GigaVUE Cloud Suite Deployment Guide - AWS

GigaVUE Cloud Suite

Product Version: 6.4

Document Version: 1.0

Last Updated: Tuesday, February 27, 2024

(See Change Notes for document updates.)

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.4.00	1.0	09/08/2023	The original release of this document with 6.4.00 GA.

Contents

GigaVUE Cloud Suite Deployment Guide - AWS 1
- Change Notes 3
- Contents 4

Overview of GigaVUE Cloud Suite for AWS 9
- GigaVUE-FM 10
- UCT-V 11
- UCT-V Controller 12
- GigaVUE V Series Node 13
- GigaVUE V Series Proxy 14
- Traffic Acquisition 14
- Monitoring Domain 15
- Monitoring Session 15
- Third Party Orchestration 15

Introduction to the Supported Features in AWS 16
- Precryption™ 16
  - How Gigamon Precryption Technology Works 17
  - Why Gigamon Precryption 17
  - Key Features 17
  - Key Benefits 18
  - How Gigamon Precryption Technology Works 18
  - Supported Platforms 20
  - Prerequisites 21
- Secure Tunnels 21
- Prefiltering 24
  - Prefiltering 25
  - AWS VPC Traffic Pre-filter 26
- Load Balancer 28
- Fabric Health Analytics for Virtual Resources 29
  - Virtual Inventory Statistics and Cloud Applications Dashboard 29
- Traffic Health Monitoring 35

Licensing GigaVUE Cloud Suite 36
- Purchase GigaVUE Cloud Suite using CPPO 37
- Volume Based License (VBL) 37
  - Base Bundles 38
  - Add-on Packages 38

How GigaVUE-FM Tracks Volume-Based License Usage 39
Manage Volume-based Licenses 39
Prerequisites 44
Subscribe to GigaVUE Cloud Suite Components 44
AWS Security Credentials 44
Amazon VPC 45
Subnet for VPC 45
Security Group 45
Key Pair 48
Default Login Credentials 48
Points to Note 49
Deploy GigaVUE Cloud Suite for AWS 50
Use Cases - Gigamon Validated Design 50
Deploying GigaVUE Cloud Suite Across Multiple Accounts on AWS Cloud 51
AWS VPC Mirroring with Application Filter Intelligence and Slicing 51
Gigamon Precryption™ with Secure Tunnel to Gain Visibility into the Cloud (AWS) Environment 51
Examples- Permissions 53
GigaVUE-FM Instance Multi Account Support Using Amazon STS 54
Example: Traffic Acquisition using the UCT-V 56
Example: Traffic Acquisition using the Customer Orchestrated Source 57
Example: Traffic Acquisition using the Customer Orchestrated Source with GwLB 58
Example: Traffic Acquisition using the Customer Orchestrated Source with NwLB 59
Example: Traffic Acquisition using VPC Mirroring 60
Example: Traffic Acquisition using VPC Mirroring with Network Load Balancer 61
Example: Traffic Acquisition using VPC Mirroring and GwLB 62
Install GigaVUE-FM on AWS 64
Subscribe GigaVUE Products 64
Initial GigaVUE-FM Configuration 65
Create AWS Credentials 66
Install Custom Certificate 68
Adding Certificate Authority 69
CA List 69
Create a Monitoring Domain 70
Managing Monitoring Domain 74
Traffic Acquisition Methods 77
Configure GigaVUE Fabric Components in GigaVUE-FM 80
Configure UCT-V Controller 81

