inline V Series solution works:



Traffic from the internet to the application server (blue arrows):

1. The traffic from the internet is sent to the Application VPC using an Internet gateway.
2. This traffic is routed to the Gateway Load Balancer endpoint, as a result of ingress routing.

3. The Gateway Load Balancer endpoint sends the traffic to the Gateway Load Balancer in the Appliance VPC using a private link that is created between Gateway Load Balancer endpoint and the Gateway Load Balancer. The Gateway Load balancer forwards the traffic to the Inline V Series Nodes. The following actions are performed in the Inline V Series Node:
 - Once the traffic reaches the Inline V Series Nodes, a copy of the packet is taken as out of band traffic.
 - The Out of Band traffic is forwarded to the GigaVUE V Series Node for further processing or it can be forwarded to the tools.
 - The Inline V Series application swaps the IP address and the Mac of the packets, where the source and destination are interchanged. As a result the Inline V Series Node becomes the source and Gateway Load Balancer becomes the destination.
- NOTE:** Packets sent from the Gateway Load Balancer will be GENEVE encapsulated and forwarded to the Inline V Series Nodes.
4. The inline traffic is sent back to the Gateway Load Balancer endpoint in the application VPC.
 5. Based on the look up in the routing table configured in the Gateway Load Balancer endpoint, the traffic is sent to the application servers (destination subnet).

Prerequisites

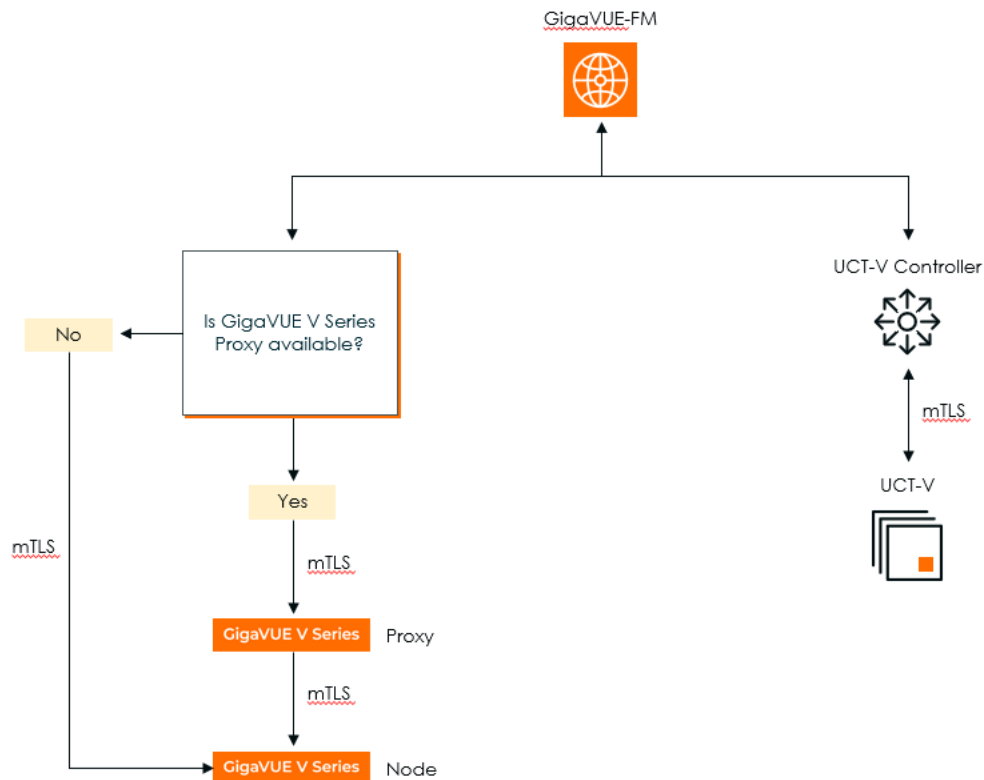
- Create or update Security Group policies of GigaVUE Cloud Suite components. Refer [Security Group](#) topic for detailed information.
- Create or update routes in various VPCs across participating mirrored AWS accounts so that all mirrored account VPCs can connect to the target account VPC where the AWS Gateway Load Balancer is deployed.
- For 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](#).
- You must create a Gateway Load Balancer endpoint. For more information, see [Create a Gateway Load Balancer endpoint](#).
- Create a routing table. For more information, see [Amazon documentation](#).

Refer to the [Acquire Traffic using Inline V Series Solution](#) section for a detailed workflow on acquiring traffic through the Inline V Series.

Secure Communication between GigaVUE Fabric Components

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

How it Works!



In this setup:

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

- GigaVUE-FM also initiates an mTLS connection to the UCT-V Controller, establishing an mTLS connection with UCT-V.

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

GigaVUE-FM acts as the PKI

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

Bring Your Own CA

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

For more details on how to integrate your PKI infrastructure with GigaVUE-FM, refer to [Integrate Private CA](#)

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

Supported Platforms

- AWS
- Azure
- OpenStack
- Nutanix
- Third Party Orchestration
- VMware ESXi
- VMware NSX-T

Supported Components

- GigaVUE V Series Node
- GigaVUE V Series Proxy

- UCT-V
- UCT-V Controller

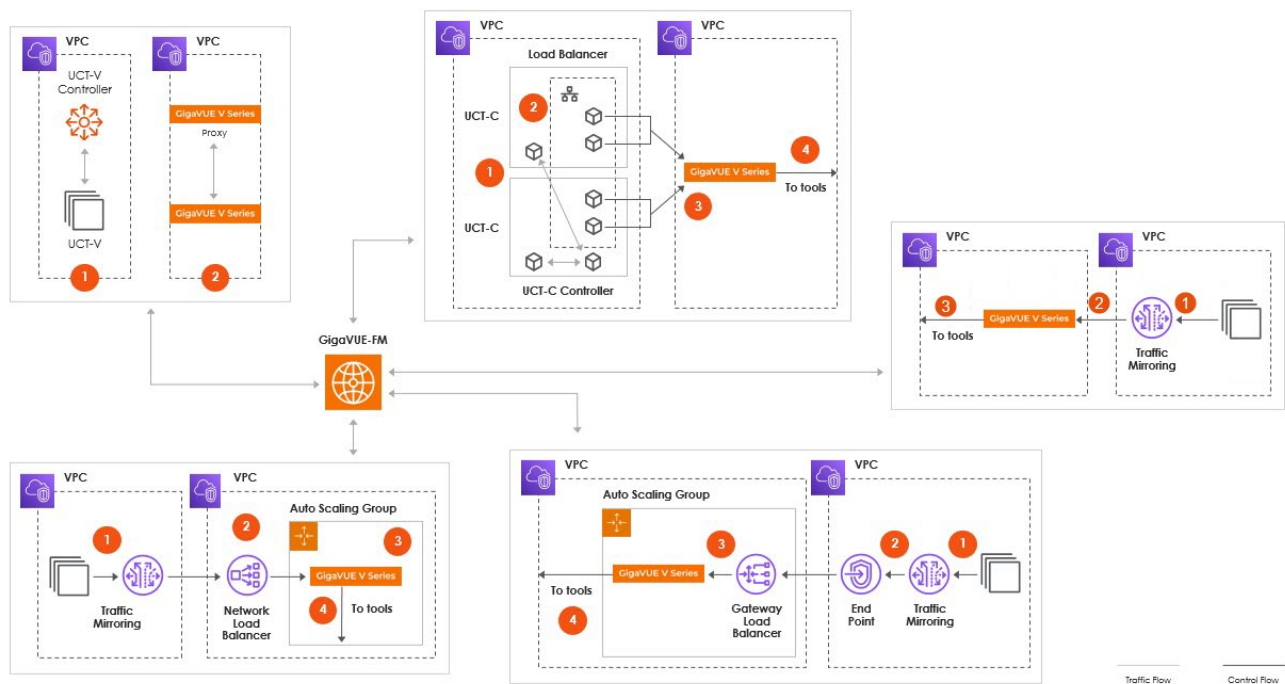
Rules and Notes

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

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

Architecture

The following diagram depicts at a high level various scenarios that GigaVUE Cloud Suite for AWS helps you to acquire and process traffic from workloads running in your AWS accounts and VPCs.



This architecture diagram illustrates different deployment options for acquiring and processing network traffic using GigaVUE fabric components. Each box represents a distinct deployment model, optimized for specific scenarios:

Acquire Traffic from Container Environment

This segment illustrates how GigaVUE V Series Nodes can be used to process traffic from a container environment.

1. UCT-C deployed within the Kubernetes environment captures traffic
2. UCT-C forwards it to the UCT-C Controller for aggregation.
3. The UCT-C Controller then sends the traffic to GigaVUE V Series Nodes for advanced processing, such as filtering or slicing
4. The processed traffic is forwarded to the tools.

GigaVUE-FM manages the entire deployment, handling configuration and orchestration, ensuring scalable and efficient traffic monitoring. Control flows manage configuration between components, while traffic flows indicate data capture and processing, enabling efficient and scalable monitoring container environments.

Regardless of how the traffic is acquired from the workload VMs or pods, GigaVUE V Series Nodes help you to process the traffic and efficiently distribute it to the analysis tools.

Acquire Traffic using UCT-V

This segment shows how UCT-V components can be used for traffic monitoring in virtualized environments.

1. The UCT-V captures traffic from virtual workloads and forwards it to the UCT-V Controller.
2. The UCT-V Controller aggregates the traffic and sends it to GigaVUE V Series Nodes for processing.
3. A GigaVUE V Series Proxy can optionally be used for communicating between the GigaVUE-FM and GigaVUE V Series Nodes.
4. The processed traffic is forwarded to the tools.

GigaVUE-FM manages the entire deployment, handling configuration and orchestration, ensuring scalable and efficient traffic monitoring. Control flows manage configuration between components, while traffic flows indicate data capture and processing, enabling efficient and scalable monitoring container environments.

Acquire Traffic using Traffic Mirroring

The segment explains how the traffic is acquired when your traffic acquisition method is Traffic Mirroring.

1. The traffic from the workload VMs is acquired using Traffic Mirroring.
2. The traffic mirroring forwards the traffic to the GigaVUE V Series Nodes. GigaVUE V Series Nodes are deployed centrally within a VPC or region, handling the processing, filtering, and forwarding of traffic acquired from the workload VMs through tunneling protocols like L2GRE, UDPGRE, or VxLAN.
3. The filtered traffic is then forwarded to monitoring tools for analysis.

With Network Load Balancer

This segment explains how to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series Nodes using a Network Load balancer.

1. The traffic is acquired from the workloads VMs using Traffic Mirroring or Customer Orchestrated Source and is passed to the Network Load balancer.
2. The Network load balancer evenly distributes the filtered traffic across GigaVUE V Series Nodes,
3. The GigaVUE V Series Nodes are deployed in an auto-scaling group to handle variable traffic loads and it processes the traffic.
4. The processed traffic is forwarded to monitoring tools.

The entire deployment is centrally managed by GigaVUE-FM, ensuring efficient traffic processing, load balancing, and scalability.

With Gateway load Balancer

This segment explains how to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series Nodes using the Gateway Load balancer.

1. The traffic is acquired from the workloads VMs using Traffic Mirroring or Customer Orchestrated Source
2. The traffic is passed via the endpoints to the gateway load balancer.
3. The gateway load balancer evenly distributes the filtered traffic across GigaVUE V Series Nodes, which are deployed in an auto-scaling group to handle variable traffic loads.
4. The GigaVUE V Series Nodes process the traffic and forward it to monitoring tools.

The entire deployment is centrally managed by GigaVUE-FM, ensuring efficient traffic processing, load balancing, and scalability.

Deployment Overview

GigaVUE Cloud Suite for AWS deployment follows a set of steps that include planning and preparation before the actual solution deployment. This section provides an overview of the activities associated with GigaVUE Cloud Suite for AWS deployment. The top-level

deployment activities are:

Plan Your Deployment	Address Prerequisites	Prepare Environment	Deploy Cloud Suite
<ul style="list-style-type: none"> • Solution architecture • Visibility targets and accounts owning them: VPCs, Subnets, EC2 instances, EKS clusters, worker nodes, and pods • Deployment location for solution components • Required IAM roles, policies, and permissions for GigaVUE Cloud Suite for AWS • Traffic acquisition method • Traffic forwarding method: Centralized or distributed GigaVUE V Series Nodes • AWS infrastructure requirements, such as Load Balancer • Network communication paths for management and data plane traffic • Credentials and key pairs • EKS Kubernetes cluster(s) 	<ul style="list-style-type: none"> • Complete detailed deployment planning • Create a project plan and assign staff • Set up AWS credentials and SSH key pairs • Configure IAM roles, policies, and cross-account trust (if needed) • Use or adapt Gigamon deployment templates (CloudFormation or Terraform) • For EKS <ul style="list-style-type: none"> ▶ Ensure Kubernetes account has cluster role privileges to deploy pods ▶ Verify access to container registries and Helm charts 	<p>Account and Access Setup</p> <ul style="list-style-type: none"> • Ensure access to and ability to deploy images from AWS Marketplace • Subscribe to GigaVUE products in AWS Marketplace • Verify project staff has <ul style="list-style-type: none"> ▶ Access to required accounts and deployment VPCs/subnets ▶ Permissions to deploy VMs, load balancers, tap software, and edit security groups ▶ Permissions to check/update firewall rules, logs, and troubleshoot ▶ Access to the Gigamon license portal <p>Network Validation</p> <ul style="list-style-type: none"> • Management plane connectivity to VPCs/subnets for GigaVUE • Data plane connectivity from traffic sources to GigaVUE V Series Nodes and tools 	<ul style="list-style-type: none"> • Deploy GigaVUE-FM, install licenses, and set up users/roles • Deploy AWS infrastructure components <ul style="list-style-type: none"> ▶ Load balancer, launch templates, and autoscaling groups • Set up Gateway Load Balancer endpoints (if applicable) • Deploy IAM roles in trusting accounts for cross-account visibility (if used) • Create a Monitoring Domain and add connections, target accounts, and VPCs • Deploy GigaVUE Fabric Components • Deploy UCT Traffic Acquisition components for Universal Cloud Tap (if applicable) • Create and deploy Monitoring Sessions and policies to process and forward traffic to tools

Deployment Planning

This section focuses on the different decisions and information that must be known before the deployment of GigaVUE Cloud Suite for AWS. It assumes you have read the previous chapters and have a good understanding of the Cloud Suite components and concepts, along with AWS components, services, and architectures.

Refer to the following sections for more detailed information:

- [Identify the Deployment Method](#)
- [Identify the AWS Regions](#)
- [Define GigaVUE-FM Deployment Location](#)
- [Identify the Traffic Acquisition Method](#)
- [Identify the Deployment Model](#)
- [Identify the AWS Accounts Involved](#)
- [Identify the Subnets Involved](#)
- [Identify the Required IAM Roles, Policies, and Permissions](#)
- [Identify or Create the Necessary Keypairs](#)

- [Identify the UCT-V Deployment Details](#)
- [Identify the UCT-C Deployment Details](#)

Identify the Deployment Method

GigaVUE Cloud Suite for AWS supports two options for deploying the Fabric Components:

- [GigaVUE-FM Orchestration](#)
- [Third Party Orchestration](#)

In either scenario, GigaVUE-FM must first be launched and running. GigaVUE-FM may be deployed from the AWS Marketplace via a template or using script-based approach such as Cloud Formation, Terraform or other.

GigaVUE-FM Orchestration

In this method, the GigaVUE Fabric Components are deployed using the GigaVUE-FM user interface. After launching GigaVUE-FM, and applying the required license, you can deploy GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller using the GigaVUE-FM interface. Once deployed, GigaVUE-FM monitors the state of the deployed fabric components, and automatically replaces or relaunches them if any error conditions occur.

The GigaVUE-FM Orchestrated option simplifies the GigaVUE Cloud Suite for AWS deployment in AWS but requires AWS API access and permissions to deploy and manage visibility fabric VMs.

Third Party Orchestration

In this method, the GigaVUE Fabric Components are deployed by an external process, typically a combination of Ansible and Terraform products or similar products. You can also use AWS as your Orchestrator. All of the GigaVUE fabric component images are accessible in AWS to support this method.

The Third Party Orchestration method provides an automated method to deploy fabric components in AWS. In this case, GigaVUE-FM can operate with a reduced set of permissions, or with no AWS API access at all (depending on solution architecture). Refer to [Architecture](#) for more details.

This method requires an additional configuration file for GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, and UCT-V to register with the Monitoring Domain created in GigaVUE-FM. However, you can use the GigaVUE-FM to monitor the fabric components health. But you cannot use GigaVUE-FM to replace or relaunch the externally deployed fabric components.

Identify the AWS Regions

GigaVUE Cloud Suite for AWS may be deployed such that a single GigaVUE-FM instance will manage and orchestrate the solution across multiple AWS regions. Each region will require its own Monitoring Domain and separate fabric components must be deployed. To avoid inter-region data transfers and associated costs, the fabric components (and tools) should be deployed in each region as best practice.

Define GigaVUE-FM Deployment Location

GigaVUE-FM may be deployed inside or outside of AWS, such as an existing GigaVUE-FM instance on-premises. While this option exists, deploying a new instance of GigaVUE-FM in AWS has the following benefits:

1. To eliminate any upgrade requirements for existing on-premises GigaVUE-FM instance and GigaVUE appliances.
2. To enable AWS Instance Role-based credentials and eliminate the need to create or configure AWS credentials in GigaVUE-FM, especially in multi-account deployments.
3. As an alternative you can use AWS access keys for credentials if GigaVUE-FM is external to AWS.



Points to Note:

- If GigaVUE-FM is deployed inside AWS, use IAM Role Based credentials.
- If GigaVUE-FM is deployed outside AWS, use Access Keys.

Identify the Traffic Acquisition Method

GigaVUE Cloud Suite for AWS supports traffic acquisition that includes AWS VPC Traffic Mirroring (TM), Gigamon Universal Cloud Tap, and customer orchestrated sources.

The traffic acquisition variations supported are:

- Direct VPC Traffic Mirroring
- VPC Traffic Mirroring with Network Load Balancer
- VPC Traffic Mirroring with Gateway Load Balancer
- UCT-V for VMs
- UCT-C for Containers
- Customer Orchestrated Source
- Customer Orchestrated Source with Gateway Load Balancer

- Customer Orchestrated Source with Network Load Balancer
- Inline V Series Solution

When creating a Monitoring Domain in GigaVUE-FM, you can choose any of the following Traffic Acquisition Methods:

- VPC Traffic Mirroring
- UCT-V
- Customer Orchestrated Source
- Inline

You can only choose one traffic acquisition method per Monitoring Domain. To use different traffic acquisition methods, you can create multiple Monitoring Domains. Currently, GigaVUE Cloud Suite for AWS does not support VPC Traffic Mirroring and UCT-V in the same Monitoring Domain.

GigaVUE Cloud Suite for AWS requires each Monitoring Domain and its fabric components to be deployed in a separate VPC.

Each Monitoring Domain supports one primary traffic acquisition type, but tunnel-based traffic sources can be added as overlays using tunnels in a Monitoring Session. This allows traffic from containers and third-party tunnel sources to be aggregated into the same Monitoring Domain, regardless of its primary acquisition type.

Identify the Deployment Model

GigaVUE Cloud Suite for AWS provides flexibility in terms of the deployment model and the deployment location of fabric components. The deployment model can be of three types:

- Centralized
- Distributed
- Hybrid

Deployment Model for GigaVUE V Series Node

Centralized

In this model, the acquired traffic is forwarded or aggregated to a central location (central VPC), typically called the Tools VPC, where the GigaVUE V Series Node, load balancers (if used), and analysis tools are all colocated. This setup optimizes resource usage by centralizing traffic processing, enabling efficient scaling and simplified management. However, AWS costs may apply for traffic transfer via Transit Gateway (TGW) or Gateway Load Balancer (GWLB). Proper resource planning ensures the central VPC can handle the aggregated traffic effectively.

Distributed

In this model, GigaVUE V Series Nodes, UCT components (if used), and analysis tools are deployed directly into each VPC to process mirrored traffic locally. This approach minimizes data transfer costs by reducing reliance on Transit Gateway (TGW) or Gateway Load Balancer (GWLB) for traffic forwarding. While this requires additional EC2 resources in each VPC, it optimizes performance, lowers AWS costs, and ensures efficient local traffic processing and analysis.

Hybrid

In this model, a combination of both centralized and distributed deployment models is used. This hybrid approach allows for flexibility, where the design is optimized based on traffic volume, cost considerations, and performance needs. By considering factors like compute costs for GigaVUE V Series Nodes and GigaVUE V Series Proxy and the data transfer costs between VPCs, you can design a solution that balances efficiency and budget. For local traffic, a distributed model reduces transfer costs, while centralizing processing may simplify management but incur higher data transfer fees. The key is to tailor the design based on your specific needs.

Deployment Model for UCT-V Controller

For UCT-V traffic acquisition, at least one UCT-V Controller must be deployed to act as a communication proxy between GigaVUE-FM and the UCT-Vs. The UCT-V Controller connects to each UCT-V and maintains a single connection to GigaVUE-FM. Its placement can be optimized to localize traffic and simplify security groups or network firewall rules.

Centralized

The centralized UCT-V Controller model simplifies deployment but requires additional network connections between the UCT-V Controller and distributed UCT-V instances.

Distributed

The distributed UCT-V Controller model enhances communication efficiency by minimizing security group and firewall requirements between GigaVUE-FM and UCT-V Controller, while localizing connections to UCT-V instances. Its small VM footprint enables the cost-effective deployment of multiple controllers.

Hybrid

In this model, a combination of both centralized and distributed deployment models is used. It is common to combine centralized and distributed deployment models based on traffic, costs, and desired traffic types to optimize for cost and performance. Considerations should

include computing costs for the controller VMs vs. the traffic crossing any VPC barrier.

Identify the AWS Accounts Involved

Most GigaVUE Cloud Suite for AWS deployments enable network visibility across multiple AWS accounts using AWS Secure Token Service (STS), Assumed Roles, and trust relationships. This eliminates the need to store credentials for different accounts in GigaVUE-FM.