Configure GigaVUE V Series Proxy 84
Configure GigaVUE V Series Node 84
Configure Role-Based Access for Third Party Orchestration 85
Users 86
Add Users 86
How to Unlock User Account 88
Create Roles 88
Create Roles 88
Create User Groups 91
Create User Groups 92
Configure GigaVUE Fabric Components in AWS 94
Configure GigaVUE V Series Nodes and V Series Proxy in AWS 95
Configure UCT-V Controller in AWS 99
Configure UCT-V in AWS 103
Install UCT-V 105
Supported Operating Systems for UCT-V 105
Install Linux UCT-V Agent 106
Windows UCT-V Installation 113
Create Images with Agent Installed 118
Configure Monitoring Session 119
Create a Monitoring Session 119
Edit Monitoring Session 121
Enable Prefiltering, Precryption, and Secure Tunnel 122
Prefiltering 122
Interface Mapping 124
Create Ingress and Egress Tunnels 125
Create Raw Endpoint 132
Create a New Map 133
Example- Create a New Map using Inclusion and Exclusion Maps 137
Add Applications to Monitoring Session 137
Deploy Monitoring Session 138
View Monitoring Session Statistics 140
View Health Status on the Monitoring Session Page 141
Health 141
V Series Node Health 141
Target Source Health 142
Visualize the Network Topology 142
Configure Application Intelligence Solutions on GigaVUE V Series Nodes for AWS 144
Configure Environment 146
Create Environment 146
Create Credentials 148

Create AWS Credentials 148
Connect to AWS 149
Create Connection 149
Create Source Selectors 156
Create Tunnel Specifications 159
User Defined Application 161
Create Rules under User Defined Application 161
Supported Protocols and Attributes 162
Mindata 166
Supported RegExp Syntax 166
Limitations 167
Slicing and Masking in Application Filtering Intelligence 168
Configuring Application Filtering Intelligence with Slicing 168
Configuring Application Filtering Intelligence with Masking 168
Configuring Application Filtering Intelligence with Slicing and Masking 169
Configure Application Intelligence Session 170
Application Metadata Intelligence 173
Create Application Metadata Intelligence Session for Virtual Environment 174
Create NetFlow Session for Virtual Environment 178
NetFlow Dashboard 182
Configure a Load Balancer 183
AWS Network Load Balancer on GigaVUE Cloud Suite 184
Architecture of an External Load Balancer 185
Configure a Network Load Balancer in AWS 186
Deploy GigaVUE V Series Solution Network Load Balancing 189
Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS 191
Architecture 192
Configure a Gateway Load Balancer in AWS 193
Deploy GigaVUE V Series Solution with Gateway Load Balancer 195
Configure Precryption in UCT-V 195
Validate Precryption connection 196
Rules and Notes 196
Configure Secure Tunnel 196
Precrypted Traffic 197
Mirrored Traffic 197
Prerequisites 197
Configure Secure Tunnel from UCT-V to GigaVUE V Series Node 197
Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2 199
Viewing Status of Secure Tunnel 203

Uninstall UCT-V 203
Uninstall Linux UCT-V 203
Uninstall Windows UCT-V 204
Upgrade or Reinstall UCT-V 204
Monitor Cloud Health 204
Configuration Health Monitoring 205
Traffic Health Monitoring 205
Create Threshold Template 206
Apply Threshold Template 207
Edit Threshold Template 208
Supported Resources and Metrics 209
View Health Status 211
Administer GigaVUE Cloud Suite for AWS 213
Configure AWS Settings 214
Configure Proxy Server 215
Role Based Access Control 217
About Events 219
About Audit Logs 221
GigaVUE-FM Version Compatibility Matrix 223
Glossary 225
Additional Sources of Information 226
Documentation 226
How to Download Software and Release Notes from My Gigamon 228
Documentation Feedback 229
Contact Technical Support 230
Contact Sales 230
Premium Support 231
The VÜE Community 231
Glossary 232

Overview of GigaVUE Cloud Suite for AWS

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

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

You can deploy the GigaVUE Cloud Suite for AWS by subscribing to it in the AWS marketplace or by installing the individual fabric components using the Amazon Machine Images (AMI).

Note: You must subscribe to each component individually.