Centralized vs Decentralized Account Deployment

When planning, identify all AWS accounts involved in the deployment:

Centralized Model

- A single central account hosts the visibility fabric components, including GigaVUE-FM, UCT-V Controller, GigaVUE V Series Nodes, and tools.
- Traffic sources reside in multiple VPCs across other AWS accounts.

Distributed Model

- The GigaVUE fabric components are deployed across all involved accounts.
- Clearly define the locations of deployed modules within each account.

Planning Action:

- For the centralized model, define the central account and list all other accounts requiring traffic visibility.
- For the distributed model, identify all accounts and specify where the modules will be deployed.

Identify the Subnets Involved

For each AWS Region, based on the chosen traffic acquisition method, identify the subnets involved.

For Traffic Mirroring and Customer Orchestrated Source

- For Centralized GigaVUE V Series Node deployment model or if load balancer used:
 - Define the central VPC and subnet where GigaVUE V Series Nodes and load balancer (if used) will be deployed.

- For the Distributed GigaVUE V Series Node deployment model:
 - Define the list of all VPCs and associated subnets where GigaVUE V Series Nodes will be deployed.
- Make note if each VPC or subnet is pre-existing or needs to be created.

For UCT-V

- For the Centralized UCT-V Controller deployment model:
 - Define the central VPC and subnet where the UCT-V Controller will be deployed.
- For the Distributed UCT-V Controller deployment model:
 - Define the list of all VPCs and associated subnets where UCT-V Controller instances will be deployed.
- Make note if each VPC or subnet is pre-existing or needs to be created.

For UCT-C

Define a list of EKS clusters that contain EC2 worker nodes where UCT-C components will be deployed. Refer to Universal Cloud TAP - Container Deployment Guide for more detailed information.

Identify the Required IAM Roles, Policies, and Permissions

GigaVUE-FM uses the AWS API to perform various tasks depending on the solution architecture. The IAM policy attached to the role used by GigaVUE-FM must contain the necessary permissions to perform those tasks. Refer to [Permissions and Privileges \(AWS\)](#) for the minimum required permission.

During the actual deployment, GigaVUE-FM provides a Permission Check tool that allows you to verify:

- access to public cloud endpoints,
- if the required permissions are in place.

NOTE: This tool is not a replacement for pre-deployment planning and permissions establishment.

Identify or Create the Necessary Keypairs

GigaVUE Fabric Components support administrative SSH access via SSH key pairs. When deploying these components the name of an AWS stored SSH Key must be provided to provision the public key on each component. The associated private key may then be used for administrative access to these components. Refer to [AWS Key Pair](#) for more details.

Identify the UCT-V Deployment Details

The UCT-V is provided as a Debian (.deb), RedHat Package Manager (.rpm), and Microsoft Installer (msi) package files. The UCT-V deployment configuration requires knowledge of the OS network interface naming conventions such as eth0, ens5, enX0, etc.

Before deploying UCT-V:

- Identify the VMs where UCT-V deployment is required.
- Familiarize yourself with OS Network interface naming conventions.
- Identify the deployment method.

Identify the UCT-C Deployment Details

GigaVUE Cloud Suite for AWS supports hybrid deployments where traffic visibility for VMs (EC2 instances) and Kubernetes cluster is simultaneously supported from the same GigaVUE-FM, Monitoring Domain and GigaVUE V Series Node. The UCT-C Tap and Controller pod components are deployed to provide traffic acquisition in Kubernetes clusters. This is currently supported only for EKS clusters with EC2 worker nodes. For the specific planning and requirements for UCT-C based deployments for Kubernetes, refer to Universal Cloud TAP - Container Deployment Guide.

Deployment Prerequisites

The following sections explain the prerequisites for successful GigaVUE Cloud Suite for AWS deployment:

- [Subscribe to GigaVUE Products](#)
- [Licensing for GigaVUE Cloud Suite for AWS](#)
- [AWS Security Credentials](#)
- [AWS Key Pair](#)
- [Subnet and Security Group for Amazon VPC](#)
- [Recommended and Supported Instance Types for AWS](#)

- [Role Based Access Control](#)
- [Configure Tokens](#)
- [GigaVUE-FM Version Compatibility](#)
- [Permissions and Privileges \(AWS\)](#)

Subscribe to GigaVUE Products

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 Cloud Suite BYOL



NOTE:

- You will not be charged for subscribing to these components.
- To subscribe to GigaVUE Products, you must add "aws-marketplace:ViewSubscriptions" permission to the IAM policy.

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

1. Login 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 version of the fabric component.
5. Click **View Purchase Options**. The terms and condition page is displayed.
6. Review the Terms and Conditions and then click "**Accept Terms**".

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 will receive a complimentary 30-day SecureVUE Plus trial Volume-Based License (VBL) with a 1TB capacity, valid from the installation date. Refer to [Default Trial Licenses](#) for more detailed information on the applications supported with this license.

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

Default Trial Licenses

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

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

This license includes the following applications:

- ERSPAN
- GENEVE
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flow map
- Header Stripping
- Header Addition
- De-duplication
- NetFlow
- Application Packet Filtering

- Application Filtering Intelligence
- Application Metadata Intelligence
- Application Metadata Exporter
- Inline SSL
- SSL Decrypt
- Precryption

NOTE: If you do not have any other volume-based licenses installed, 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 on the VBL page.

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

Refer to Volume Based License (VBL) for more detailed information on VBL and the available add-on packages.

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

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.

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

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

- For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales team.
- 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 SKUs¹. 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.

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

The following add-on SKUs are available:

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

How GigaVUE-FM Tracks Volume-Based License Usage


GigaVUE-FM 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: 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** to navigate to the Licensing Portal.
9. Upload the Fabric Inventory file in the portal.
10. Select the required license and select **Activate**. A license key is provided.
11. Record the license key or keys.
12. Return to GigaVUE-FM and select **Choose File to** upload the file.

Manage Volume-Based Licenses

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

Manage active Volume-Based License

To manage active Volume-Based License (VBL):

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

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


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

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

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

Manage Inactive Volume-Based License

To manage inactive Volume-Based License (VBL):

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

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

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

NOTE: The License Type, Activation ID and Entitlement ID fields are not displayed by default in the Inactive tab of VBL page. To display these fields, 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. Refer to Add Email Notification Recipients for more details on how to add email recipients.
Filter	Use this button to narrow down the list of active Volume-Based Licenses that are displayed on the VBL active page.
Export	Use this button to export the details in the VBL active page to a CSV or XLSX file.
Deactivate	Use this button to deactivate the licenses. You can only deactivate licenses that have expired.

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

For 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

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 and Privileges \(AWS\)](#) are associated with 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.

Refer to [Create AWS Credentials](#) for more details on how to configure AWS Credentials in GigaVUE-FM.

AWS Key Pair

When configuring GigaVUE-FM and GigaVUE fabric components in AWS, you'll need to specify the defined key pair. A key pair, consisting of a public key and a private key, is a set of security credentials that you use to prove your identity when connecting to an Amazon EC2 instance.

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.

Important considerations for a successful deployment:

- The key pair is crucial for securely accessing your Gigamon instances in AWS.
- Keep the private key file safe, as it is required to connect to the instances.
- You cannot recover the private key if lost; you will have to create a new key pair.
- Key pairs are region-specific in AWS

To create a key pair in AWS, refer to [Create a key pair for your Amazon EC2 instance](#) section in AWS Documentation for more detailed instructions on how to create a key pair.

Subnet and Security Group for Amazon VPC

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

- [Subnet for VPC](#)
- [Security Group](#)

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 GigaVUE-FM uses to communicate with the GigaVUE V Series Nodes and UCT-V Controllers.
- **Data Subnet** that can accept incoming mirrored traffic from UCT-V 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.

To create a security group, refer to [Create a security group](#) topic in the AWS Documentation.

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

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

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

GigaVUE-FM				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	443	Administrator Subnet	Allows GigaVUE-FM to accept Management connection using REST API. Allows users to access GigaVUE-FM UI securely through an HTTPS connection.
Inbound	TCP	22	Administrator Subnet	Allows CLI access to user-initiated management and diagnostics.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-V Controller using REST API.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Node using REST API when GigaVUE V Series Proxy is not used.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Proxy using REST API.
Inbound	TCP	443	UCT-C Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-C Controller using REST API.
Inbound	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive traffic health updates from GigaVUE V Series Nodes.
Inbound	TCP	5671	UCT-V Controller IP	Allows GigaVUE-FM to receive statistics from UCT-V Controllers.
Inbound	TCP	9600	UCT-V Controller	Allows GigaVUE-FM to receive certificate requests from UCT-V Controller.
Inbound	TCP	9600	GigaVUE V Series Proxy	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Proxy.

Inbound	TCP	9600	GigaVUE V Series Node	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Node.
Inbound	TCP	5671	UCT-C Controller IP	Allows GigaVUE-FM to receive statistics from UCT-C Controllers.
Inbound	UDP	2056	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive Application Intelligence and Application Visualization reports from GigaVUE V Series Node.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	9900	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic with UCT-V Controller.
Outbound (optional)	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Proxy.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Node.
Outbound	TCP	8443 (default)	UCT-C Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic to UCT-C Controller.
Outbound	TCP	80	UCT-V Controller IP	Allows GigaVUE-FM to send ACME challenge requests to UCT-V Controller.
Outbound	TCP	80	GigaVUE V Series Node	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Node.
Outbound	TCP	80	GigaVUE V Series Proxy	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Proxy.
Outbound	TCP	443	Any IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.
UCT-V Controller				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate control and management plane traffic with GigaVUE-FM

Deployment Prerequisites

Subnet and Security Group for Amazon VPC

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

Deployment Prerequisites

Subnet and Security Group for Amazon VPC

Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	UDP (VXLAN)	VXLAN (default 4789)	GigaVUE V Series Node IP	Allows UCT-V to tunnel VXLAN traffic to GigaVUE V Series Nodes
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	GigaVUE V Series Node IP	Allows UCT-V to tunnel L2GRE traffic to GigaVUE V Series Nodes
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	GigaVUE V Series Node IP	Allows UCT-V to securely transfer the traffic to the GigaVUE V Series Node
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V to send traffic health updates to UCT-V Controller.
Outbound (This is the port used for Third Party Orchestration)	TCP	8892	UCT-V Controller IP	Allows UCT-V to receive the registration requests and heartbeat to UCT-V Controller.
Outbound	TCP	8300	UCT-V Controller IP	Allows UCT-V to receive ACME validation flow from UCT-V Controller
GigaVUE V Series Node				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8889	GigaVUE-FM IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE-FM
Inbound	TCP	8889	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	UDP (VXLAN)	VXLAN (default 4789)	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive VXLAN tunnel traffic to UCT-V
Inbound	IP Protocol (L2GRE)	L2GRE	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive L2GRE tunnel traffic to UCT-V
Inbound	UDPGRE	4754	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from UDPGRE Tunnel
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.

Deployment Prerequisites

Subnet and Security Group for Amazon VPC

Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Node to receive the ACME challenge requests from the GigaVUE-FM
Inbound	TCP	80	GigaVUE V Series Proxy IP	Allows UCT-V to receive the ACME challenge requests from the GigaVUE V Series Proxy
Inbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	UCT-V subnet	Allows to securely transfer the traffic to GigaVUE V Series Nodes.
Inbound (Optional - This port is used only for configuring AWS Gateway Load Balancer)	UDP (GENEVE)	6081	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from AWS Gateway Load Balancer.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM.
Outbound	UDP (VXLAN)	VXLAN (default 4789)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	UDP	2056	GigaVUE-FM IP	Allows GigaVUE V Series Node to send Application Intelligence and Application Visualization reports to GigaVUE-FM.
Outbound	UDP	2055	Tool IP	Allows GigaVUE V Series Node to send NetFlow Generation traffic to an external tool.
Outbound	UDP	8892	GigaVUE V Series Proxy	Allows GigaVUE V Series Node to send certificate request to GigaVUE V Series Proxy IP.
Outbound	TCP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	<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	443	GigaVUE-FM IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE-FM when GigaVUE V

Deployment Prerequisites

Subnet and Security Group for Amazon VPC

				Series Proxy is not used.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	Tool IP	Allows to securely transfer the traffic to an external tool.
GigaVUE V Series Proxy (optional)				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Proxy to receive the ACME challenge requests from the GigaVUE-FM
Inbound	TCP	8300	GigaVUE V Series Node	Allows GigaVUE V Series Proxy to receive certificate requests from GigaVUE V Series Node for the configured params and provides the certificate using those parameters.
Inbound	TCP	8892	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate control and management plane traffic with GigaVUE V Series Node
Universal Cloud Tap - Container deployed inside Kubernetes worker node				
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	42042	Any IP address	Allows UCT-C to send statistical information to UCT-C Controller.
Outbound	UDP	VXLAN (default)	Any IP address	Allows UCT-C to tunnel traffic to

Deployment Prerequisites

Subnet and Security Group for Amazon VPC

		4789)		the GigaVUE V Series Node or other destination.
UCT-C Controller deployed inside Kubernetes worker node				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8443 (configurable)	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-C Controller.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	5671	Any IP address	Allows UCT-C Controller to send statistics to GigaVUE-FM.
Outbound	TCP	443	GigaVUE-FM IP	Allows UCT-C Controller to communicate with GigaVUE-FM.

Ports to be opened for Backward Compatibility:

These ports must be opened for backward compatibility when GigaVUE-FM is running version 6.10 or later, and the fabric components are on (n-1) or (n-2) versions.

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

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

Recommended and Supported Instance Types for AWS

This section provides information on the recommended and supported instance types for AWS.

Recommended Instance Types

The following table

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.

Supported Instance Types

GigaVUE-FM supports both nitro and non-nitro-based instances; the following sections list the supported nitro and non-nitro-based instances.

Supported Nitro Instance Types

VPC Traffic Mirroring is supported on the following EC2 instance types:

Purpose	Instance types
General purpose	M5, M5a, M5ad, M5d, M5dn, M5n, M6g, M6gd, T3, T3a
Compute optimized	C5, C5d, C5n, C6g, C6gd
Memory optimized	R5, R5a, R5ad, R5d, R5dn, R5n, R6g, R6gd, X1, X1e, z1d
Storage optimized	D3, D3en, I3, I3en
Accelerated computing	F1, G4, Inf1, P3, P3dn

Supported Non-Nitro Instance Types

VPC Traffic Mirroring is available on the following non-Nitro instance types:

Purpose	Instance types
General purpose	M4
Compute optimized	C4
Memory optimized	R4, X1, X1e
Storage optimized	D2, H1
Accelerated computing	G3, G3s, P2

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
Infrastructure Management: This includes the following cloud infrastructure resources: <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
Traffic Control Management: This includes the following traffic control resources: <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
Third Party Orchestration: This includes the following resource: <ul style="list-style-type: none"> • Cloud Orchestration 	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.

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. Refer to [Create AWS Credentials](#) for more details.

Role-Based Access for Third Party Orchestration

Before deploying the fabric components using a third party orchestrator, we must create users, roles and the respective user groups in GigaVUE-FM. You can use the user group to create a token for registration data, which helps deploy fabric components in your orchestrator.

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


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

Users

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

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

To add users perform the following steps:

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

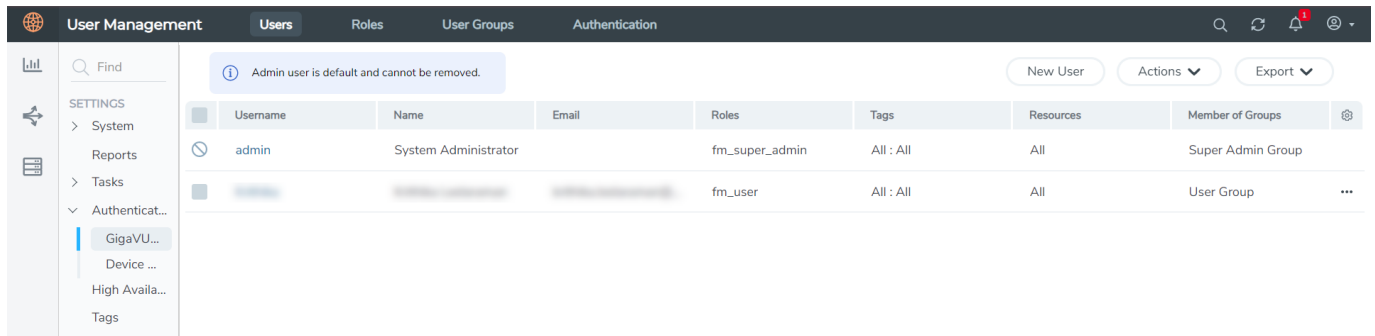


Figure 1 FM Users Page

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

Add User ✕

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

Name

Username

Password

Confirm password

Email

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 -!@#\$%^&*()+

Figure 2 *Create User*

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

NOTE: GigaVUE-FM will prompt for your password.

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

The new user is added to the summary list view.


Role

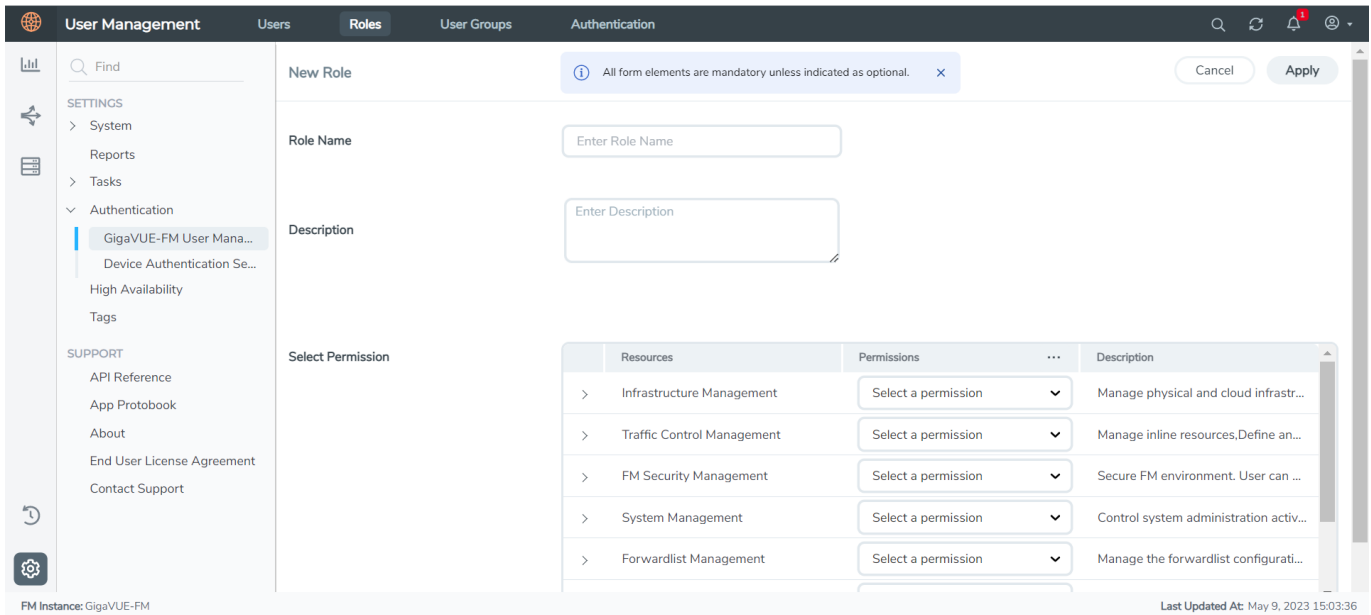
A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

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

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

To create a role

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




The screenshot displays the 'New Role' configuration page in the GigaVUE-FM User Management interface. The left sidebar contains a navigation menu with categories like SETTINGS, Authentication, and SUPPORT. The main area is titled 'New Role' and includes a warning message: 'All form elements are mandatory unless indicated as optional.' The form consists of three main sections: 'Role Name' with a text input field, 'Description' with a larger text area, and 'Select Permission' which is a table. The table has columns for Resources, Permissions, and Description. The Resources column lists various management tasks like Infrastructure Management, Traffic Control Management, FM Security Management, System Management, and Forwardlist Management. Each resource has a 'Select a permission' dropdown in the Permissions column. The bottom of the page shows the instance name 'FM Instance: GigaVUE-FM' and the last update timestamp 'May 9, 2023 15:03:36'.

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

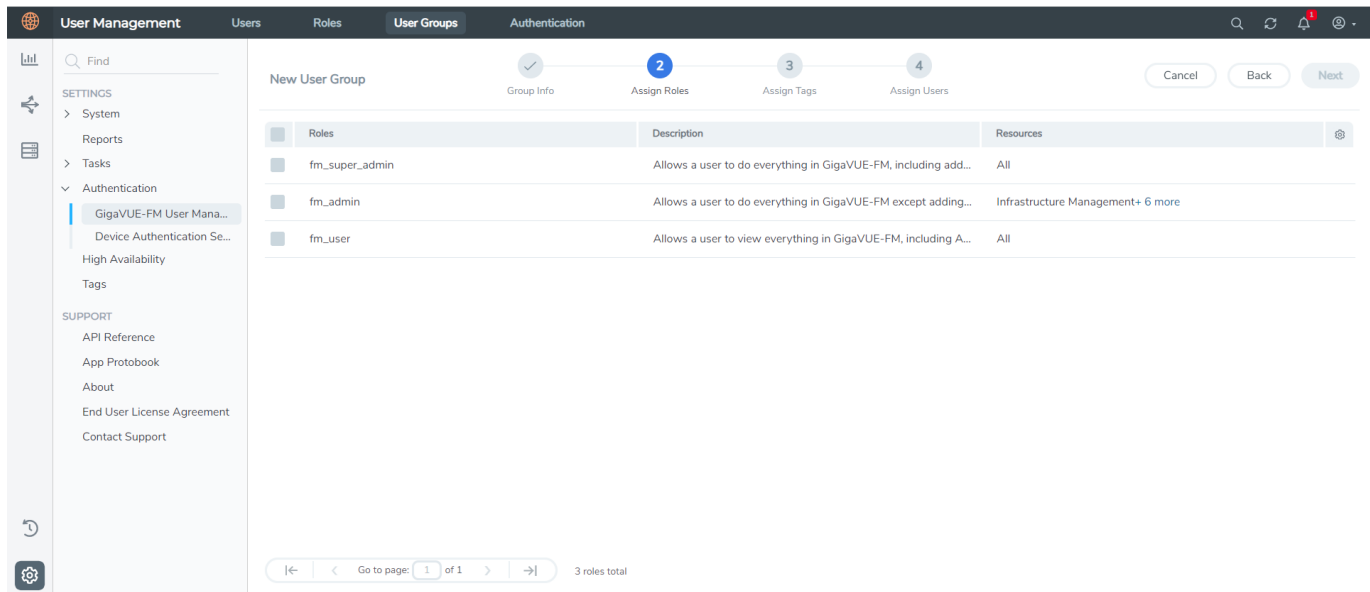
User Groups

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

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

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

- Click **New Group**. In the Wizard that appears, perform the following steps. Click **Next** to progress forward and click **Back** to navigate backward and change the details.



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

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

Click on the ellipses to perform the following operations:

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

What to do Next:

Log in to GigaVUE-FM using the newly created user credentials and create tokens. Refer to [Configure Tokens](#).

Configure Tokens

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

This feature verifies the identity of a user for accessing the GigaVUE-FM REST APIs by generating tokens.

GigaVUE-FM allows you to generate a token only if you are an authenticated user and based on your privileges in accessing the GigaVUE-FM. You can copy the generated tokens from the GUI, which can be used to access the REST APIs. Token inherits the Role-Based Access (RBAC) privilege (read or write) of the user groups assigned to a particular user.

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

Prerequisite

You must create user groups in GigaVUE-FM, refer to [Configure Role-Based Access for Third Party Orchestration](#)

Rules and Notes

- Authentication using a token is an additional mechanism to access GigaVUE-FM REST APIs, and it does not replace the existing GigaVUE-FM authentication mechanism.
- Only authenticated users can create tokens.
- The token expires or becomes invalid under the following circumstances:
 - Based on the configured value for expiry. The default value is 30 days, and the maximum value is 105 days.
 - When a related user group that exists as part of the token is deleted, the corresponding token is deleted.
 - When there is a password change for the user(local), the corresponding token is deleted.
 - When there is a change in the authentication type, all the tokens are deleted.
- During the back up and restoration of the GigaVUE-FM, previously generated tokens will not be available.
- In FMHA role changeover, active GigaVUE-FM tokens are active.
- For basic authentication, activities such as creating, revoking, and reviewing of Token APIs are restricted.
- For expired or invalid tokens, you will see the error code 401 on GigaVUE-FM REST API access.

This section explains about the following:

- [Create Token](#)
- [Revoke Tokens](#)
- [Export Token](#)

Create Token

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

To create a token, follow these steps:

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

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

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


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

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

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

Revoke Tokens

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

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

Export Token

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

- To export a token, select the token, click the **Export Selected** drop-down list box, and then select the **CSV** or **XLSX** format as per requirement.
- To export all the tokens, select the token, click the **Export All** drop-down list box, and then select the **CSV** or **XLSX** format as per requirement.

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

GigaVUE-FM Version Compatibility

GigaVUE-FM version 6.11.00 supports the latest version (6.11.00) of GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, and UCT-V, as well as (n-2) versions. For better compatibility, it is always recommended to use the latest version of fabric components with GigaVUE-FM.

Default Login Credentials for GigaVUE Fabric Components

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:

Product	Login credentials
	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: gigamon Password: Use the SSH key.

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, you must first enable the permissions listed below and attach the policies to an IAM role. You must then, 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. Refer to [IAM roles for Amazon EC2](#) in the AWS Documentation for more details.

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 Inline Policies and Basic Authentication](#)
- [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 Acquiring Traffic using Inline V Series](#)
- [Check for Required IAM Permissions](#)

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.

- A policy must be included 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 there are inline policies 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 there are inline policies 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"
```

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": {
    "Effect": "Allow",
    "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 Inline Policies and Basic Authentication

IMPORTANT: The following example is provided as an example.

IAM permissions required for Inline Policies

If there are inline policies 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",
```

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. Refer to [Install GigaVUE-FM on AWS](#) for more detailed information.

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](#).

These are the minimum permissions that are 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](#).

What to do Next:

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

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. Refer to [Install GigaVUE-FM on AWS](#) for more detailed information.

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](#).

These are the minimum permissions that are 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. Refer to [Create AWS Credentials](#) for more details.

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. Refer to [Install GigaVUE-FM on AWS](#) for more detailed information.

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](#).

These are the minimum permissions that are 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",
        "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. Refer to [Create AWS Credentials](#) for more details.

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. Refer to [Install GigaVUE-FM on AWS](#) for more detailed information on how 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](#).

These are the minimum permissions that are 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](#).

If you are using inline policy or basic authentication, then you must 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. Refer to [Create AWS Credentials](#) for more details.

Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring

Prerequisites:

Before configuring the required permissions and privileges in AWS, you must install GigaVUE-FM. 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](#).

These are the minimum permissions that are 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. Refer to [Create AWS Credentials](#) for more details.

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. Refer to [Install GigaVUE-FM on AWS](#) for more detailed information on how 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](#).

These are the minimum permissions that are 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](#).

If you are using inline policy or basic authentication, then you must 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. Refer to [Create AWS Credentials](#) for more details.

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. 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",
        "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](#).

If you are using inline policy or basic authentication, then you must 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. Refer to [Create AWS Credentials](#) for more details.

Minimum Permissions Required for Acquiring Traffic using Inline V Series

Prerequisites:

Before configuring the required permissions and privileges in AWS, you must install GigaVUE-FM. 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 Inline V Series and authenticate using an IAM instance role.

```

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