Refer to the following sections for details:

- GigaVUE-FM
- UCT-V
- UCT-V Controller
- GigaVUE V Series Node
- GigaVUE V Series Proxy
- Traffic Acquisition
- Monitoring Domain
- Monitoring Session
- Third Party Orchestration

GigaVUE-FM

GigaVUE® Fabric Manager (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 which is not possible from individual nodes.

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

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

GigaVUE-FM can be installed on-premises, launched from an Amazon Machine Image (AMI) in AWS.

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

- UCT-V Controller (only if you are using UCT-V as the traffic acquisition method)
- GigaVUE V Series® 2 Node
- (Optional) GigaVUE V Series® Proxy

UCT-V

UCT-V (earlier known as G-vTAP) is an agent that is installed in the VM instance from where you want to receive the network traffic. This agent mirrors the selected traffic over a tunnel (GRE or VXL) from the instances (virtual machines) to the GigaVUE V Series Node. The UCT-V is offered as a Debian (.deb), Redhat Package Manager (.rpm) package and for Windows server ZIP package and MSI is offered.

Next generation UCT-V is a lightweight solution that acquires traffic from Virtual Machines and in-turn improves the performance of the UCT-V mirroring capability. The solution has a prefiltering capability at the tap level that reduces the traffic flow from the agent to GigaVUE V Series Node and in-turn reduces the load on the GigaVUE V Series Node. Next generation UCT-V gets activated only on Linux systems with a Kernel version above 5.4.

Note: The Precryption feature requires the kernel version to be 5.4 and above.

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

For more information on installing the UCT-V see, Install UCT-Vs.

UCT-V Controller

UCT-V Controller (earlier known as G-vTAP Controller) manages multiple UCT-Vs and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes. GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs. A UCT-V Controller can only manage UCT-Vs that has the same version. For example, the UCT-V Controller v 6.4 can only manage UCT-Vs v 6.4. If you have UCT-Vs v 6.3 still deployed in the EC2 instances, you must configure both UCT-V Controller v 6.3 and v 6.4. 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. The tunnel type can be L2GRE or VXLAN.

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

GigaVUE V Series Node

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

For more information on installing and configuring a GigaVUE V Series Node, refer to Configure GigaVUE V Series Nodes and V Series Proxy in AWS

GigaVUE V Series Proxy

GigaVUE V Series Proxy manages multiple GigaVUE V Series nodes and orchestrates the flow of traffic from GigaVUE V Series nodes to the GigaVUE-FM. This is an optional component.

You can deploy a GigaVUE V Series Proxy when the GigaVUE-FM cannot establish a direct connection with the GigaVUE V Series Nodes. For instance, if you have hundreds of GigaVUE V Series Nodes in AWS, and the GigaVUE-FM is on-premises, you can deploy a GigaVUE V Series Proxy in AWS. By exposing only its IP and TCP port 8890 to GigaVUE-FM, you enable GigaVUE-FM to efficiently manage all 100 GigaVUE V Series Nodes through this single point of communication.

GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series nodes.

For more information on installing and configuring a GigaVUE V Series Proxy, refer to Configure GigaVUE V Series Nodes and V Series Proxy in AWS

Traffic Acquisition

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

You can acquire traffic using the following methods:

- Traffic Acquisition Method using UCT-V
- Traffic Acquisition Method using VPC Mirroring
- Traffic Acquisition Method using Customer Orchestrated Source

Monitoring Domain

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

For more information on creating a Monitoring Domain, see Create a Monitoring Domain.

Monitoring Session

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

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

For more information on creating a monitoring session, see Configure Monitoring Session.

Third Party Orchestration

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

Introduction to the Supported Features in AWS

GigaVUE Cloud Suite for AWS supports the following features:

- Precryption™
- Secure Tunnels
- Prefiltering
- Load Balancer
- Fabric Health Analytics for Virtual Resources
- Traffic Health Monitoring

Precryption™

License: Requires **SecureVUE Plus** license.