```

```

        "iam:ListAccountAliases",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "autoscaling:DescribeAutoScalingGroups",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstances",
        "ec2:CreateTags"
    ],
    "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. Refer to [Create AWS Credentials](#) for more details.

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.

The following are the prerequisites that are required 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. Refer to [Permissions and Privileges \(AWS\)](#) for more detailed information on how to configure the required permissions in 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. Refer to [Subscribe to GigaVUE Products](#) for more detailed information on how to subscribe to the 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 will verify the minimum required permissions. Any missing permissions will be 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](#)

Points to Note for GigaVUE Cloud Suite for AWS

Keep in mind the following notes and rules when deploying GigaVUE Cloud Suite:

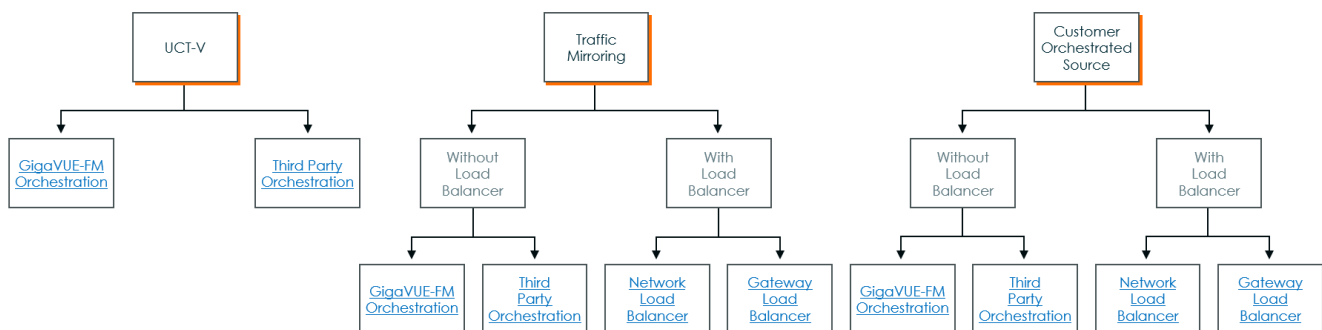
- It is recommended to deploy the GigaVUE-FM in AWS.
- If you already have GigaVUE-FM running outside of your AWS environment, you can connect that existing GigaVUE-FM to your AWS using Basic Credentials (Access Keys).
- If the GigaVUE-FM is deployed outside of the AWS, then the GigaVUE-FM encrypts and 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.
- Deployment of GigaVUE fabric components through a third-party orchestrator is supported.
- 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, that is, all fragments over 200 packets per second get dropped by the ENA (Elastic Network Adapter) of AWS.

- When GigaVUE-FM and GigaVUE V Series Nodes are deployed in different cloud platforms, then the GigaVUE-FM public IP address must be added to the **Data Notification Interface** as the Target Address in the Event Notifications page. Refer to [Configuration Settings](#) section for configuration details.
- 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.

Deployment Options for GigaVUE Cloud Suite for AWS

This section provides detailed information on the multiple ways in which GigaVUE Cloud Suite for AWS can be configured to provide visibility for physical and virtual traffic. There are ten different ways in which GigaVUE Cloud Suite for AWS can be configured based on the traffic acquisition method and the method in which you want to deploy fabric components.

Different deployment options for GigaVUE Cloud Suite for AWS based on the Traffic Acquisition Method




Refer to the following topics for more detailed information:

- [Acquire Traffic using UCT-V - GigaVUE-FM Orchestration](#)
- [Acquire Traffic using UCT-V - Third Party Orchestration](#)
- [Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration](#)
- [Acquire Traffic using Traffic Mirroring – Third Party Orchestration](#)
- [Acquire Traffic using Traffic Mirroring with Network Load Balancer](#)
- [Acquire Traffic using Traffic Mirroring with Gateway Load Balancing](#)

- [Acquire Traffic using Customer Orchestrated Source with Network Load Balancer](#)
- [Acquire Traffic using Customer Orchestrated Source with Gateway Load Balancing](#)
- [Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration](#)
- [Acquire Traffic using Customer Orchestrated Source - Third Party Orchestration](#)
- [Acquire Traffic using Inline V Series Solution](#)


Acquire Traffic using UCT-V - GigaVUE-FM Orchestration

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

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Configure the permissions required in AWS	Minimum Permissions Required for Acquiring Traffic using the UCT-V
3	Create the AWS Credentials	Create AWS Credentials
4	Install UCT-Vs	For Linux: Linux UCT-V Installation For Windows: Windows UCT-V Installation
5	Create a Monitoring Domain <div>  <ul style="list-style-type: none"> • Ensure that the Use FM to Launch Fabric toggle button is enabled. • Select UCT-V as the Traffic Acquisition Method. </div>	Create a Monitoring Domain
6	Configure and deploy GigaVUE Fabric Components in GigaVUE-FM	Configure GigaVUE Fabric Components in GigaVUE-FM
7	Create Monitoring session	Create a Monitoring Session (AWS)
8	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (AWS)
9	Deploy Monitoring Session	Deploy Monitoring Session (AWS)
10	View Monitoring Session Statistics	View Monitoring Session Statistics (AWS)

Acquire Traffic using UCT-V - Third Party Orchestration


This section outlines the workflow for acquiring traffic with UCT-V and deploying GigaVUE Fabric Components using Third Party Orchestration. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Configure the permissions required in AWS	Minimum Permissions Required for Acquiring Traffic using the UCT-V
3	Create the AWS Credentials	Create AWS Credentials
4	Create user groups, role, and users to create tokens.	Configure Role-Based Access for Third Party Orchestration
5	Create tokens in GigaVUE-FM for deploying fabric components using Third Party Orchestration	Configure Tokens
6	Create a Monitoring Domain <div>  <ul style="list-style-type: none"> Ensure that the Use FM to Launch Fabric toggle button is disabled. </div>	Create a Monitoring Domain
7	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode
8	Install UCT-Vs	For Linux: Linux UCT-V Installation For Windows: Windows UCT-V Installation
9	Create Monitoring Session	Create a Monitoring Session (AWS)
10	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (AWS)
11	Deploy Monitoring Session	Deploy Monitoring Session (AWS)
12	View Monitoring Session Statistics	View Monitoring Session Statistics (AWS)

Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration

This section outlines the workflow for acquiring traffic with Traffic Mirroring and deploying GigaVUE Fabric Components using GigaVUE-FM. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.


NOTE: When GigaVUE-FM and the workload VMs requiring monitoring are in different AWS accounts, you must configure a load balancer. Refer to [Acquire Traffic using Traffic Mirroring with Network Load Balancer](#) or [Acquire Traffic using Traffic Mirroring with Gateway Load Balancing](#) for configuration steps.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Configure the required permissions in AWS	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring
3	Create the AWS Credentials	Create AWS Credentials
4	Create a Monitoring Domain <div>  <ul style="list-style-type: none"> • Ensure that the Use FM to Launch Fabric toggle button is enabled. • Select VPC as the Traffic Acquisition Method. </div>	Create a Monitoring Domain
5	Configure and deploy GigaVUE Fabric Components 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
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)

Acquire Traffic using Traffic Mirroring – Third Party Orchestration

This section outlines the workflow for acquiring traffic with Traffic Mirroring and deploying GigaVUE Fabric Components using Third Party Orchestration. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.

NOTE: When GigaVUE-FM and the workload VMs requiring monitoring are in different AWS accounts, you must configure a load balancer. Refer to [Acquire Traffic using Traffic Mirroring with Network Load Balancer](#) or [Acquire Traffic using Traffic Mirroring with Gateway Load Balancing](#) for configuration steps.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Configure the required permissions in AWS.	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring
3	Create the AWS Credentials in GigaVUE-FM	Create AWS Credentials
4	Create user groups, role, and users to create tokens.	Configure Role-Based Access for Third Party Orchestration
5	Create tokens in GigaVUE-FM for deploying fabric components using Third Party Orchestration	Configure Tokens
6	Create a Monitoring Domain <div>  <ul style="list-style-type: none"> • Ensure that the Use FM to Launch Fabric toggle button is disabled. • Select VPC as the Traffic Acquisition Method. </div>	Create a Monitoring Domain
7	Deploy the GigaVUE Fabric Components using AWS.	Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode
8	Create a Monitoring Session	Create a Monitoring Session (AWS)
9	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (AWS)
10	Deploy Monitoring Session	Deploy Monitoring Session (AWS)
11	View Monitoring Session Statistics	View Monitoring Session Statistics (AWS)

Acquire Traffic using Traffic Mirroring with Network Load Balancer

This section outlines the workflow for acquiring traffic using Traffic Mirroring with Network Load Balancer. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Configure the permissions required in AWS <div> NOTE: If GigaVUE-FM and the workload VMs requiring monitoring are in different AWS accounts (cross-account), you must configure the IAM permissions as described in the GigaVUE-FM Instance Multi Account </div>	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring with Network Load Balancer

Step No	Task	Refer the following topics
	Support Using Amazon STS section.	
3	Create the AWS Credentials	Create AWS Credentials
4	Configure Network Load Balancer and deploy GigaVUE V Series Nodes	Configure Network Load Balancer in AWS
5	Create Monitoring session	Create a Monitoring Session (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)


Acquire Traffic using Traffic Mirroring with Gateway Load Balancing

This section outlines the workflow for acquiring traffic with Traffic Mirroring and deploying GigaVUE Fabric Components with a Gateway Load Balancer. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Configure the permissions required in AWS NOTE: If GigaVUE-FM and the workload VMs requiring monitoring are in different AWS accounts (cross-account), you must configure the IAM permissions as described in the GigaVUE-FM Instance Multi Account Support Using Amazon STS section.	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring and GwLB
3	Create the AWS Credentials	Create AWS Credentials
4	Configure Gateway Load Balancer and deploy GigaVUE V Series Nodes	Configure a Gateway Load Balancer in AWS
5	Create Monitoring session	Create a Monitoring Session (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)


Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration

This section outlines the workflow for acquiring traffic with Customer Orchestrated Source and deploying GigaVUE Fabric Components using GigaVUE-FM. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Permissions required in AWS	Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source
3	Create the AWS Credentials in GigaVUE-FM	Create AWS Credentials
4	Create a Monitoring Domain <div>  <ul style="list-style-type: none"> Ensure that the Use FM to Launch Fabric toggle button is enabled. Select Customer Orchestrated Source as the Traffic Acquisition Method. </div>	Create a Monitoring Domain
5	Configure and deploy GigaVUE Fabric Components	Configure GigaVUE Fabric Components in GigaVUE-FM
6	Create Monitoring session	Create a Monitoring Session (AWS)
7	Create Ingress and Egress Tunnel Endpoints	Create Ingress and Egress Tunnels (AWS)
8	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (AWS)
9	Deploy Monitoring Session	Deploy Monitoring Session (AWS)
10	View Monitoring Session Statistics	View Monitoring Session Statistics (AWS)

Acquire Traffic using Customer Orchestrated Source - Third Party Orchestration


This section outlines the workflow for acquiring traffic with Customer Orchestrated Source and deploying GigaVUE Fabric Components using Third Party Orchestration. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Permissions Required in AWS	Minimum Permissions Required for Acquiring Traffic using the Customer Orchestrated Source
3	Create the AWS Credentials in GigaVUE-FM	Create AWS Credentials
4	Create user groups, role, and users to create tokens.	Configure Role-Based Access for Third Party Orchestration
5	Create tokens in GigaVUE-FM for deploying fabric components using Third Party Orchestration	Configure Tokens
6	Create a Monitoring Domain <div>  <ul style="list-style-type: none"> Ensure that the Use FM to Launch Fabric toggle button is disabled. Select Customer Orchestrated Source as the Traffic Acquisition Method. </div>	Create a Monitoring Domain
7	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode
8	Create Monitoring session	Create a Monitoring Session (AWS)
9	Create Ingress and Egress Tunnel Endpoints	Create Ingress and Egress Tunnels (AWS)
10	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (AWS)
11	Deploy Monitoring Session	Deploy Monitoring Session (AWS)
12	View Monitoring Session Statistics	View Monitoring Session Statistics (AWS)

Acquire Traffic using Customer Orchestrated Source with Network Load Balancer

This section outlines the workflow for acquiring traffic using Customer Orchestrated Source with Network Load Balancer. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.


Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Configure the permissions required in AWS	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring with Network Load

Step No	Task	Refer the following topics
		Balancer
3	Create the AWS Credentials	Create AWS Credentials
4	Create user groups, role, and users to create tokens.	Configure Role-Based Access for Third Party Orchestration
5	Create tokens in GigaVUE-FM for deploying fabric components using Third Party Orchestration	Configure Tokens
6	Configure Network Load Balancer and register GigaVUE V Series Nodes in AWS.	Configure Network Load Balancer in AWS
7	Create a Monitoring Domain and Launch the fabric components in GigaVUE-FM. <div>  <ul style="list-style-type: none"> • Ensure that the Use Load Balancer toggle button is enabled. • Select Customer Orchestrated Source as the Traffic Acquisition Method. </div>	Deploy Visibility Fabric with Network Load Balancer
8	Create Monitoring session	Create a Monitoring Session (AWS)
9	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (AWS)
10	Deploy Monitoring Session	Deploy Monitoring Session (AWS)
11	View Monitoring Session Statistics	View Monitoring Session Statistics (AWS)

Acquire Traffic using Customer Orchestrated Source with Gateway Load Balancing


This section outlines the workflow for acquiring traffic with Customer Orchestrated Source and deploying GigaVUE Fabric Components with a Gateway Load Balancer. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Configure the permissions required in AWS	Minimum Permissions Required for Acquiring Traffic using Traffic Mirroring and GwLB
3	Create the AWS Credentials	Create AWS Credentials
4	Configure Gateway Load Balancer and register GigaVUE V Series Nodes in AWS.	Configure a Gateway Load Balancer in AWS
5	Create a Monitoring Domain and Launch the fabric	Deploy Visibility Fabric with

Step No	Task	Refer the following topics
	components in GigaVUE-FM. <div>  <ul style="list-style-type: none"> • Ensure that the Use Load Balancer toggle button is enabled. • Select Customer Orchestrated Source as the Traffic Acquisition Method. </div>	Gateway Load Balancer
6	Create Monitoring session	Create a Monitoring Session (AWS)
7	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
8	Deploy Monitoring Session	Deploy Monitoring Session
9	View Monitoring Session Statistics	View Monitoring Session Statistics (AWS)

Acquire Traffic using Inline V Series Solution

This section outlines the workflow for acquiring traffic using Inline V Series and deploying GigaVUE Fabric Components using Third Party Orchestration. It provides step-by-step guidance on configuring traffic acquisition, processing, and forwarding to your desired destination.

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS.	Install GigaVUE-FM on AWS
2	Configure the permissions required in AWS.	Minimum Permissions Required for Acquiring Traffic using Inline V Series
3	Create Tokens for deploying fabric components using Third Party Orchestration.	Configure Tokens
3	Create the AWS Credentials.	Create AWS Credentials
4	Configure Gateway Load Balancer for Inline V Series Node and Out-of-Band V Series Nodes.	Configure a Gateway Load Balancer in AWS for Inline V Series Solution
5	Create a Monitoring Domain and register the fabric components in GigaVUE-FM. <div>  <ul style="list-style-type: none"> • Ensure that the Use Load Balancer toggle button is enabled. • Select Inline as the Traffic Acquisition Method. </div>	Deploy GigaVUE V Series Nodes for Inline V Series Solution
6	Create and configure Monitoring session.	Configure Monitoring Session

Step No	Task	Refer the following topics
7	Create routing table in AWS.	<ul style="list-style-type: none"> • Configure routing • Architecture patterns for inline inspection
8	View Monitoring Session Statistics.	View Monitoring Session Statistics (AWS)
9	View Dashboards for Inline V Series Solution.	Analytics for Inline V Series Solution

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.

Refer to the following sections for details:

- [Install GigaVUE-FM on AWS](#)
- [Integrate Private CA](#)
- [Create AWS Credentials](#)
- [Create a Monitoring Domain](#)
- [Configure GigaVUE Fabric Components in GigaVUE-FM](#)
- [Configure UCT-V](#)
- [Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode](#)
- [Configure AWS Elastic Load Balancing](#)
- [Managing Monitoring Domain](#)

Install GigaVUE-FM on AWS

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

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. Login 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 version GigaVUE Cloud Suite BYOL version. For more information on Licensing, refer to [Licensing for GigaVUE Cloud Suite for AWS](#)
5. Click **View Purchase Options**. The terms and condition page is displayed.
6. Review the Terms and Conditions and then click "**Accept Terms**".
7. Review the summary and then click "**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. Choose your deployment **Region**.
 - d. Click **Continue to Launch**.
9. In the **Configure this software** page, select the following details. Refer to [Launch an instance using defined parameters](#) in AWS documentation.
 - a. Select the **Launch from Website** option in the **Choose Action** field.
 - b. Select the instance type from the **EC2 Instance Type** drop-down list. Refer to [Recommended and Supported Instance Types for AWS](#).
 - c. Choose the VPC for deploying GigaVUE-FM from the **VPC Settings** drop-down list.
 - d. In the **Subnet Settings**, choose your desired 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. Choose your preferred **Key Pair** for secure access to the instance.
 - g. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
 - h. Click **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 by following 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.
3. 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 login 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 will be 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

Integrate Private CA

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


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

Rules and Notes

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

Generate CSR

To create an intermediate CA certificate:


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

The CSR is downloaded successfully.

Upload CA Certificate

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

To upload the signed CA certificate to GigaVUE-FM:

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

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

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

Deployment Option	Reference Topics
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
Acquire Traffic using Inline V Series in AWS	Minimum Permissions Required for Acquiring Traffic using Inline V Series

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and then click **Settings > Credentials**
2. On the **Credential** page, click the **Add** button. 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. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to [AWS Security Credentials](#)
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Click **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 in AWS
Using Gateway Load balancer	Configure a Gateway Load Balancer in AWS

Deployment Options	Reference Topics
Using Gateway Load balancer for Inline V Series	Configure a Gateway Load Balancer in AWS for Inline V Series Solution
Without a Load Balancer and using 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 a Load Balancer and using Third Party Orchestration	
Deploying GigaVUE Fabric Components using AWS Traffic Acquisition Method as VPC Mirroring or Customer Orchestrated Source	Configure Tokens
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	Create AWS Credentials

Deployment Options	Reference Topics
Acquisition method as Traffic Mirroring or Customer Orchestrated Source	
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 click **Monitoring Domain**.
2. On the Monitoring Domain page, click the **New** button. The **Monitoring Domain Configuration** page appears.
3. Click **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 any 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. Refer to [Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode](#) for detailed information.
- **VPC Traffic Mirroring:** If you select the 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. Refer to [Configure AWS Elastic Load Balancing](#) for detailed information.



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. Refer to the [Permissions and Privileges \(AWS\)](#) topic for details.
- 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 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**.

- **Inline:** If you select this option, you can directly capture the inline traffic from the instances.

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. The UCT-V tunnel MTU should be 50 bytes less than the destination interface MTU size of the UCT-V. When using IPv6 tunnels, the maximum MTU value is 8931. The UCT-V tunnel MTU should be 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** [Configure GigaVUE Fabric Components in GigaVUE-FM](#) to or 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.

NOTE: China regions are not supported.

12. From the **Accounts** drop-down list, select the AWS accounts.
13. From the **VPCs** drop-down list, select the VPCs to monitor.
14. Click **Save**.



Notes:

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

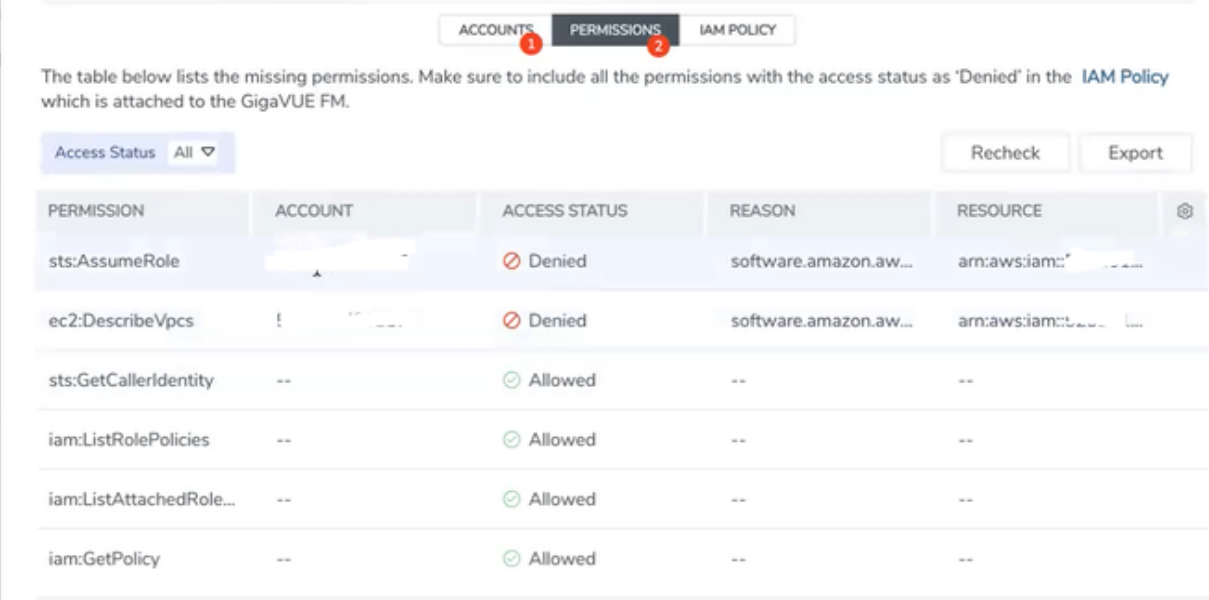
You can view the new Monitoring Domain in the **Monitoring Domain** page list view.

To edit a Monitoring Domain, select the deployed Monitoring Domain and click **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 the steps given below:

1. Go to **Inventory > VIRTUAL > AWS**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Click **New**. The **Monitoring Domain Configuration** page appears.
3. Enter the details as mentioned in the [Create a Monitoring Domain](#) section.
4. Click 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. Click on the **Permission Status** to view the missing permissions.
7. The **ACCOUNTS** tab lists the accounts and the permissions status. Review the accounts that has an error in the permission status.
8. 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.



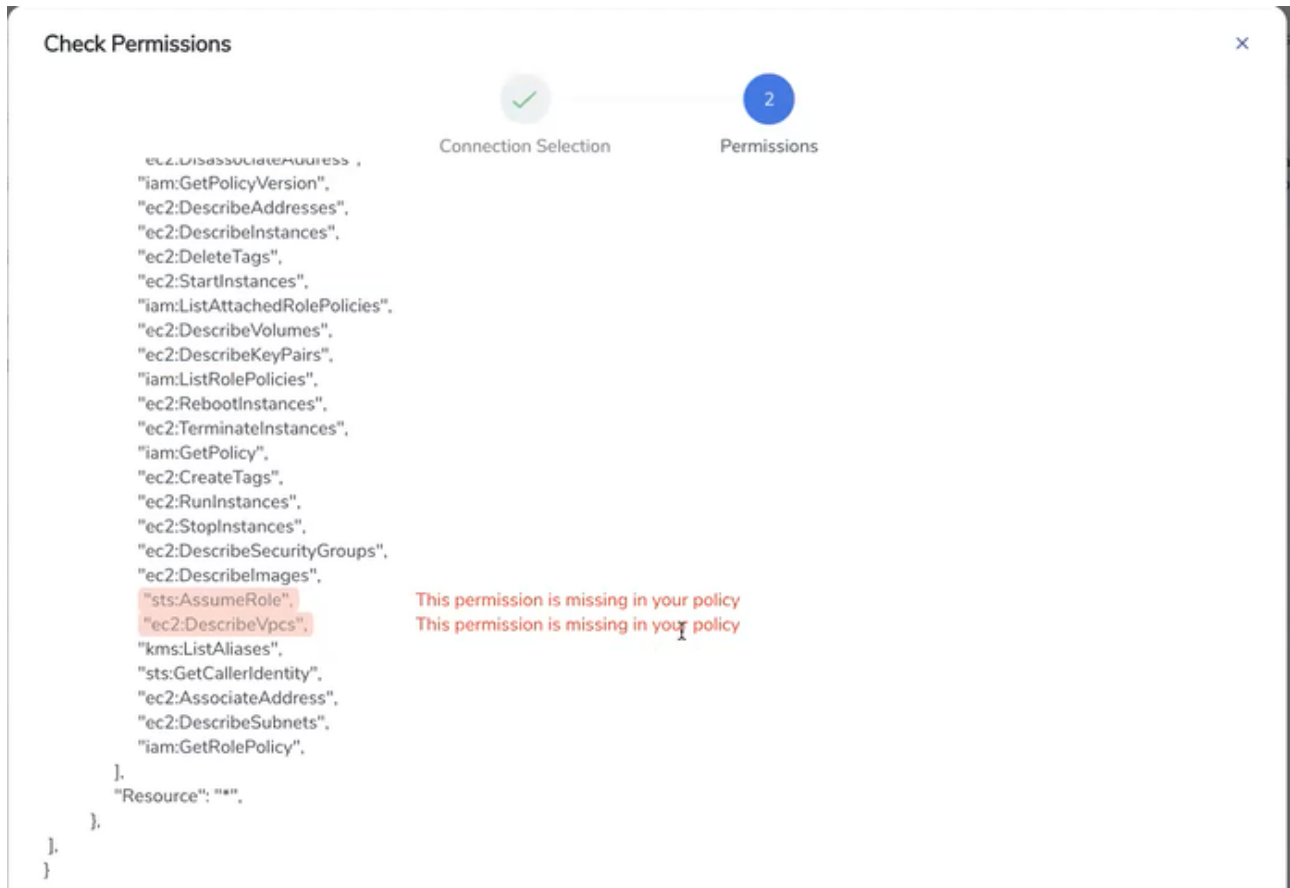
The table below lists the missing permissions. Make sure to include all the permissions with the access status as 'Denied' in the [IAM Policy](#) which is attached to the GigaVUE FM.

Access Status: All ▼

Recheck Export

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

- The **IAM POLICY** tab lists the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite for AWS. You must update the AWS IAM policy with the missing permissions that are highlighted in the JSON. To recheck the IAM policy, go to the **PERMISSIONS** tab and click the **Recheck** button.



When you click Copy or Download, the entire JSON will be 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. Refer to [Configure AWS Settings](#) for more detailed information.

To view permission status report, in the **Monitoring Domain** page, click **Actions > View Permission Status Report**. To view or delete individual reports, select the report and click **Actions** button.

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. Refer to [Configure GigaVUE Fabric Components in GigaVUE-FM](#) for more detailed information on how to deploy GigaVUE Fabric Components using GigaVUE-FM.
- **Use FM to Launch Fabric** is disabled: You must deploy GigaVUE Fabric Components using AWS. Refer to [Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode](#) for more detailed information on how to deploy GigaVUE Fabric Components using AWS.

Configure GigaVUE Fabric Components in GigaVUE-FM

You can configure the following fabric components:

- UCT-V Controller
- GigaVUE V Series Proxy
- GigaVUE V Series Node

Prerequisite:

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

1. Go to **Inventory > VIRTUAL > AWS**.
2. Select the required Monitoring Domain and click **Actions > Deploy Fabric**. The **AWS Fabric Launch Configuration** page appears.
3. From the **Centralized VPC** drop-down list, select the alias of the centralized VPC in which the UCT-V Controllers, V Series Proxies, and the GigaVUE V Series Nodes are launched.

NOTE: Click **Check Permissions** to ensure you have the required permissions for inventory, security groups, fabric launch, and IAM policy. Refer to [Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM](#) for more details.

4. From the EBS Volume Type drop-down list, select one of the following Elastic Block Store (EBS) volume that you can attach to the fabric components:
 - gp2 (General Purpose SSD)
 - gp3 (General Purpose SSD)
 - io1 (Provisioned IOPS SSD)
 - io2 (Provisioned IOPS SSD)
 - Standard (Magnetic)

NOTE: The default EBS Volume Type is **gp3 (General Purpose SSD)**.

5. To encrypt the EBS volume with AWS Key Management Service (KMS), turn on the **Enable Encryption** toggle, and then, from the **KMS Key** drop-down list, select the required KMS key. Refer to [Create a KMS Key](#) in the AWS Documentation.
6. From the **SSH Key Pair** drop-down list, select the key pair that you created to launch the UCT-V Controller, GigaVUE V Series node, and GigaVUE V Series Proxy from GigaVUE-FM. Refer to [Create a key pair](#) in the AWS Documentation.
7. From the **Management Subnet** drop-down list, select the subnet you use for communication between the controllers and the nodes and with GigaVUE-FM.
8. From the **Security Groups** drop-down list, select one or more security groups you created for the GigaVUE fabric nodes. Refer to [Security Group](#).
9. Turn on the **Enable Custom Certificates** toggle, to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the Trust Store. If the certificate is unavailable in the Trust Store, communication does not happen, and a handshake error occurs.

NOTE: If the certificate expires after the successful deployment of the fabric components, the fabric components move to the failed state.

10. From the **Custom SSL Certificate** drop-down list, select the custom certificate that you have already installed. Otherwise, select **Create New** to upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. Refer to [Install Custom Certificate on AWS](#).
11. Turn on the **Prefer IPv6** toggle to deploy all the fabric controllers and the tunnel between the hypervisor and GigaVUE V Series Nodes using an IPv6 address. If the IPv6 address is unavailable, it uses an IPv4 address.

NOTE: You can enable this option only when deploying a new GigaVUE V Series Node. If you want to enable this option after deploying the GigaVUE V Series Node, you must delete the existing GigaVUE V Series Node and deploy it again with this option enabled.

12. Complete the required fields to configure the following GigaVUE Fabric Components:
 - **UCT-V Controller** – Configure UCT-V Controllers in the AWS cloud only if you want to capture traffic using UCT-Vs. A UCT-V Controller can manage only UCT-Vs that have the same version. If there is a version mismatch between the UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the UCT-Vs in the instances.
 - **GigaVUE V Series Proxy** – Turn on the **Configure a V Series Proxy** toggle, if GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network.
 - **GigaVUE V Series Node** – Creating a GigaVUE V Series Node profile automatically launches the GigaVUE V Series Nodes.

NOTE: Refer to [GigaVUE Fabric Components Configuration – Field References](#).

13. Click **Save**.

GigaVUE Fabric Components Configuration – Field References

The following table lists and describes the fields you must complete to configure the UCT-V Controller, GigaVUE V Series Proxy, and GigaVUE V Series Node.

Field	Description
UCT-V Controller <ul style="list-style-type: none"> Configure UCT-V Controllers in the AWS cloud only if you want to capture traffic using UCT-Vs. A UCT-V Controller can manage only UCT-Vs that have the same version. If there is a version mismatch between the UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the UCT-Vs in the instances. 	
Controller Version (s)	<p>To add UCT-V Controllers:</p> <ol style="list-style-type: none"> Under Controller Versions, click Add. 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. From the Instance Type drop-down list, select a size for the UCT-V Controller. Refer to Recommended Instance Types for AWS. In the Number of Instances field, enter the number of UCT-V Controllers to launch. The minimum number you can enter is 1.
Agent Tunnel Type	<p>Select one of the following tunnel types to send the traffic from UCT-Vs to GigaVUE V Series Nodes:</p> <ul style="list-style-type: none"> GRE VXLAN – Select this type if Windows UCT-Vs co-exist with Linux UCT-Vs. Secure tunnels (TLS-PCAPNG) – ??
Agent CA	<p>Select the Certificate Authority (CA) you want to use to connect the tunnel. UCT-V uses this CA to verify the server-side certificate of the GigaVUE V Series Node.</p> <p>NOTE: Note: Use this field only when configuring secure tunnels.</p>
IP Address Type	<p>Select one of the following IP address types:</p> <ul style="list-style-type: none"> 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 GigaVUE-FM. 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. Elastic—If you want a static public IP address for your instance, ensure that you have the elastic IP address available in your VPC. The elastic IP address does not change when you stop or start the

Field	Description
	<p>instance.</p> <ul style="list-style-type: none"> o From the Elastic IPs drop-down list, select the required IP addresses.
Additional Subnets	<p>(Optional) If there are UCT-Vs on networks that are not IP routable from the management network, you must specify additional networks or subnets so that the UCT-V Controller can communicate with all the UCT-Vs.</p> <p>Click Add Subnet to select additional networks (subnets) if needed. Make sure to select a list of security groups for each additional network.</p>
Tags	<p>(Optional) The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a</p> <p>tag) that is easy to identify such as us-west-2- uctvcontrollers.</p> <p>To add a tag, click Add, and enter a Key and Value. For example, enter Name as your Key and us-west-2-uctv-controllers as the Value.</p>
GigaVUE V Series Proxy	
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	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.
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.

Field	Description
	<ul style="list-style-type: none"> 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 there are GigaVUE V Series Nodes on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the GigaVUE V Series Proxy can communicate with all the GigaVUE V Series Nodes.</p> <p>Click 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>
GigaVUE V Series Node	
SSL Key	Select the SSL key from the drop-down list.
Version	Enter the GigaVUE V Series Node version.
Instance Type	<p>The instance type for the GigaVUE V Series Node. Refer to Recommended and Supported 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> <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 launched.</p> <div> <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> </div>

Field	Description
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"> 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-vseries.

Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM

To check for permissions from the AWS Fabric Launch page, follow the steps given below:

1. In the AWS Fabric Launch page, enter the details as mentioned in [Configure GigaVUE Fabric Components in GigaVUE-FM](#).
2. Click the **Check Permissions** button. The **Check Permissions** widget opens.
3. The permission status for Inventory, Security Group, and Fabric Launch are displayed in this widget.
4. Click the **INVENTORY** tab and click **Check Inventory Permissions**, to view the required inventory permissions. Inventory permissions with the access status "Denied" could be missing in the IAM Policy or have restricted boundary.
5. Click the **SECURITY GROUPS** tab and click **Check Security Group Permissions**, to view the required ports that need to be opened for the security groups. The ports in the **Denied** State are not open in the security group. The ports with the status **Explicit denied** are blocked or restricted by the user. The ports with status **Partially configured** have incorrect IP address.
6. Click the **FABRIC LAUNCH** tab and click **Check Fabric Launch Permissions**, to view the permissions required for deploying the GigaVUE fabric components. The Virtual Machine permissions with the access status "Denied" could be missing in the IAM Policy.

NOTE: The permissions "Microsoft.Compute/virtualMachines/write" and "Microsoft.Network/networkInterfaces/join/action" are dependent and cannot be validated separately. So, if either of the permissions is denied or not configured, then both permissions will be displayed as "Denied".

- The **IAM POLICY** tab lists the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite for AWS. You must update the AWS IAM policy with the missing permissions that are highlighted in the JSON.

Configure UCT-V

This section provides the configuration steps for how to install UCT-V in your virtual machines.

Prerequisite:

Before installing UCT-V, you must deploy the GigaVUE Fabric Components in GigaVUE-FM. Refer to [Configure GigaVUE Fabric Components in GigaVUE-FM](#) for more detailed information.

Refer to the following sections for more information:

- [Supported Operating Systems for UCT-V](#)
- [Install UCT-V](#)
- [Create Images with UCT-V](#)
- [Uninstall UCT-V](#)
- [Upgrade or Reinstall UCT-V](#)

Supported Operating Systems for UCT-V

Supported Operating System for UCT-V¹ is 6.5.00, 6.6.00, 6.7.00, 6.8.00, 6.9.00, 6.10.00, 6.11.00

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

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

GigaVUE-FM version 6.11 supports UCT-V version 6.11 as well as (n-2) versions. It is always recommended to use the latest version of UCT-V with GigaVUE-FM, for better compatibility.

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

Install UCT-V

UCT-V can be installed on both Linux and Windows environments. Refer to the following topics for detailed instructions on how to configure UCT-V:

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

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

Supported Platforms

UCT-V is supported on the following platforms for GigaVUE-FM:

- AWS
- Azure
- OpenStack

UCT-V is supported on the following platforms for Third Party Orchestration:

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

Linux UCT-V Installation

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

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

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

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

- [Linux Network Firewall Requirements](#)
- [Install Linux UCT-Vs using Installation Script](#)
- [Install Linux UCT-Vs using Manual Configuration](#)
- [Register Linux UCT-V](#)

Prerequisites

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

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

- [Linux Network Firewall Requirements](#)
- [Linux UCT-V Installation](#)

Linux Network Firewall Requirements

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

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

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

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

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

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

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

Install Linux UCT-Vs using Installation Script

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

- a. Download the UCT-V6.11.00 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-6.11.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.11.00-amd64.deb
```

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

- a. Download the UCT-V6.11.00 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-6.11.00-x86_64.rpm
$ sudo rpm -i gigamon-gigavue-uctv-6.11.00-x86_64.rpm
```

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

sudo uctv-wizard

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

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

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

Options	Use Command	Description
		<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> <p>Enter N if you wish to configure manually. Refer to the Install Linux UCT-Vs using Manual Configuration section for more details.</p> <div> NOTE: Configuration of L2GRE ports is not supported through the uctv-wizard. </div>
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, there is zero interference required as the script installs and configures everything automatically.
- One Touch Installation** - When using .deb or .rpm packages with all prerequisite packages in place, UCT-V determines that all dependencies are met, and it will perform auto-configuration and restart the service.
- Two Touch Installation** - When using .deb or .rpm packages with missing prerequisite packages, the platform displays a warning message about the missing packages. You should install the missing packages using the 'sudo uctv-wizard pkg-install' command.

Install Linux UCT-Vs using Manual Configuration

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

Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

1. Download the UCT-V6.11.00 Debian (.deb) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue-uctv-6.11.00-amd64.deb
```

```
$ sudo dpkg -i gigamon-gigavue-uctv-6.11.00-amd64.deb
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Download the UCT-V6.11.00 RPM (.rpm) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gigamon-gigavue-uctv-6.11.00-x86_64.rpm
```

```
$ sudo rpm -i gigamon-gigavue-uctv-6.11.00-x86_64.rpm
```

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

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

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

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

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

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

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

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

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

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

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

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

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

- Save the file.
- Restart the UCT-V service.
\$ **sudo service uctv restart**

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

```
$ sudo service uctv status
```



Notes:

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

```
sudo systemctl reset-failed uctv.service
```
- After installing UCT-V, refer to [Deploy Fabric Components using Generic Mode](#) for platform specific information to configure UCT-V using Third Party Orchestration.

Post Deployment Check:

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

1. Enter the command:

```
sudo uctvl uctv-show
```

2. Manually execute the following command:

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

Register Linux UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. 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. **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.

Registration:

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

- c. Restart the UCT-V service.

Linux platform:

```
$ sudo service uctv restart
```

For more details on how to create tokens, refer to [Configure Tokens](#).