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

This section explains about:

- How Gigamon Precryption Technology Works
- Why Gigamon Precryption
- Key Features
- Key Benefits
- Precryption Technology on Single Node

[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 or G-vTAP) of unencrypted traffic and the traffic processing (at the V Series) which will better safeguard the traffic while in transit. However, if a user does not use the option for encrypted tunnels for communication, decrypted traffic will remain unencrypted while in transit between the point of acquisition and processing.

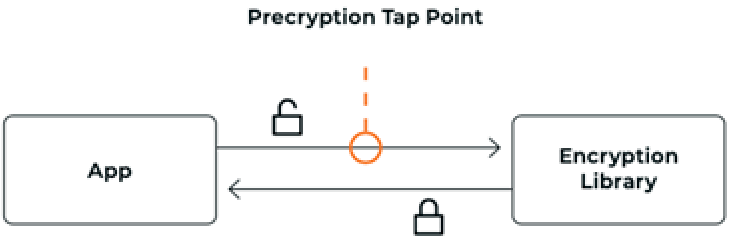
Please note that this information is subject to change, and we encourage you to stay updated on any modifications or improvements made to this feature.

By using this feature, you acknowledge and accept the current limitations and potential risks associated with the transmission of decrypted traffic.

- Precryption Technology on Multi-Node
- Supported Platforms
- Prerequisites

How Gigamon Precryption Technology Works

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



In this way, Precryption captures network traffic in plaintext, either before it has been encrypted, or after it has been decrypted. Precryption functionality doesn't interfere with the actual encryption of the message nor its transmission across the network. There's no proxy, no retransmissions, no break-and-inspect. Instead, this plaintext copy is forwarded to the Gigamon Deep Observability Pipeline for further optimization, transformation, replication, and delivery to tools.

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

Why Gigamon Precryption

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

Key Features

The following are the key features of this technology:

- Plaintext visibility into communications with modern encryption (TLS 1.3, mTLS, and TLS 1.2 with Perfect Forward Secrecy).

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

Key Benefits

The following are the key benefits of this technology:

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

How Gigamon Precryption Technology Works

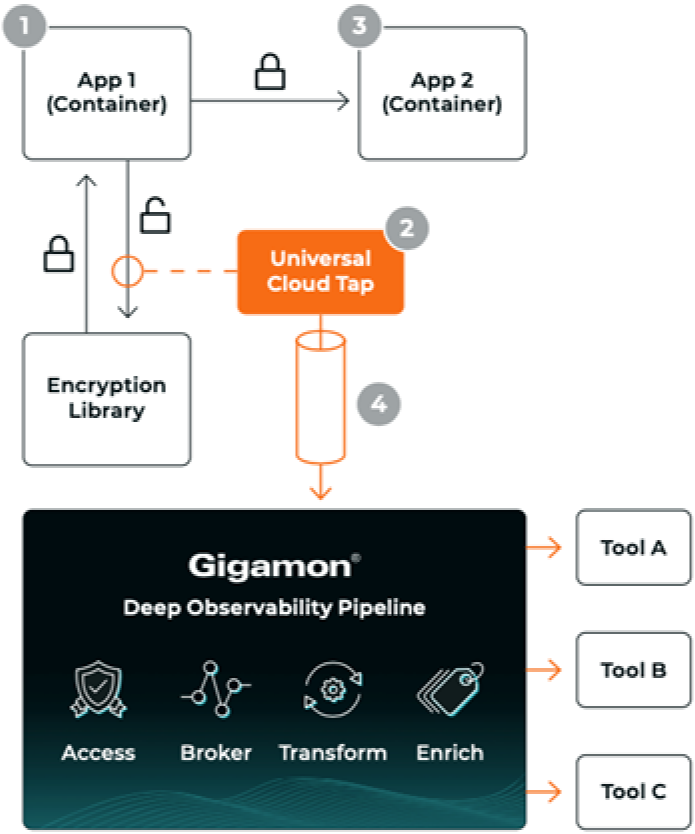
This section explains about how Precryption technology works on single node and multiple node in the following sections:

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

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.