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

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

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

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](#)

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, ensure the following TCP ports are configured:
 - Port 8301 (Inbound)



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

Install Windows UCT-Vs

Rules and Notes:

- VXLAN is the only tunnel type supported for Windows UCT-V.
- Loopback Interface is not supported for Windows UCT-V.
- Before registering Windows UCT-V, you should generate a token and place it in the **C:\ProgramData\uctv\gigamon-cloud.conf** configuration file. Refer to [Configure Tokens](#).

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 (v1.81 OEM)**

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

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

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V **6.11.00** 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, 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> 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. </div>
adapter-setup	uctv-wizard adapter-setup	<p>Checks the compatible network adapters, increases the send buffer size and restarts the service. Before changing the buffer size, the existing configuration is saved as a backup.</p> <p>You can choose between the following:</p> <ul style="list-style-type: none"> If you wish to skip the prompts for changing the buffer size of compatible network adapters, enter the option as y. Enter N if you wish to set it up manually. Refer to the Install Windows UCT-Vs using Manual Configuration section for more details.
adapter-restore	uctv-wizard adapter-restore	<p>Using this command, you can restore the backup copy of the network adapter buffer size configuration saved in the in the uctv-wizard adapter-setup step.</p> <div> NOTE: You need to manually restart the network adapters for changes to take effect immediately. </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.

Options	Use Command	Description
		<ul style="list-style-type: none"> 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

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

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V **6.11.00** MSI package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Install the downloaded MSI package as **Administrator** and the UCT-V service starts automatically.

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

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



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

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

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

For IPv4:

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

For IPv6:

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

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

For IPv4:

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

For IPv6:

```
2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress
2001:db8:abcd:ef02::/64 mirror-src-egress
2001:db8:abcd:ef01::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

For more details on how to create tokens, refer to [Configure Tokens](#).

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

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

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.

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.

Create Images with UCT-V

If you want to avoid downloading and installing the UCT-Vs every time there is a new instance to be monitored, you can save the UCT-V running on an instance as a private AMI.

To save the UCT-V as an AMI from your EC2 console, right click on the instance and navigate to **Image and Templates > Create Image**.

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 through GigaVUE-FM \(Recommended Method\)](#)
- [Upgrade UCT-V manually](#)

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

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

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

This method can be complicated when you need to upgrade UCT-Vs for a large number of VMs. However, you can upgrade UCT-V in the workload VM without any hands-on involvement through GigaVUE-FM. Refer to the sections below for more details and step-by-step process:

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

Rules and Notes:

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

Upload the UCT-V Images

Follow the below-listed steps to upload UCT-V image files in GigaVUE-FM:

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

- Click **Choose File**, upload the UCT-V files from your local, and click **Ok**.

**Notes:**

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

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

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

Upgrade the UCT-V

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

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

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

7. Click **Create**. The image upgrade task is now created.



Note:

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



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



Notes:

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

You can view the different stages of the upgrade process in UCT-V Upgrade Dashboard

page. Each stage will be marked with  if it is successful and  in case of failure. If the upgrade is successful, GigaVUE-FM will update the upgrade status as **Success** for the selected UCT-V.



Notes:

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

Upgrade UCT-V manually

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

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

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

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

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

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

Prerequisite:

Before deploying GigaVUE Fabric Components in AWS, you must create a Monitoring Domain in GigaVUE-FM with **Use FM to Launch Fabric** toggle button disabled. Refer to [Create a Monitoring Domain](#) for more detailed information.

Points to Note:

- When you deploy the fabric components using third party orchestration, you cannot delete the Monitoring Domain without unregistering the registered fabric components.
- 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. The key must be **GigamonNode**, and the value can be anything, but it must not contain numbers or 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 of these interfaces when deploying the GigaVUE V Series Node in AWS. Refer to [Launch an instance using the Launch Instance Wizard](#) topic in Amazon EC2 Documentation for more detailed information on how to add network interfaces when launching an instance.
- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For more details, refer to the Configure Role-Based Access for Third-Party Orchestration section in the 6.9 Documentation.
- Token must be configured in the **User Management** page. Refer to [Configure Tokens](#) for more detailed information.

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

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

What to do Next:

After deploying the GigaVUE Fabric Components in AWS, 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.

Configure UCT-V Controller in AWS

You can deploy UCT-V Controller in AWS 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, enter or select the following details:

Parameters	Description	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the UCT-V Controller.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is t2.medium.		Yes

Parameters	Description	Reference	Mandatory field
Advanced Details			
Metadata Version	Select V2 only (token required) as the version.		Yes
User Data	<p>The UCT-V Controller uses this user data to generate config file (/etc/gigamon-cloud.conf) used to register with GigaVUE-FM.</p> <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <VPC Name> token: <Token> remoteIP: <IP address of the GigaVUE-FM> sourceIP: <IP address of UCT-V Controller> (Optional Field) remotePort: 443</pre>		

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

Register UCT-V Controller using a Configuration File

To register UCT-V Controller using a configuration file:

1. Log in to the UCT-V Controller.
2. 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>
  token: <Token>
  remoteIP: <IP address of the GigaVUE-FM>
  sourceIP: <IP address of UCT-V Controller> (Optional Field)
  remotePort: 443
```

3. Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

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

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

```
network:
  version: 2
  renderer: networkd
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPv4/24>              # e.g., 192.168.1.10/24
        - <IPv6/64>              # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>           # e.g., 8.8.8.8
          - <DNS_IPV6>           # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPv4_GW>         # e.g., 192.168.1.1
        - to: ::/0
          via: <IPv6_GW>         # e.g., 2001:db8:abcd:0012::fffe
```

Example netplan config:

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

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

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

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

Configure UCT-V in AWS

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

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

To register UCT-V using a configuration file:

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



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

```
Registration:
groupName: <Monitoring Domain Name>
subGroupName: <VPC Name>
token: <Token>
remoteIP: <IP address of the UCT-V Controller 1>,
<IP address of the UCT-V Controller 2>
sourceIP: <IP address of UCT-V> (Optional Field)
```

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

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

Configure GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS

You can deploy GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS using any of the following methods:

- [Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data](#)
- [Register GigaVUE V Series Node and Proxy using a Configuration File](#)

Register GigaVUE V Series Node and GigaVUE V Series Proxy using User Data

This section provides information on how to register GigaVUE V Series Node and GigaVUE V Series Proxy (if used) when launching the virtual machine in AWS using user data. Refer to the following sections for more details:

- [Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data](#)
- [Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using User Data](#)

Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Node using the user data in AWS GUI, enter or select the following details:

Parameters	Instructions	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Node.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is c5n.xlarge.		Yes

Parameters	Instructions	Reference	Mandatory field
Advanced Details			
Metadata Version	Select V2 only (token required) as the version.		Yes
User Data	<p>The GigaVUE V Series Node uses this user data to generate config file (/etc/gigamon-cloud.conf) used to register with GigaVUE-FM.</p> <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <VPC Name> token: <Token> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443</pre>		

Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using User Data

When deploying GigaVUE V Series Node with GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and then deploy the GigaVUE V Series Node.

Register GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Proxy using the user data in AWS GUI, enter or select the following details:

Parameters	Description	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Proxy.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list.		Yes

Parameters	Description	Reference	Mandatory field
Advanced Details			
Metadata Version	Select V2 only (token required) as the version.		Yes
User Data	<p>The GigaVUE V Series Proxy uses this user data to generate config file (/etc/gigamon-cloud.conf) used to register with GigaVUE-FM.</p> <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <VPC Name> token: <Token> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443</pre>		Yes

Register GigaVUE V Series Node when using GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Node via GigaVUE V Series Proxy using the user data in AWS GUI, enter or select the following details:

Parameters	Instructions	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Node.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is c5n.xlarge.		Yes

Parameter s	Instructions	Referenc e	Mandator y field
Advanced Details			
Metadata Version	Select V2 only (token required) as the version.		Yes
User Data	<p>The GigaVUE V Series Node uses this user data to generate config file (/etc/gigamon-cloud.conf) used to register with GigaVUE-FM.</p> <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <VPC Name> token: <Token> remoteIP: <IP address of the GigaVUE V Series Proxy> remotePort: 8891</pre>		Yes

Register GigaVUE V Series Node and Proxy using a Configuration File

This section provides information on how to register GigaVUE V Series Node and GigaVUE V Series Proxy (if used) using a configuration file after launching the virtual machine in AWS. Refer to the following sections for more details:

- [Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using a Configuration file](#)
- [Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file](#)

Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using a Configuration file

To register GigaVUE V Series Node using a configuration file:

1. Log in to the GigaVUE V Series Node.
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, refer to the below table for details:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <VPC Name>
  token: <Token>
  remoteIP: <IP address of the GigaVUE-FM>
  remotePort: 443
```

3. Restart the GigaVUE V Series Node service.
\$ sudo service vseries-node restart

Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file

When deploying GigaVUE V Series Node with GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and then deploy the GigaVUE V Series Node.

Register GigaVUE V Series Proxy using Configuration file:

1. Log in to the GigaVUE V Series Node.
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, refer to the below table for details:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <VPC Name>
  token: <Token>
  remoteIP: <IP address of the GigaVUE-FM>
  remotePort: 443
```

3. Restart the GigaVUE V Series Proxy service.
\$ sudo service vps restart

Register GigaVUE V Series Node when using GigaVUE V Series Proxy using Configuration File

To register GigaVUE V Series Node using a configuration file:

1. Log in to the GigaVUE V Series Node.
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, refer to the below table for details:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <VPC Name>
  token: <Token>
  remoteIP: <IP address of the GigaVUE V Series Proxy>
  remotePort: 8891
```

3. Restart the GigaVUE V Series Node service.
\$ **sudo service vseries-node restart**

The deployed GigaVUE V Series node or proxy registers with the 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, GigaVUE-FM tries to reach the GigaVUE V Series node or proxy and if that fails as well then GigaVUE-FM unregisters the GigaVUE V Series node or proxy and it will be removed from GigaVUE-FM.

Upgrade GigaVUE Fabric Components using Third Party Orchestration

In a Third Party Orchestration deployment method, there is no direct upgrade procedure. Instead, to upgrade the fabric components, you will have to replace the existing version of the fabric components with the latest version. This requires reinstallation and reconfiguration of the entire setup to ensure compatibility with the updated version.

It is recommended to back up all necessary configurations and data prior to initiating this process to prevent any potential data loss.

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

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

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

Configure 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:

- [Configure Network Load Balancer in AWS](#)
- [Configure a Gateway Load Balancer in AWS](#)
- [Configure a Gateway Load Balancer in AWS for Inline V Series Solution](#)

Configure Network Load Balancer in AWS

Prerequisites

- Create or update Security Group policies of GigaVUE Cloud Suite components. Refer [Security Group](#) topic for detailed information.
- 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.

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 [Permissions and Privileges \(AWS\)](#) section for detailed information.
- When configuring Network Load Balancer, the GigaVUE V Series Nodes must be deployed using Third Party Orchestration.
- Token must be configured in the **User Management** page. Refer to [Configure Tokens](#) for more detailed information.

Perform the following steps to configure an external network load balancer in AWS:

1. [Create a Target Group](#)
2. [Create a Load Balancer](#)
3. [Create a Launch Template for Auto Scaling group](#)
4. [Create an Auto Scaling group using a Launch Template](#)

Create a Target Group

Enter or select the following details to configure target groups in AWS.

Parameters	Description	Reference	Mandatory field
Basic Configuration			
Choose a target type	Select IP address as the target type	Create a target group for your Network Load Balancer	Yes
Protocol	Select UDP as the protocol from the drop-down list		Yes
Port	Enter 4789 as the port value		Yes
Health Checks			
HealthCheckProtocol	Select TCP as the protocol.	Health checks for Network Load Balancer target groups	Yes
HealthCheckPort	Enter 8889 as the port.		Yes
HealthCheckIntervalSeconds	Enter 10 seconds as the approximate amount of time, in seconds.		Yes

Create a Load Balancer

Enter or select the following details to configure a load balancer in AWS.

Parameters	Description	Reference	Mandatory field
Basic Configuration			
Scheme	Select Internal as the scheme for the load balancer	Create a Network Load Balancer	Yes
Network Mapping			
VPC	Select the VPC for your targets (GigaVUE V Series Node)	Create a Network Load Balancer	Yes
Listeners and routing			
Protocol	Select UDP as the protocol.	Create a Network Load Balancer	Yes
Port	Enter 4789 as the port.		Yes

Create a Launch Template for Auto Scaling group

Enter or select the following details to create a launch template for auto scaling groups in AWS.

Parameters	Description	Reference	Mandatory field
Launch Template contents			
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node.	Create a launch template for an Auto Scaling group	Yes
Instance type	Select t3a.xlarge as the instance type.		Yes
Key pair name	Select a Key pair for the instance.		Yes
Network Settings			
Device Index	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,	Create a launch template for an Auto Scaling group	Yes
Firewall (security groups)	Keep this blank and configure one or more security groups as part of the network interface.		Yes
Advanced Settings			
Advanced details	<div>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.</div> <div><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> remotePort: 443</pre></div>	Create a launch template using advanced settings	Yes

Create an Auto Scaling group using a Launch Template

Enter or select the following details to create an auto scaling group and launch the fabric components using the launch template in AWS.

Parameters	Description	Reference	Mandatory field
Configure group size and scaling policies			
Group Size	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.	Creating an Auto Scaling group using a launch template	Yes
Automatic Scaling	Select Target tracking scaling policy and enter the following details to define a policy: Metric Type: 1000000000 (bytes) Instance warmup: 300 seconds	Create a target tracking scaling policy	Yes
Add tag	Provide a tag key and value for each tag.	Tag Auto Scaling groups and instances	No

In the Instances page, you can view the GigaVUE V Series Node instance deployed by the load balancer.

After configuring the network load balancer in AWS, you must register the GigaVUE V Series Node with GigaVUE-FM. Refer to [Deploy Visibility Fabric with Network Load Balancer](#) section for more detailed information on how to deploy the GigaVUE V Series Node across the AWS accounts with Network load balancer configured.

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 in AWS](#) 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's a navigation bar with tabs for 'AWS', 'Monitoring Domains', 'Connections', 'Fabric', 'UCT-V', and 'Settings'. The 'Monitoring Domains' tab is active. The main form includes the following fields:

- Monitoring Domain***: md1
- Traffic Acquisition Method***: VPC Traffic Mirroring (dropdown)
- Traffic Acquisition Tunnel MTU***: 8951
- Use FM to launch V Series Proxy**: No (toggle)
- Use Load Balancer**: Yes (toggle)
- Connections**: A section with a dropdown arrow, containing:
 - Name***: Enter a connection name
 - Credential***: Credential Name... (dropdown)
 - Region***: Region Name... (dropdown)
 - Accounts***: Select Accounts... (dropdown)
 - VPCs***: Select VPCs... (dropdown)

At the top right, there are buttons for 'Check Permissions', 'Save', and 'Cancel'. A blue notification banner on the right side 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](#).

Configure a Gateway Load Balancer in AWS

Prerequisites

- Create or update Security Group policies of GigaVUE Cloud Suite components. Refer [Security Group](#) topic for detailed information.

- 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. Refer to [Subnet and Security Group for Amazon VPC](#) for more information.
- 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 [Permissions and Privileges \(AWS\)](#) section for detailed information.
- 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](#).
- Token must be configured in the **User Management** page. Refer to [Configure Tokens](#) for more detailed information.

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. [Create a Target Group](#)
2. [Create a Load Balancer](#)
3. [Create a Launch Template for Auto Scaling group](#)
4. [Create an Auto Scaling group using a Launch Template](#)

Create a Target Group

Enter or select the following details as mentioned in the table to configure target groups in AWS.

Parameters	Description	Reference	Mandatory field
Basic Configuration			
Choose a target type	Select IP address as the target type	Create a target group for your Gateway Load Balancer	Yes
Protocol	Verify that Protocol is GENEVE		Yes
Port	Verify that the port value is 6081		Yes
Health Checks			

Parameters	Description	Reference	Mandatory field
HealthCheckProtocol	Select TCP as the protocol.	Health checks for Gateway Load Balancer target groups	Yes
HealthCheckPort	Enter 8889 as the port.		Yes
HealthCheckIntervalSeconds	Enter 10 seconds as the approximate amount of time, in seconds.		Yes

Create a Load Balancer

Enter or select the following details as mentioned in the table to configure a load balancer in AWS.

Parameters	Description	Reference	Mandatory field
Network Mapping			
VPC	Select the VPC for your targets (GigaVUE V Series Node)	Create a Gateway Load Balancer	Yes
IP Listener routing			
Default action	Select the target group to receive traffic. If you don't have a target group, choose Create target group.	Create a target group	Yes

Create a Launch Template for Auto Scaling group

Enter or select the following details to create a launch template for auto scaling groups in AWS.

Parameters	Description	Reference	Mandatory field
Launch Template contents			
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node.	Create a launch template for an Auto Scaling group	Yes

Parameters	Description	Reference	Mandatory field
Instance type	Select c5n.xlarge as the instance type.		Yes
Key pair name	Select a Key pair for the instance.		Yes
Network Settings			
Device Index	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,	Create a launch template for an Auto Scaling group	Yes
Firewall (security groups)	Keep this blank and configure one or more security groups as part of the network interface.	Security Group	Yes
Advanced Settings			
Advanced details	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. <div>#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</div>	Create a launch template using advanced settings	Yes

Create an Auto Scaling group using a Launch Template

Enter or select the following details to create an auto scaling group and launch the fabric components using the launch template in AWS.

Parameters	Description	Reference	Mandatory field
Configure group size and scaling policies			
Group Size	Enter the Desired capacity as 0. The Desired capacity value must be less than the Maximum Capacity value.	Creating an Auto Scaling group using a launch	Yes

Parameters	Description	Reference	Mandatory field
	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.	template	
Automatic Scaling	Select Target tracking scaling policy and enter the following details to define a policy: Metric Type: 1000000000 (bytes) Instance warmup: 300 seconds	Create a target tracking scaling policy	Yes
Add tag	Provide a tag key and value for each tag.	Tag Auto Scaling groups and instances	No

In the Instances page, you can view the GigaVUE V Series Node instance deployed by the load balancer.

After configuring the network load balancer in AWS, you must register the GigaVUE V Series Node with GigaVUE-FM. Refer to [Deploy Visibility Fabric with Gateway Load Balancer](#) section for more detailed information on how to deploy the GigaVUE V Series Node across the AWS accounts with Network load balancer configured.

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** or **Inline** 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 in AWS](#) 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 tabs for 'AWS', 'Monitoring Domains', 'Connections', 'Fabric', 'UCT-V', and 'Settings'. The 'Monitoring Domains' tab is active. The configuration form 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)
- Connections**: A section containing a table with the following fields:
 - Name***: Enter a connection name
 - Credential***: Credential Name...
 - Region***: Region Name...
 - Accounts***: Select Accounts...
 - VPCs***: Select VPCs...

A 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.' The bottom of the page has 'Check Permissions', 'Save', and 'Cancel' buttons.

5. Click **Save**. The Monitoring Domain is created successfully and you are navigated to the **AWS Fabric Launch Configuration** page.
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 **Desire capacity** value for the Auto Scaling Group in AWS. Refer to [Configure a Gateway Load Balancer in AWS](#) 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](#)

Configure a Gateway Load Balancer in AWS for Inline V Series Solution

Points to Note:

- When configuring Gateway Load Balancer, the GigaVUE V Series Nodes must be deployed using Third Party Orchestration.
- Inline V Series solution requires a dedicated Gateway Load Balancer deployed in your VPC.

Perform the following steps to configure a gateway load balancer for Inline V Series Solution in AWS:

1. [Create a Target Group](#)
2. [Create a Gateway Load Balancer](#)
3. [Create a Launch Template for Inline GigaVUE V Series Node](#)
4. [Create an Auto Scaling group using a Launch Template for Inline GigaVUE V Series Node](#)
5. [Create a Launch Template for Out of Band GigaVUE V Series Node](#)
6. [Create an Auto Scaling group using a Launch Template for Out of Band GigaVUE V Series Node](#)

Create a Target Group

Enter or select the following details as mentioned in the table to create a target groups in AWS.

Parameters	Instructions	Reference	Mandatory field
Basic Configuration			
Choose a target type	Select Instance as the target type.	Create a target group for your Gateway Load Balancer	Yes
Protocol	Verify that Protocol is GENEVE .		Yes
Port	Verify that the port value is 6081 .		Yes
VPC	Select the VPC where you want to create the Gateway Load balancer and the target group.	Yes	Port
Health Checks			
Health check protocol	Select TCP as the protocol.	Health checks for Gateway Load Balancer target groups	Yes

Parameters	Instructions	Reference	Mandatory field
Health check port	Select the option to override the port and enter 8889 as the port value.		Yes
Healthy threshold	Enter 2 as the threshold count value.		
Unhealthy threshold	Enter 2 as the threshold value.		
Timeout	Enter 2 seconds as the timeout.		
Interval	Enter 5 seconds as the approximate amount of time.		Yes

Once the target group details are configured and saved, you will be prompted to select targets. Skip this step and click **Create target group** to finalize the configuration.

Create a Gateway Load Balancer

Enter or select the following details as mentioned in the table to create a gateway load balancer in AWS.

Parameters	Instructions	Reference	Mandatory field
Network Mapping			
VPC	Select the VPC for your targets (GigaVUE V Series Node)	Create a Gateway Load Balancer	Yes
Availability Zone and subnets	Select the zones and the corresponding subnets where you want to launch the GigaVUE V Series Node.	Create a Gateway Load Balancer	Yes
IP Listener routing			
Default action	Select the target group to receive traffic. If you don't have a target group, choose Create target group.	Create a target group	Yes

NOTE: Once the Gateway Load Balancer is created and associated with subnets and Availability Zones, these settings cannot be modified. If you need to make changes later, you'll have to delete and recreate the load balancer.

After creating the Gateway Load balancer, configure Cross-zone load balancing to balance traffic flows between the GigaVUE V Series Nodes deployed across multiple availability zones. Refer to [Cross-zone load balancing](#) section in AWS Documentation for more details.

Create a Launch Template for Inline GigaVUE V Series Node

Enter or select the following details to create a launch template for auto scaling groups in AWS.

Parameters	Instructions	References	Mandatory field
Launch Template contents			
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node. From the AWS Marketplace AMIs . Search Gigamon and choose the GigaVUE Cloud Suite V Series Image. Subscribe to it.	Create a launch template for an Auto Scaling group	Yes
Instance type	Select c5n.xlarge as the instance type.		Yes
Key pair name	Select a Key pair for the instance.		Yes
Network Settings			
Subnet	Select Don't include in launch template option.	Create a launch template for an Auto Scaling group	Yes
Firewall (security groups)	Choose Select existing security group option. Keep the security group blank and configure one or more security groups as part of the network interface as mentioned in the following steps.	Security Group	Yes
Advanced Network configurations			
GigaVUE V Series Node requires a minimum of 2 Network Interfaces one for data and other one for mgmt. Add 2 Network Interfaces.			
Network interface 1 - Data Interface			
Device Index	Enter the device index as 0 for the data interface	Create a launch template for an Auto Scaling group	Yes
Subnet	The subnet is automatically assigned by AWS.		
Security Group	Choose the security group.		
Network interface 2 - Management Interface			
Device Index	Enter the device index as 1 for the mgmt interface	Create a launch template for an Auto	Yes

Parameter s	Instructions	Referenc e	Mandator y field
		Scaling group	
Subnet	Select the subnet.		
Security Group	Select the same security group.		
Advanced Settings			
Advanced details	<p>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 files (/etc/gigamon-cloud.conf and /etc/vseries-inline.conf) and register with GigaVUE-FM using Third Party Orchestration.</p> <div> <p>NOTE: Token must be configured in the User Management page. Refer to Configure Tokens for more detailed information.</p> <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Enter a name for the Monitoring Domain> subGroupName: <Enter the VPC Name> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443 token: <token> - path: /etc/vseries-inline.conf owner: root:root permissions: '0644' content: ""</pre> </div>	Create a launch template using advanced settings	Yes

Create an Auto Scaling group using a Launch Template for Inline GigaVUE V Series Node

Enter or select the following details to create an auto scaling group and launch the fabric components using the launch template in AWS.

Parameters	Instructions	Reference	Mandatory field
Choose launch template or configuration			
Launch template	Choose the Launch Template created for Inline GigaVUE V Series Node	Creating an Auto Scaling group using a	Yes

Parameters	Instructions	Reference	Mandatory field
Choose launch template or configuration		launch template	
VPC	Select the VPC for your targets (GigaVUE V Series Node)		
Availability Zone and subnets	Select the zones and the corresponding subnets where you want to launch the GigaVUE V Series Node.		
Integrate with other services			
Load balancing	Choose Attach to an existing load balancer option.	Creating an Auto Scaling group using a launch template	
Existing load balancer target groups	Select the Target Group created above.		
Attach to an existing load balancer	Choose the Choose from your load balancer target groups option.		Yes
Configure group size and scaling			
Group Size	<div>Enter the Min desired capacity as 0. The Desired capacity value must be less than the Maximum Capacity value.</div> <div>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.</div>	Creating an Auto Scaling group using a launch template	Yes
Automatic Scaling	Select Target tracking scaling policy	Create a target tracking scaling policy	Yes
Add tags			
Tags	Provide Key as GigamonNode and Value as VSeriesNode for each tag.	Tag Auto Scaling groups and instances	No

Create a Launch Template for Out of Band GigaVUE V Series Node

This step is optional. You can create a launch template for Out of Band GigaVUE V Series Node if you wish to send to process the acquired traffic.

Enter or select the following details to create a launch template for auto scaling groups in AWS.

Parameters	Instructions	Reference	Mandatory field
Launch Template contents			
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node.	Create a launch template for an Auto Scaling group	Yes
Instance type	Select c5n.xlarge as the instance type.		Yes
Key pair name	Select a Key pair for the instance.		Yes
Network Settings			
Device Index	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,	Create a launch template for an Auto Scaling group	Yes
Firewall (security groups)	Keep this blank and configure one or more security groups as part of the network interface.	Security Group	Yes
Advanced Settings			
Advanced details	<div>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.</div> <div>NOTE: Token must be configured in the User Management page. Refer to Configure Tokens for more detailed information.</div> <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Enter a name for the Monitoring Domain> subGroupName: <Enter the VPC Name> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443 token: <token></pre>	Create a launch template using advanced settings	Yes

Create an Auto Scaling group using a Launch Template for Out of Band GigaVUE V Series Node

This step is optional. You can create a auto scaling groups for Out of Band GigaVUE V Series Node if you wish to send to process the acquired traffic. You can configure multiple auto-scaling groups based on the number of node groups or tiers you need to set up.

Enter or select the following details to create an auto scaling group and launch the fabric components using the launch template in AWS.

Parameters	Instructions	Reference	Mandatory field
Choose launch template or configuration			
Launch template	Choose the Launch Template created for Out-of-Band GigaVUE V Series Node	Creating an Auto Scaling group using a launch template	Yes
Configure group size and scaling			
Group Size	Enter the Desired capacity as 0. The Desired capacity value must be less that the Maximum Capacity value. <div> 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. </div>	Creating an Auto Scaling group using a launch template	Yes
Automatic Scaling	Select Target tracking scaling policy and enter the following details to define a policy: Metric Type: 1000000000 (bytes) Instance warmup: 300 seconds	Create a target tracking scaling policy	Yes
Add tag	Provide Key as GigamonNode and Value as VSeriesNode for each tag.	Tag Auto Scaling groups and instances	No

In the Instances page, you can view the GigaVUE V Series Node instance deployed by the load balancer.

What to do Next

After creating load balancer and autoscaling groups, you must create a Monitoring Domain and launch the GigaVUE V Series Node in GigaVUE-FM. Refer to [Deploy GigaVUE V Series Nodes for Inline V Series Solution](#).

After configuring the target group, update the following attributes to enable traffic rebalancing when a V Series Node becomes unhealthy:

- **Target failover** – Turn this On to rebalance existing traffic flows. Refer to [Target failover](#) section in AWS Documentation for details.
- **Deregistration delay** – Adjust as needed to ensure seamless transition of traffic. Refer to [Deregistration delay](#) section in AWS Documentation for details.

Deploy GigaVUE V Series Nodes for Inline V Series Solution

GigaVUE V Series Node will be launched and managed by AWS Load Balancer and it will be registered with GigaVUE-FM.

To deploy GigaVUE V Series Node across the AWS accounts with Gateway Load Balancing in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > AWS**, and then click **Monitoring Domain**.
2. On the Monitoring Domain page, click the **New** button. The **Monitoring Domain Configuration** page appears.
3. In the **Monitoring Domain Configuration** page, select **Inline** as the Traffic Acquisition method. Refer to [Create a Monitoring Domain](#) for detailed information.
4. 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 in AWS for Inline V Series Solution](#) section for more detailed information.
5. (optional) Turn on the **Use FM to launch Proxy** toggle, to launch the GigaVUE V Series Proxy using GigaVUE-FM.

NOTE: You can use GigaVUE V Series Proxy if GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network. GigaVUE V Series Proxy is an optional component.

- a. From the **Image** drop-down list, select the required image.
 - b. From the **Size** drop-down list, select the instance size.
 - c. Under **Number of Instances**, specify the required number of instances.
 - d. Under **Management Subnet**:
 - e. Select the **IP Address Type** as Private or Public.
 - f. From the **Subnet** drop-down list, select the management subnet.
 - g. Click **Add Subnet** under **Additional Subnets** to add additional subnets.
 - h. Click **Add** under **Tags** to assign tags for resource identification.
6. Click **Save**. The Monitoring Domain is created successfully and you are navigated to the **AWS Fabric Launch Configuration** page.
 7. From the **Centralized VPC** drop-down list, select the VPC.
 8. From the **Gateway Load Balancer** drop-down list, select the Load Balancer configured in AWS.

9. Under **Node Groups**, you can configure multiple node groups based on the deployment use case. Refer to [Inline V Series \(AWS\)](#) for more details.
 - a. Inline Node Group: This node group is used for the Inline V Series Node that is used for traffic acquisition.
 - i. In the **Inline Node Group Name** field, enter a name for the node group.
 - ii. From the **Inline Auto Scaling Group** drop-down list, select the auto scaling group in which the Inline V Series Node is deployed.
 - b. Node Group (optional): You can configure this section if you wish to process the traffic using GigaVUE V Series Node. You can add or delete node groups using the + and - buttons.
 - i. In the **Node Group Name** field, enter a name for the node group.
 - ii. From the **Auto Scaling Group** drop-down list, select the auto scaling group configured in AWS.

NOTE: You can configure a maximum of eight Node groups.

10. Click **Save**.

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 in AWS for Inline V Series Solution](#) section 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 for Inline V Series](#)


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](#)
- [VPC](#)
- [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 VPCs. You can click **+** to create a new monitoring domain. This filter once applied also works even when the tabs are swapped.


To edit or delete a specific Monitoring Domain, select the Monitoring Domain, click the ellipses .

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

Monitoring Domain

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

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

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

Use the following buttons to manage your Monitoring Domain:

Button	Description
New	Use to create new monitoring domain.
Manage Certificates	<p>You can use this button to perform the following actions:</p> <ul style="list-style-type: none"> • Re-issue- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments. • Renew- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime. Auto-renewal is performed based on the duration specified in the Certificate Settings page. Refer to Configure Certificate Settings for more details.
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.

Button	Description
	<ul style="list-style-type: none"> • 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 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 • Acquisition Method • Load Balancer • 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>

VPC

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

The list view shows the following details:

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

Fabric

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

The list view shows the following details:

- VPC
- 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.
- **Generate Sysdump** - You can select one or multiple GigaVUE V Series Nodes (Maximum 10) to generate the system files. The generation of sysdump takes a few minutes in a GigaVUE V Series Node. You can proceed with other tasks, and upon completion, the status appears in the GUI. These system files are helpful for troubleshooting. For more information, refer to [Debuggability and Troubleshooting](#).

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

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

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

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

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 UCT-V Features

Refer to the following sections for more detailed information:

- [Configure Prefiltering](#)
- [Create Precryption Template for UCT-V](#)
- [Configure Secure Tunnel \(AWS\)](#)

Configure Prefiltering

For prefiltering the traffic, GigaVUE-FM allows you to create a prefiltering policy template and the policy template can be applied to a monitoring session.

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

Each monitoring session can have a maximum of 16 rules.

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

Rules and Notes

- Prefiltering is supported on UCT-V for Windows systems and Linux systems running Kernel version 4.18 or later.
- Prefiltering is supported for both Linux and Windows UCT-Vs .
- For single monitoring session only one prefiltering policy is applicable. All UCT-Vs 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.

Create Prefiltering Policy Template

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

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

1. Go to **Traffic > Resources > Prefiltering**. Click **UCT-V**.
2. Click **New**.
3. Enter the name of the template in the **Template Name** field.
4. Enter the name of a rule in the **Rule Name** field.
5. Click any one of the following options:
 - Pass — Passes the traffic.
 - Drop — Drops the traffic.

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

6. Click any one of the following options as per the requirement:
 - Bi-Directional — Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
 - Ingress — Filters the traffic that flows in.
 - Egress — Filters the traffic that flows out.

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

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

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

- L3
- L4

9. Select the **Filter Name** from the following options:

- ip4Src
- ip4Dst
- ip6Src
- ip6Dst
- Proto - It is common for both ipv4 and ipv6.

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

- Not Equal to
- Equal to

11. Enter the source or destination port value in the **Value** field.

12. Click **Save**.

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

To enable prefiltering for a Monitoring Session, refer to [Configure Monitoring Session Options \(AWS\)](#).

Create Precryption Template for UCT-V

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

Rules and Notes:

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

- When a single UCT-V is associated with two different Monitoring Sessions with contrasting pass and drop rules, then instead of prioritizing a single rule, GigaVUE-FM will pass all the traffic.
- Once the templates are associated with a Monitoring Session, any changes made in the template will not be reflected in the Monitoring Session.

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

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

Create Precryption Template for Filtering based on Applications

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

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

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

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

Create Precryption Template for Filtering based on L3-L4 details

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

Fields	Description
Template	Enter a name for the template.
Rule Name	Enter a name for the rule.
Action	<p>Choose any one of the following options:</p> <ul style="list-style-type: none"> • Pass — Passes the traffic. • Drop — Drops the traffic. <p>NOTE: In the absence of a Precryption rule, traffic is implicitly allowed. However, once rules are defined, they include an implicit pass all rule. Should the traffic not conform to any of the specified rules, it will be passed.</p>
Direction	<p>Choose any one of the following options:</p> <ul style="list-style-type: none"> • Bi-Directional — Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule. • Ingress — Filters the traffic that flows in. • Egress — Filters the traffic that flows out.
Priority	Select the value of the priority based on which the rules must be prioritized for filtering. Select the value as 1 to pass or drop a rule in top priority. Similarly, you can select the value as 2, 3, 4 upto 8, where 8 can be used for setting a rule with the least priority. Drop rules are added based on the priority and, then pass rules are added.
Filters	
Filter Type	<p>Select the Filter Type from the following options:</p> <ul style="list-style-type: none"> • L3 • L4 <p>NOTE: L4 Filter Type can only be used with L3.</p>
L3:	
Filter Name	<p>Select the Filter Name from the following options:</p> <ul style="list-style-type: none"> • IPv4 Source • IPv4 Destination • IPv6 Source • IPv6 Destination • Protocol - It is common for both IPv4 and IPv6.
Filter Relation	<p>Select the Filter Relation from any one of the following options:</p> <ul style="list-style-type: none"> • Not Equal to • Equal to
Value	Enter or Select the Value based on the selected Filter Name .

Fields	Description
	NOTE: When using Protocol as the Filter Name , select TCP from the drop-down menu.
L4:	
Filter Name	Select the Filter Name from the following options: <ul style="list-style-type: none"> Source Port Destination Port
Filter Relation	Select the Filter Relation from any one of the following options: <ul style="list-style-type: none"> Not Equal to Equal to
Value	Enter the source or destination port value.

4. Click **Save**.

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

The template is successfully created. To enable Precryption, refer to [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 Secure Tunnel (AWS)

The Secure tunnel can be configured on:

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

Precryption Traffic

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

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

It is recommended always to enable secure tunnels for Precryption traffic to securely transfer 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](#)
- [Configure Secure Tunnel between GigaVUE V Series Nodes and GigaVUE HC Series](#)

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><tr><th>Field</th><th>Action</th></tr><tr><td>Alias</td><td>Alias name of the CA.</td></tr><tr><td>File Upload</td><td>Choose the certificate from the desired location.</td></tr></table>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 Upload SSL Keys section.</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 Precryption 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 Configure GigaVUE Fabric Components in GigaVUE-FM section.</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><tr><th>Field</th><th>Action</th></tr><tr><td>Alias</td><td>Alias name of the CA.</td></tr><tr><td>File Upload</td><td>Choose the certificate from the desired location.</td></tr></table>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 Precryption 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</p>						

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

S. No	Task	Refer to								
	monitoring domain and configuring the fabric components in GigaVUE-FM in the second GigaVUE V Series Node.	Node. To select the SSL key, refer to Configure GigaVUE Fabric Components in GigaVUE-FM section.								
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.	<p>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.</p> <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><tr><th>Field</th><th>Action</th></tr><tr><td>Alias</td><td>The name of the tunnel endpoint.</td></tr><tr><td>Description</td><td>The description of the tunnel endpoint.</td></tr><tr><td>Type</td><td>Select TLS-PCAPNG for creating egress secure tunnel.</td></tr></table> <div><p>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.</p></div>	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.
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.									

S. No	Task	Refer to									
		<table><tr><th>Field</th><th>Action</th></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></table>	Field	Action	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										
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).										
		4. Click Save .									

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

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 the steps given below:

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

Viewing Status of Secure Tunnel for UCT-V

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

To verify the status of secure tunnel:

1. Go to **Inventory > VIRTUAL > AWS** , and then click **Monitoring Domain**.
2. In the Monitoring Domain page, **Tunnel status** displays the status of the tunnel. The green color represents that the tunnel is connected and the red represents that the tunnel is not connected.

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

Configure Monitoring Session

This chapter describes how to setup ingress and egress tunnel, maps, applications in a monitoring session to receive and send traffic to the GigaVUE 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 \(AWS\)](#)
- [Configure Monitoring Session for Inline V Series](#)
- [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.
 - From the **VPC** drop-down list, select the required VPCs to include as part of the Monitoring Domain.
 - Enable the **Distribute Traffic** option to identify duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring.

NOTE: Note: Distributed Deduplication is only supported on GigaVUE V Series Node version 6.5.00 and later.

4. Select **Save**.
The Monitoring Session Overview page appears.

Monitoring Session Page (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

Tab	Description
	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.
Topology	Displays the fabric and monitored instances based on the connections configured in your network. You can select a specific connection to explore its associated subnets and instances in the topology view, offering a clear visualization of the monitored network elements. Refer to Visualize the Network Topology (AWS) .

NOTE: Ensure that the GigaVUE V Series Node and GigaVUE-FM are time synchronized or configure NTP time synchronization.

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

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

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

- Create a new Monitoring Session
- Rename a Monitoring Session
- Hover over, click the check box of the required Monitoring Session(s) and perform bulk actions (Delete, Deploy, or Undeploy).

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:

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

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

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

Enable Prefiltering

To enable Prefiltering:

1. In the **TRAFFIC ACQUISITION** page, go to **Mirroring > Edit Mirroring**.
2. Enable the **Mirroring** toggle button.
3. Enable **Secure Tunnel** option if you wish to use Secure Tunnels. Refer to the *Configure Secure Tunnel* section in the respective GigaVUE Cloud Suite Deployment Guide.
4. You can select an existing Prefiltering template from the **Template** drop-down menu, or you can create a new template using **Add Rule** option and apply it. Refer to [Create Prefiltering Policy Template](#). Click the **Save as Template** to save the newly created template.
5. Click **Save** to apply the template to the Monitoring Session.

Enable Precryption

Keep in mind the following before you enable Precryption:

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

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

To enable Precryption:

1. In the **TRAFFIC ACQUISITION** page, select **Precryption** tab and click **Edit Precryption**.
2. Enable the **Precryption** toggle button. Refer to Precryption™ topic in the respective cloud guides for details.

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

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

Applications:

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

L3-L4

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

Validate Precryption connection

To validate the Precryption connection, follow the steps:

- To confirm it is active, navigate to the Monitoring Session **Overview** tab and check the Traffic Acquisition Options.
- Click **Precryption**, to view the rules configured.

Limitations

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

TRAFFIC PROCESSING

To navigate to **TRAFFIC PROCESSING** tab:

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

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

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

Apply Threshold Template

To apply threshold:

1. In the **TRAFFIC PROCESSING** page, select **Thresholds** under **Options** menu.
2. You can select an existing threshold template from the **Select Template** drop-down list, or you can create a new template using **New Threshold Template** option and apply it. Refer to [Traffic Health Monitoring](#) section for more details on Threshold Template. Click **Save** to save the newly created template.
3. Click **Apply** to apply the template to the Monitoring Session.

NOTE: You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

You can also view the related details of the applied thresholds, such as Traffic Element, Metric, Type, Trigger Values, and Time Interval in the **Threshold** window. Click **Clear Thresholds** to clear the applied thresholds across the selected Monitoring Session.

Enable User Defined Applications

To enable user defined application:

1. In the **TRAFFIC PROCESSING** page, click **User Defined Applications** under **Options** menu.
2. Enable the **User-defined Applications** toggle button.
3. You can add from the existing applications or create new User-Defined Application from the **Actions** drop-down. Refer to [User Defined Application](#).

Enable Distributed De-duplication

In the TRAFFIC PROCESSING page, click **Distributed De-duplication** under **Options** menu. Enabling the Distributed De-duplication option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring. Refer to [Distributed De-duplication](#).



Notes:

- Distributed De-duplication is only supported on V Series version 6.5.00 and later.
- From version 6.9.00, Traffic Distribution option is renamed to Distributed De-duplication.

Configure a 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 GigaVUE-FM, you must add the tag "in_use_by_gigamon" to the traffic mirror filter. 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	
Q in_use_by_gigamon X	Q Enter value	Remove
Q vpcs X	Q vpc-94372df0,vpc-0661a4db9f738700a,vpc-05469543577a2507d X	Remove

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](#).

Configure Monitoring Session for Inline V Series

When the **Traffic Acquisition Method** is **Inline**, the **IVTAP** application is available on the canvas by default. You can configure up to three tiers in a Monitoring Session and define multiple Sub Policies. Each Sub Policy can have its own ingress and egress tunnels, along with applications for traffic processing.

Rules and Notes:

1. You can configure a maximum of three tiers in a Monitoring Session.
2. You can configure a maximum of 8 Sub Policies in a Monitoring Session.
3. Each Sub Policy can have its own Ingress Tunnels, Egress Tunnels, and Applications.
4. Tier 1 supports only Maps—Inline traffic is disabled and reserved for future use.
5. Traffic from an out-of-band endpoint can either:
 - Pass through a Map and be sent to a tool using an Egress Tunnel.
 - (optional) Be sent to the GigaVUE V Series Node of the next tier for further processing.

To configure the Monitoring Session for Inline V Series Solution:

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. When the **Traffic Acquisition Method** is **Inline**, the **IVTAP** application is available on the canvas by default.

3. Drag and drop the following items to the canvas as required for Tier 1 or Sub Policy 1:
 - a. Maps from the **Map Library** section.
 - b. (Optional) Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
 - c. Egress tunnels from the **Tunnels** section.
4. (Optional) Drag and drop the following items to the canvas as required for Tier 2 or Sub Policy 2:
 - a. Ingress tunnel (as a source) from the **New** section.
 - b. Maps from the **Map Library** section.
 - c. Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
 - d. GigaSMART apps from the **Applications** section.
 - e. Egress tunnels from the **Tunnels** section.
5. Repeat Step 4 to configure a third tier, if required.
6. After placing the required items in the canvas, hover your mouse over each element, click the dot, and drag the arrow over to another item (map, application, or tunnel).
7. To create a connection between the sub-policy, hover your mouse over the egress tunnel, click the dot, and drag the arrow to the Ingress Tunnel of another Sub Policy.
8. The Blue Dot serves as an identifier to differentiate between tiers.
9. From the Actions drop-down list, select **Deploy**. The **Deploy Monitoring Session** pop-up appears.
10. For each Policy (Tier) configured in the Monitoring Session, enter the following details:
 11. In the **Policy Name** field, verify the auto-generated policy name or enter a custom name.
 12. From the **Node Group** drop-down list, select the appropriate node group associated with this policy.
 13. Under **Interface Mapping**, configure the interfaces:
 - From the **Ingress - <Tunnel>** drop-down list, select the input interface.
 - From the **Egress - <Tunnel>** drop-down list, select the output interface.
14. Click **Deploy** the Monitoring Session.

To view the GigaVUE V Series Node associated with each Sub Policy, navigate to the **V SERIES NODES** tab and select a policy from the **Select a Sub policy** drop-down menu.

What to do Next:

NOTE: To ensure traffic is routed to the GigaVUE V Series Node, you must create routing tables in AWS.

After deploying the Monitoring Session in GigaVUE-FM, you must create routing tables in AWS with the configurations specified in the [Architecture patterns for inline inspection](#) section in AWS Documentation. For more details on how to configure routing table refer to [Configure routing](#).

Create Ingress and Egress Tunnels (AWS)

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


NOTE: GigaVUE-FM lets you configure ingress tunnels in a Monitoring Session when you use the Traffic Acquisition Method UCT-V.

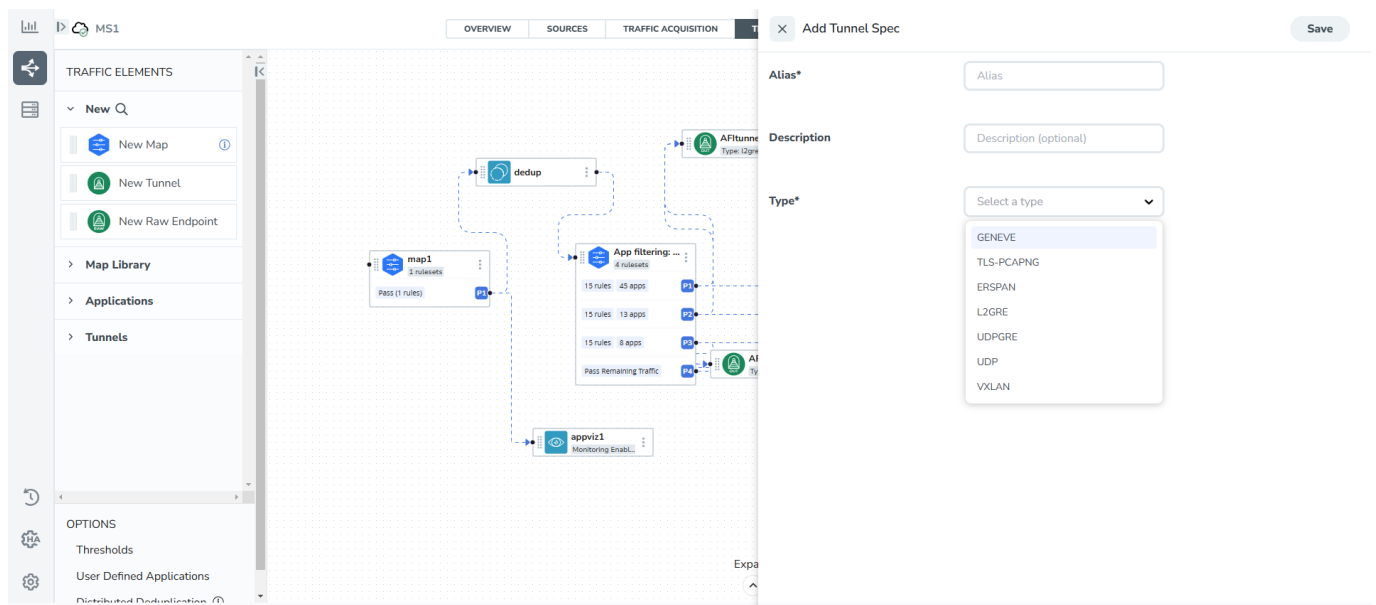
Create a new tunnel endpoint

To create,

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. 1. In the canvas, select the  icon on the left side of the page to view the traffic processing elements.
3. 2. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace.
3. 3. The **Add Tunnel Spec** quick view appears.
4. 4. Enter the **Alias**, **Description**, and **Type** details.
5. 5. 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 click **Details**.
2. In the quick view, go to the **Threshold** tab.

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

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

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

Table 1: Details - Add Tunnel Specifications

Field	Description	
Alias	The name of the tunnel endpoint.	
Description	The description of the tunnel endpoint.	
Admin State	<div>Use this option to send or stop the traffic from GigaVUE-FM to the egress tunnel endpoint. Admin State is enabled by default.</div> <div>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.</div> <div>NOTE: This option is not supported for TLS-PCAPNG tunnels.</div>	
Type	The type of the tunnel. Select from the options below to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE.	
VXLAN		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
NOTE: In the scenario where secure tunnels need to be established between a GigaVUE V Series Node and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to configure secure tunnels on your physical device conveniently. For details, refer to Secure Tunnels .		
In	Choose In (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value that is used to identify the VXLAN. The value ranges from 1 to 16777215.
	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.

Field	Description	
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Multi Tunnel	<p>Enable the multi-tunnel flag to create multiple tunnels for flow distribution to the 5G-Cloud application. Refer to 5G-Cloud Ericson SCP Support.</p> <p>Applicable Platforms: OpenStack, Third Party Orchestration, VMware ESXi</p> <div> <p>NOTE: You can configure either a single-step or multi-step setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session.</p> </div>
	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 to carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.

Field	Description	
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It routes the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
NOTE: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to the Secure Tunnels .		
In	Choose In (Decapsulation) to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
Out	Choose Out (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint.	
	Remote Tunnel IP	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.

Field	Description	
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
ERSPAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
NOTE: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to Secure Tunnels section.		

Field	Description	
In	IP Version	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	The port from which the connection 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 network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable the receipt of acknowledgments.
	Sync Retries	Enter the number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable the receipt of acknowledgments when there is a delay.
UDP:		

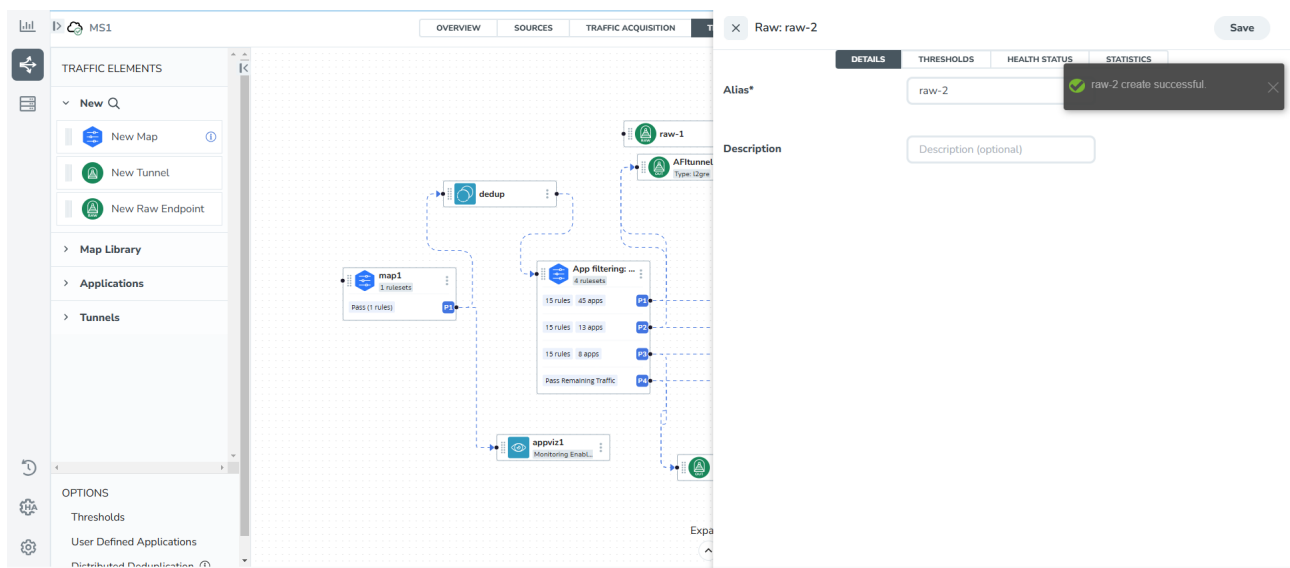
Field	Description	
Out	L4 Destination IP Address	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. For details, refer to Application Metadata Exporter .
	Source L4 Port	The port from which the connection is established 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 the **New** expand menu to the graphical workspace.
2. On the new raw endpoint icon, click the  menu button and select **Details**. The **Raw** quick view page appears.
3. Enter the Alias and Description details for the Raw End Point and click **Save**.




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

Create a New Map (AWS)

Keep in mind the following when creating a map:

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

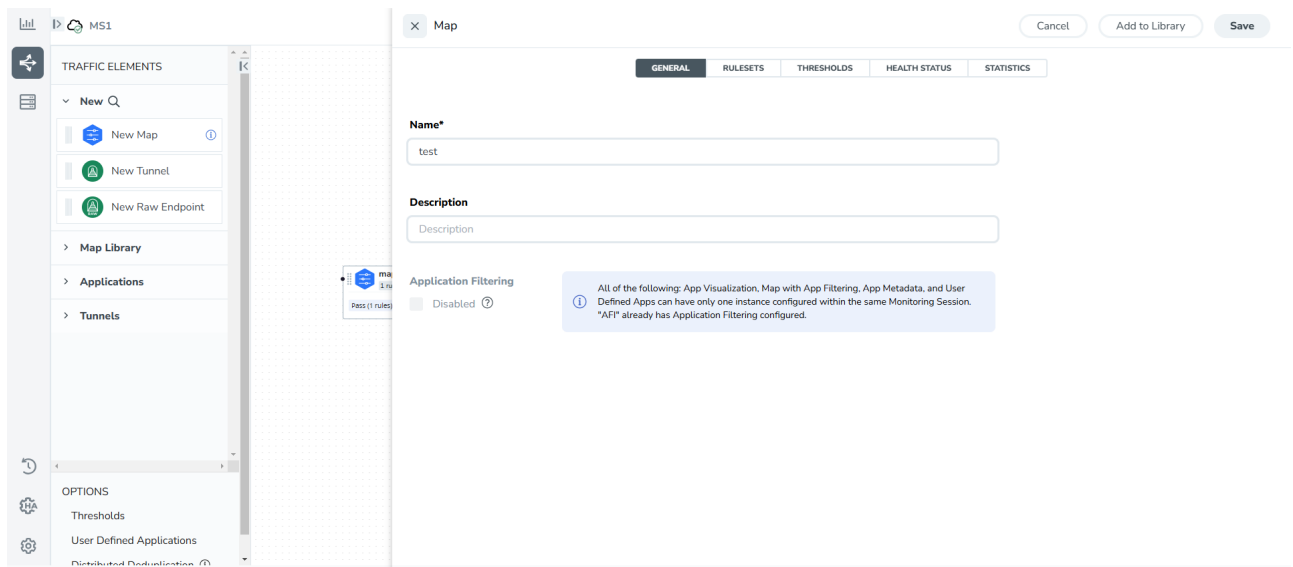
Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	<p>A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session.</p> <p>The below formula describes how ATS works:</p> <p>Selected Targets = Traffic Filter Maps \cap Inclusion Maps - Exclusion Maps</p> <p>Below are the filter rule types that work in ATS:</p> <ul style="list-style-type: none"> • mac Source • mac Destination • ipv4 Source • ipv4 Destination • ipv6 Source • ipv6 Destination • VM Name Destination • VM Name Source • VM Tag Destination • VM Tag Source <p>The traffic direction is as follows:</p> <ul style="list-style-type: none"> • For any rule type as Source - the traffic direction is egress. • For Destination rule type - the traffic direction is ingress. • For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Notes:</p> <ul style="list-style-type: none"> • 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 a packet is fragmented then all the fragments will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide* for detailed information.

To create a new map:

1. Drag and drop **New Map** from the **New** expand menu to the graphical workspace. The **Map** quick view appears.



2. On the new Map quick view, click on **General** tab and enter the required information as described below.
 - a. Enter the **Name** and **Description** of the new map.
 - b. Enable the **Application Filtering** option if you wish to use Application Filtering Intelligence. Enabling this option allows you to filter traffic based on Application name or family. Refer to [Application Filtering Intelligence](#).


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

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

3. Click on **Rule Sets** tab.a. **To create a new rule set:**

- i. Click **Actions > New Ruleset**.
- ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
- iii. Enter the Application Endpoint in the Application EndPoint ID field.
- iv. Select a required condition from the drop-down list.
- v. Select the rule to **Pass** or **Drop** through the map.


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

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

4. Click **Save**.

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

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

- To edit a map, click the  menu button of the required map on the canvas and click **Details**, or click **Delete** to delete the map.
- To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, click on the Thresholds tab. For more details on how to create or apply threshold templates, refer to [Monitor Cloud Health](#).
- Hover over the rules and apps buttons on the map to view the rule and applications configured for the selected map. Click the rules and apps buttons to open the quick view menu for RULESETS.

Example- Create a New Map using Inclusion and Exclusion Maps

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

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

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

Map Library

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*.

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).
Note: 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.

Note: 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.

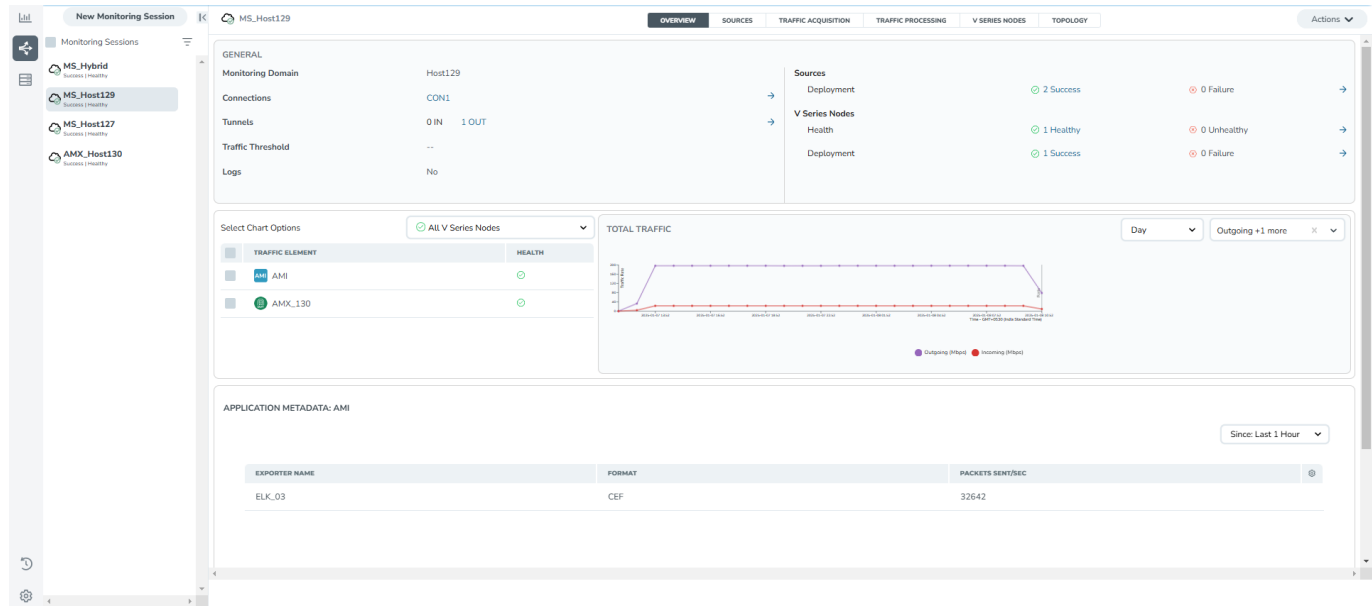
- When you select the **Status** link, the Deployment Report is displayed.
- When the deployment is incorrect, the Status column displays one of the following errors:
 - **Success:** Not deployed on one or more instances due to V Series Node failure.
 - **Failure:** Not deployed on all V Series Nodes 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.

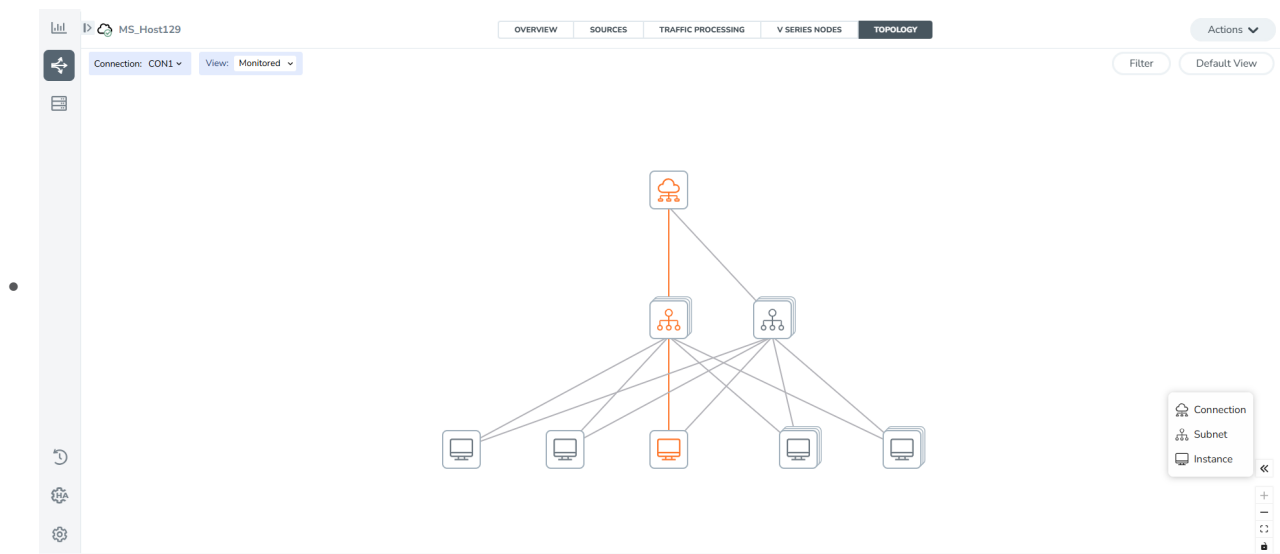
To view the topology in GigaVUE-FM:

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 the subnet or VM group icons to view details such as the subnet ID, subnet range, and the total number of subnets and instances.
8. Select the subnet or VM group icons to explore the subnets or instances within the group.

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

- Use the **Filter** button to filter the instances based on the VM name, VM IP, OS Type, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitored instances.
- Apply Navigation controls, such as:
 - Use **+** 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.

Monitor Cloud Health

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

- [Configuration Health Monitoring](#)
- [Traffic Health Monitoring](#)
- [View Health Status](#)

Configuration Health Monitoring

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

It supports specific fabric components and features on the respective cloud platforms.

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

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

Traffic Health Monitoring

GigaVUE-FM monitors the traffic health of the entire Monitoring Session and each individual GigaVUE V Series Node in that session. It checks for issues like packet drops or traffic overflows.

When it detects a problem, GigaVUE-FM updates the health status of the related Monitoring Session. It monitors traffic health in near real-time.

The GigaVUE V Series Node tracks traffic levels. If traffic goes above or below the configured threshold, it alerts GigaVUE-FM. GigaVUE-FM then uses this data to calculate traffic health.

If you deploy GigaVUE-FM and GigaVUE V Series Nodes in different cloud platforms, you must add the GigaVUE-FM public IP address as the Target Address in the Data Notification Interface on the Event Notifications page.

For details, refer to the section in the *GigaVUE Administration Guide* .

This feature supports GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

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

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

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

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

Masking	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Dedup	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
HeaderStripping	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
TunnelEncapsulation	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
LoadBalancing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SSLDecryption	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Application Metadata	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
AMI Exporter	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

5G-SBI	<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
SBIPOE	<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
PCAPNG	<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

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.

- Enter the appropriate information for the threshold template as described in the following table:

Field	Description
Threshold Template Name	The name of the threshold template.
Thresholds	
Traffic Element	Select the resource for which you wish to apply the threshold template. Ex: TEP, REP, Maps, Applications like Slicing, De-dup etc
Time Interval	Frequency at which the traffic flow needs to be monitored.
Metric	Metrics that need to be monitored. For example: Tx Packets, Rx Packets.
Type	<p>Difference: The difference between the stats counter at the start and end time of an interval, for a given metric.</p> <p>Derivative: Average value of the statistics counter in a time interval, for a given metric.</p>
Condition	<p>Over: Checks if the statistics counter value is greater than the 'Set Trigger Value'.</p> <p>Under: Checks if the statistics counter value is lower than the 'Set Trigger Value'.</p>
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.

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

Apply Threshold Template

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

Apply Threshold Template to Monitoring Session

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

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

NOTE: You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

Apply Threshold Template to Applications

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

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

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

Clear Thresholds

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

Clear Thresholds for Applications

To clear the thresholds of a particular application in the Monitoring Session, follow these steps:

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

Clear Thresholds across the Monitoring Session

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

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

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

View Health Status

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

View Health Status of an Application

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

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

This displays the application's configuration and traffic health and the thresholds applied to it.

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

View Health Status for Individual GigaVUE V Series Nodes

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

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

Upgrade GigaVUE-FM in AWS

This chapter describes how to upgrade the GigaVUE-FM instance deployed in AWS. GigaVUE-FM deployed in AWS can be upgraded in two ways. Refer to the following sections for more detailed information:

- [Upgrade GigaVUE-FM](#)
- [Upgrade GigaVUE-FM using Snapshot in AWS](#)

Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS

This chapter describes how to upgrade UCT-V Controller, GigaVUE V Series Proxy and GigaVUE V SeriesNodes.

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 replaced in the **AWS Fabric Launch Configuration** page.

UCT-V Controller version can be changed in the following two ways:

- [Upgrade between Major Versions](#)
- [Upgrade within the Same Major Version](#)

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

Upgrade between Major Versions

To upgrade between the major versions of UCT-V Controller, you must add the new version of the UCT-V Controller and remove the existing version.

NOTE: You can only add UCT-V Controllers which has different major versions. For example, you can only add UCT-V Controller version 6.8.00 if your existing version is 6.9.00.

1. Go to **Inventory > VIRTUAL > AWS**.
2. Click **Actions > Edit Fabric**. The **AWS Fabric Launch Configuration** page appears.
3. Under **Controller Versions**, click **Add**.
4. 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.
5. From the **Instance Type** drop-down list, select a size for the UCT-V Controller.
6. In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.

The screenshot shows the 'Controller Versions' section of the AWS Fabric Launch Configuration page. An 'Add' button is clicked, opening a dropdown menu for selecting a UCT-V Controller image. The dropdown list shows several options, with 'gigamon-gvtap-cntlr-1.8-4' selected. The 'Instance Type' dropdown is set to 'VXLAN', and the 'Number of Instances' is set to 1. The 'Agent Tunnel Type' is set to 'Private', and the 'IP Address Type' is set to 'Private'.

You cannot modify 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 or upgrade the UCT-V to the same version as the UCT-V Controller. Refer to [Configure UCT-V](#) for more detailed information on how to install or upgrade UCT-V.
2. Delete the UCT-V Controller with older version.

Upgrade within 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 6.10.00 to 6.10.01.

1. Go to **Inventory > VIRTUAL > AWS**.
2. Click **Actions > Edit Fabric**. The **AWS Fabric Launch Configuration** page appears.
3. Under **Controller Versions**, select a UCT-V Controller image within the same major version from the **Version** drop-down list.
4. Specify the **Number of Instances**. The minimum number you can specify is 1.
5. Select the **Subnet** from the drop-down.

You cannot modify the rest of the fields.

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.

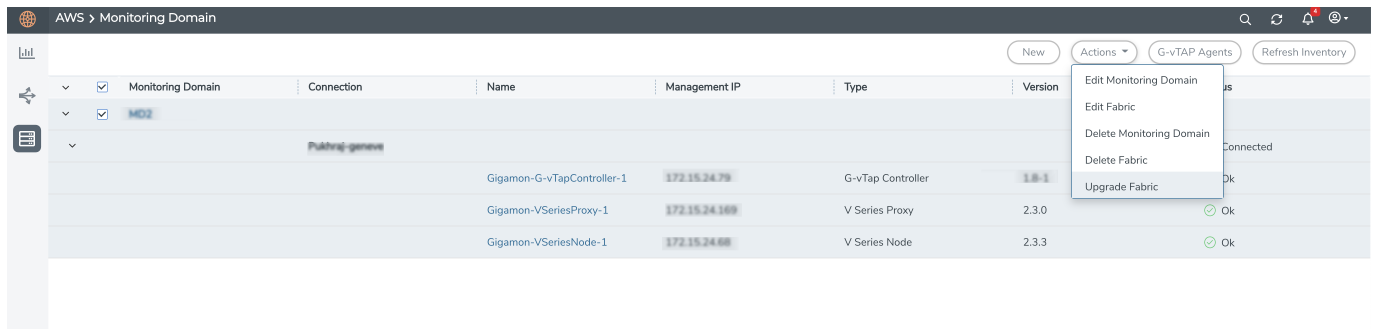
There are two ways to upgrade the GigaVUE V Series Proxy and Nodes. You can:

- 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 is 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 appears.

Fabric Nodes Upgrade

V Series Proxy

☒ Upgrade

Current Version: 2.3.0

Image:

☐ Change Instance Type

Batch Size: 1

V Series Node

☒ Upgrade

Current Version: 2.3.3

Image:

☐ Change Instance Type

Batch Size: 1

4. To upgrade the GigaVUE V Series Nodes or Proxy, select the **Upgrade** checkbox.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V Series Proxy or Nodes.
6. Select the **Change Instance Type** checkbox to change the instance type of the nodes or proxy, only if required.
7. To upgrade the GigaVUE V Series Nodes or Proxy, specify the batch size in the **Batch Size** box.

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

8. Click **Upgrade**.

The upgrade process takes a while depending on the number of GigaVUE V Series Proxy and Nodes upgrading in your 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.

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](#)
- [Configure Certificate Settings](#)
- [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**.

Advanced Settings		Edit
	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
	Use UCT-V conf file ⓘ	Enabled
	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.

Settings	Description
Permissions status purge interval in days	Specifies the number of days at which the permissions report must be auto purged,
Use UCT-V conf file	<p>Enable this option to allow interface mirroring to follow the configuration defined in the file. Disable it to mirror traffic from all physical interfaces.</p> <div>  Notes: <ul style="list-style-type: none"> When changing the UCT-V conf file option from enabled to disabled, ensure to undeploy the Monitoring Session and delete the Monitoring Domain. Once changed, you should create a new Monitoring Domain and configure the Monitoring Session. When changing the UCT-V conf file option from disabled to enabled, do the following: <ul style="list-style-type: none"> a. Edit the uctv.conf file <ul style="list-style-type: none"> i. Windows: C:\ProgramData\Uctv\uctv.conf ii. Linux: /etc/uctv/uctv.conf b. Delete the skipConf file from the backup folder <ul style="list-style-type: none"> i. Windows: C:\ProgramData\Uctv\bak\skipConf ii. Linux: /var/lib/uctv/bak/skipConf c. Restart the UCT-V <ul style="list-style-type: none"> i. Windows: Restart from the Task Manager ii. Linux: sudo service uctv restart </div>
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**.

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**.

NOTE: The updated mappings take effect when deployed.

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 then click **Settings**.
2. From the Settings drop-down list, select **Proxy Server Configuration**.
3. Click **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

☐ NTLM

4. In the **Alias** field, enter a name for the proxy server.
5. In the **Host** field, enter the hostname or IP address of the proxy server.
6. In the **Port** field, enter the port number used by the proxy server for connecting to the Internet(0–65535).
7. (Optional) In the **Username** field, enter the proxy server username.
8. In the **Password** field, enter the password for the proxy server.
9. (Optional) To use NTLM authentication:
 - Select the **NTLM** checkbox.
 - Enter the **Domain** name of the client accessing the proxy server.
 - Enter the **Workstation** name or the computer accessing the proxy server.
10. Click **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.

Configure Certificate Settings

To configure certificate settings:

1. Go to **Inventory > VIRTUAL**.
2. Select your cloud platform.
3. Select **Settings > Certificate Settings**. The **Certificate Settings** page appears.

- From the **Algorithm** drop-down list, select the algorithm that determines the cryptographic security of the certificate.

NOTE: Note: If selecting RSA 8192, the certificate generation may take longer due to the increased key size.

- In the **Validity** field, enter the total validity period of the certificate.
- In the **Auto Renewal** field, enter the number of days before expiration of the auto-renewal process should begin.
- Select **Save**.

About Events

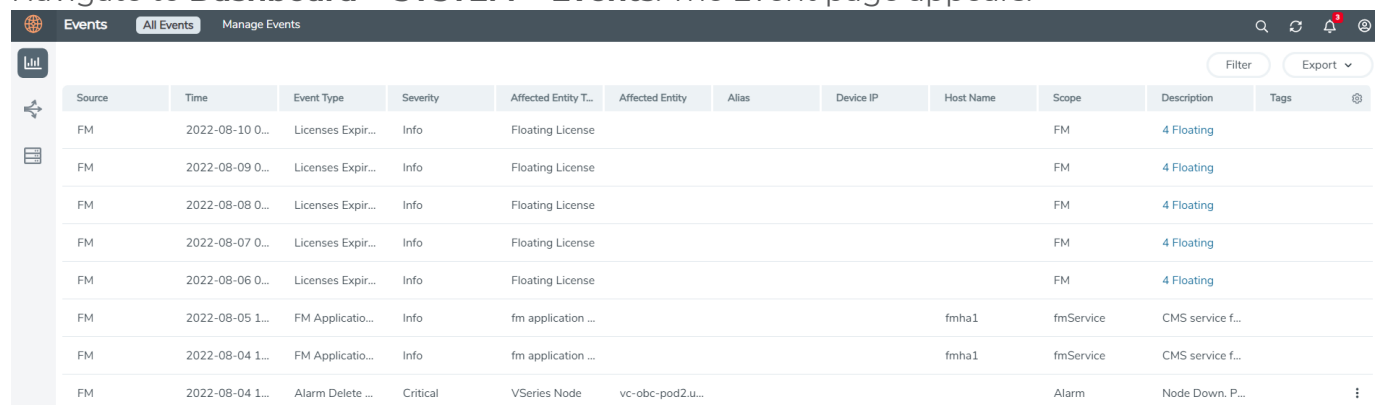
The Events page displays all the events occurring in the virtual fabric component, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

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

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

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

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



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

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

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

To filter the alarms and event:

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

About Audit Logs

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

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

All Audit Logs Filter Manage

Filter : none

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

< < Go to page: 1 of 16 > > Total Records: 106

The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: <ul style="list-style-type: none"> Log in and Log out based on users. Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details on whether the user was in GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

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

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

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

To filter the audit logs, do the following:

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

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

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

Cloud Platform	Instance Size	Maximum Number of Flows
AWS	AMD - Large (c5n.2xlarge)	300k
	AMD - Medium (t3a.xlarge)	100k
	ARM - Large (c7gn.2xlarge)	100k
	ARM - Medium (m7g.xlarge)	200k

- h. Click **Deploy**. Refer to Application Intelligence section in the GigaVUE V Series Applications Guide for more detailed information on how to deploy the Application Intelligence applications.
2. When GigaVUE-FM version is 6.5.00, and the GigaVUE V Series Node version is below 6.5.00, after migrating 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 will be seen while redeploying the monitoring session.

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

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> <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> <p>NOTE: You cannot use the time based filter</p> </div>

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

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

Dashboard	Displays	Visualizations	Displays
	<p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session • V Series node • Application: Select the required application. By default, the visualizations displayed includes all the applications. <p>By default, the following statistics are displayed:</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Errored Packets • Dropped Packets 		
		<i>App 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>	<i>Endpoint Bytes</i>	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	Visualizations	Displays
	<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) 		
		Endpoint Packets	Displays received traffic vs transmitted traffic, as the number of packets.

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


Analytics for Inline V Series Solution

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

Analytics support is available for the following cloud platforms:

- AWS
- Azure

To access the dashboards:

1. From the left navigation pane, go to  -> **Analytics -> Dashboards.**
2. Navigate to **System Dashboards -> Inline.**
3. From the **Load Balancer** drop-down list, select the Gateway load Balancer configured in AWS.
4. From the **Monitoring Session** drop-down list, select the Monitoring Session in which Inline V Series solution is configured.
5. From the **Node Name** drop-down list, select the GigaVUE V Series Node.

The following tables lists the various visualizations for Inline V Series solution:

Table 2: Overall 5G Apps Dashboard

Dashboard	Description	Visualizations	Details
Inline Source (Packets)	Displays the overall visualization details of Inline V Series Solution	LoadBalancer to Inline Source Average Packets	Displays the Inline traffic received from the Load balancer to the Inline V Series Node interface in packets.
		Inline Source to Load Balancer Average Packets	Displays the Inline traffic sent back from the Inline V Series Node interface to the Load balancer in packets.
		LoadBalancer to Inline Source App Average Packets	Displays the Inline traffic received from the Inline V Series Node interface to the IVTAP application in packets.
		Inline Source to LoadBalancer App Average Packets	Displays the Inline traffic sent back from the IVTAP application to the Inline V Series Node interface in packets.
		Average IVTAP App Total Packets Drop	Displays the IVTAP application total packet drops while processing the Inline traffic received from Inline V Series Node interface.
		Average Inline Source IVTAP Errors	Displays the IVTAP application errors while processing the Inline traffic received from Inline V Series Node interface
		Average Out-of-band Ingress Tunnel rx Packets	Displays the Out-of-Band traffic (Mirrored traffic) received from Inline V Series Node interface.
		Average Tool Tunnel tx Packets	Displays the bytes transmitted to the tool from GigaVUE V Series Node of the last tier.
		Average Out-of-band Ingress Tunnel Packets Drop	Displays the Out-of-Band traffic packet drops while receiving traffic(Mirrored traffic) from Inline V Series Node interface.
		Average Out-of-band Ingress Tunnel Errors	Displays the Out-of-Band errors while receiving traffic(Mirrored traffic) from Inline V Series Node interface.
Inline Source (Bytes)	Displays the overall visualization details of Inline V Series Solution	Load Balancer to Inline Source Average Bytes	Displays the Inline traffic received from the Load balancer to the Inline V Series Node

Dashboard	Description	Visualizations	Details
			interface in bytes.
		Inline Source to Load Balancer Average Bytes	Displays the Inline traffic sent back from the Inline V Series Node interface to the Load balancer in bytes.
		LoadBalancer to Inline Source App Average Bytes	Displays the Inline traffic received from the Inline V Series Node interface to the IVTAP application in bytes.
		Inline Source to LoadBalancer App Average Bytes	Displays the Inline traffic sent back from the IVTAP application to the Inline V Series Node interface in bytes.
		Average Out-of-band Ingress Tunnel rx Bytes	Displays the Out-of-Band traffic (Mirrored traffic) received from Inline V Series Node interface in bytes.
		Average Tool Tunnel tx Bytes	Displays the bytes transmitted to the tool from GigaVUE V Series Node of the last tier in bytes.
Heart Beat Analytics		Average LoadBalancer To Inline Source Heart Beat Packets	Displays the Health Check request packets (Heart beat packets) received by Inline V Series Node from Load balancer
		Average Inline Source To LoadBalancer Heart Beat Packets	Displays the Health Check response packets (Heart beat packets) sent by Inline V Series Node to Load balancer.

Debuggability and Troubleshooting

Use the following information to help diagnose and resolve GigaVUE V Series Nodes issues.

Sysdumps

A sysdump is a log and system data package generated when a GigaVUE V Series Node experiences a crash (such as kernel, application, or hardware failure). These files are essential for debugging.

Note: You cannot download sysdump files if the associated fabric component is deleted or unreachable.

Sysdumps—Rules and Notes

Consider the following points before you generate sysdumps:

- - You can generate only one sysdump file at a time for a GigaVUE V Series Node.
- - You cannot generate a sysdump file when generation of another sysdump file is in progress.
- - The limit of sysdump files available per GigaVUE V Series Node is six. When you generate a seventh sysdump file, the file overwrites the first sysdump file.
- - You can download only one sysdump file per GigaVUE V Series Node at a time.
- - You can delete sysdump files in bulk for a GigaVUE V Series Node.
- - To ensure efficient usage, the system limits the number of simultaneous sysdump generation requests to 10 GigaVUE V Series Nodes.
- - GigaVUE V Series Node sysdumps are not stored in Fabric Manager but generated and stored on the GigaVUE V Series Node itself.

Generate a Sysdump File

To generate a sysdumps file:

1. Perform one of the following:
 - Go to **Inventory > VIRTUAL > AWS > Fabric**.
 - Go to **Inventory > VIRTUAL > Azure > Fabric**.
 - Go to **Inventory > VIRTUAL > OpenStack > Fabric**.The **Fabric** page appears.
2. Select the required node, and use one of the following options to generate a sysdump file:
 - - Select **Actions > Generate Sysdump**.
 - - In the lower pane, go to **Sysdump**, and select **Actions > Generate Sysdump**.
3. View the latest status, click **Refresh**.

The screenshot shows the AWS GigaVUE Cloud Suite interface. At the top, there are tabs for Monitoring Domains, Connections, Fabric (selected), and UCT-V. Below the tabs, there are filters for Monitoring Domains and Connections. The main table displays Fabric Nodes with columns: FABRIC NODES, MONITORING DOMAIN, CONNECTIONS, TYPE, MANAGEMENT IP, and VERS. A row is selected, showing 'Sigamon-UCT-VContro...' under FABRIC NODES and 'FunctionalTestVPC' under MONITORING DOMAIN. Below the table, there is a section for 'Fabric Node: Gigamon-VSeriesNode-1...' with tabs for Interface, Configuration, Certificates, Sysdump (selected), and Refresh. The Sysdump tab shows a table of sysdump files with columns: FILE NAME, STATUS, DATE CREATED, and FILE SIZE. The first row is selected. An 'Actions' menu is open, showing options: Generate Sysdump, Download, Delete, and Delete All.

FABRIC NODES	MONITORING DOMAIN	CONNECTIONS	TYPE	MANAGEMENT IP	VERS
Sigamon-UCT-VContro...	FunctionalTestVPC	FunctionalTest...	UCT-V Controller	35.155.221.200	6.10

FILE NAME	STATUS	DATE CREATED	FILE SIZE
sysdump-ip-20-0-1-209-2025	Completed	2025-01-10 10:43:01	1.163 KB
sysdump-ip-20-0-1-209-2025	Completed	2025-01-10 10:41:49	1.169 KB
sysdump-ip-20-0-1-209-2025	Completed	2025-01-10 10:41:03	0.871 KB
sysdump-ip-20-0-1-209-2025	Completed	2025-01-10 10:41:00	1.342 KB

Other Actions

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

FAQs - Secure Communication between GigaVUE Fabric Components

This section addresses frequently asked questions about Secure Communication between GigaVUE Fabric Components and GigaVUE-FM. Refer to Secure Communication between GigaVUE Fabric Components section for more details.

1. Is there a change in the upgrade process for GigaVUE-FM and GigaVUE V Series Node?

No. The upgrade process remains unchanged across all supported upgrade paths. You can upgrade your nodes without any additional steps. The upgrade results in the automatic deployment of the appropriate certificates based on the node versions

GigaVUE-FM	GigaVUE V Series Nodes	Custom Certificates Selected (Y/N)	Actual Node Certificate
6.10	6.10	Y	GigaVUE-FM PKI Signed Certificate
6.10	6.9 or earlier	Y	Custom Certificate
6.10	6.9 or earlier	N	Self-Signed Certificate

2. What is the new authentication type used between GigaVUE-FM and the GigaVUE Fabric Components? Is backward compatibility supported?

Backward compatibility is supported, ensuring that fabric components running on version 6.9 or earlier remain compatible with GigaVUE-FM 6.10. The following authentication types are supported across different versions:

GigaVUE-FM	GigaVUE Fabric Components	Authentication
6.10	6.10	Tokens + mTLS Authentication (Secure Communication)
6.10	6.9 or earlier	User Name and Password

3. What are the new ports that must be added to the security groups?

The following table lists the port numbers that must be opened for the respective fabric components:

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

4. Is the registration process different for deploying the fabric components using Third-Party Orchestration?

Yes. Beginning with version 6.10, you must use tokens in the gigamon-cloud.conf file instead of the username and password. To generate the token in GigaVUE-FM, go to **Settings > Authentication > User Management > Token**. For more details, refer to [Configure Tokens](#).

Example Registration Data for UCT-V:

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

5. Are there any changes to the UCT-V manual installation and upgrade process?

Starting from version 6.10, you must add tokens during manual installation and upgrades.

- Create a configuration file named gigamon-cloud.conf with the token and place it in the /tmp directory during UCT-V installation
- After installing UCT-V, you can add the configuration file in the /etc directory.

Important! Without this token, UCT-V cannot register with GigaVUE-FM.

6. Can I use my PKI infrastructure to issue certificates for the Fabric Components?

Direct integration of your PKI with GigaVUE-FM is not supported. However, you can provide your Intermediate Certificate Authority (CA) to sign the node certificate.

7. What happens to the existing custom certificates introduced in the 6.3 release?

- The custom certificate feature is not supported for the fabric components with version 6.10 or higher, even if a custom certificate is selected in the Monitoring Domain. However, this feature remains available for older versions.
- When upgrading from version 6.9 or earlier with custom certificates upgrades to version 6.10, the system automatically generates and deploys certificates signed by GigaVUE-FM.
- If deploying version 6.9 or earlier components from a 6.10 GigaVUE-FM, custom certificates are still applied.

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

When the upgrade process begins, GigaVUE-FM transmits the certificate specifications to the new fabric components using the launch script. The fabric components utilize these specifications to generate their own certificates.

9. Is secure communication supported in FMHA deployment?

Yes, it is supported. However, you must follow a few manual steps before upgrading the fabric components to 6.10. For details, refer to [Configure Secure Communication between Fabric Components in FMHA](#).

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

Glossary

This appendix lists the AWS terminologies used in this document. To find a brief definition of these terms, refer to [AWS Glossary](#).

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 6.11 Hardware and Software Guides	
DID YOU KNOW?	If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing Edit > Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware	how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide	
GigaVUE-HC3 Hardware Installation Guide	
GigaVUE-HC1-Plus Hardware Installation Guide	
GigaVUE-HCT Hardware Installation Guide	
GigaVUE-TA25 Hardware Installation Guide	
GigaVUE-TA25E Hardware Installation Guide	
GigaVUE-TA100 Hardware Installation Guide	

GigaVUE Cloud Suite 6.11 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA400E Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide
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

GigaVUE Cloud Suite 6.11 Hardware and Software Guides	
Universal Cloud TAP - Container Deployment Guide	
Gigamon Containerized Broker Deployment Guide	
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions	
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions	
Reference Guides	
GigaVUE-OS CLI Reference Guide	library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices
GigaVUE-OS Security Hardening Guide	
GigaVUE Firewall and Security Guide	
GigaVUE Licensing Guide	
GigaVUE-OS Cabling Quick Reference Guide	guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix	compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide	samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices	Sanitization guidelines for GigaVUE Fabric Management Guide and GigaVUE-OS devices.
Release Notes	
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes	new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release
NOTE: Release Notes are not included in the online documentation.	
NOTE: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon . Refer to How to Download Software and Release Notes from My Gigamon .	
In-Product Help	
GigaVUE-FM Online Help	how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

1. Log in to [My Gigamon](#).
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to:

documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	

For Online Topics	Online doc link	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>
For PDF Topics	Document Title	<i>(shown on the cover page or in page header)</i>
	Product Version	<i>(shown on the cover page)</i>
	Document Version	<i>(shown on the cover page)</i>
	Chapter Heading	<i>(shown in footer)</i>
	PDF page #	<i>(shown in footer)</i>
How can we improve?	Describe the issue	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The **VÜE Community** is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜECommunity 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)