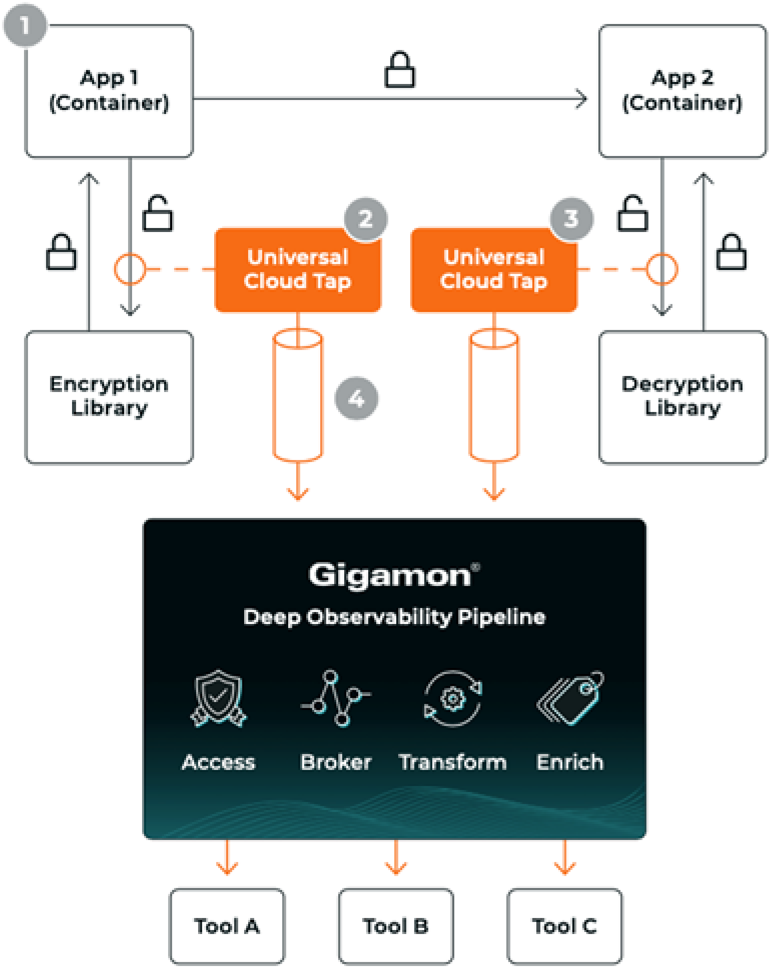
3. The encrypted message is sent to the receiving application, with unmodified encryption. No proxy, no re- encryption, no retransmissions.
4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to GigaVUE V Series in the deep observability pipeline. Gigamon further optimizes, transforms, and delivers data to tools, without need for further decryption



5.

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 in a tunnel, and forwards to V Series in the deep observability pipeline where it is further enriched, transformed, and delivered to tools, without further decryption.

5. 

Supported Platforms

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

Platform Type	Platform
Public Cloud	- AWS - Azure - GCP (via Third Party Orchestration)
Private Cloud	- 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	● EKS ● AKS
Private Cloud	● OpenShift ● Native Kubernetes (VMware)

Prerequisites

Deployment Prerequisites

- Linux Kernel version 5.4 and above
- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x
- Protocol version IPv4
- For GigaVUE-FM, to capture the statistics, you must add the port 5671 in the security group
- Port 9900 should be enabled in security group settings on the UCT-V controller to receive the statistics information from UCT-V agent
- For UCT-C, you must add the port 42042 and port 5671 in the security group

License Prerequisite

- Precryption™ requires SecureVUE Plus license.

Note

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

Secure Tunnels

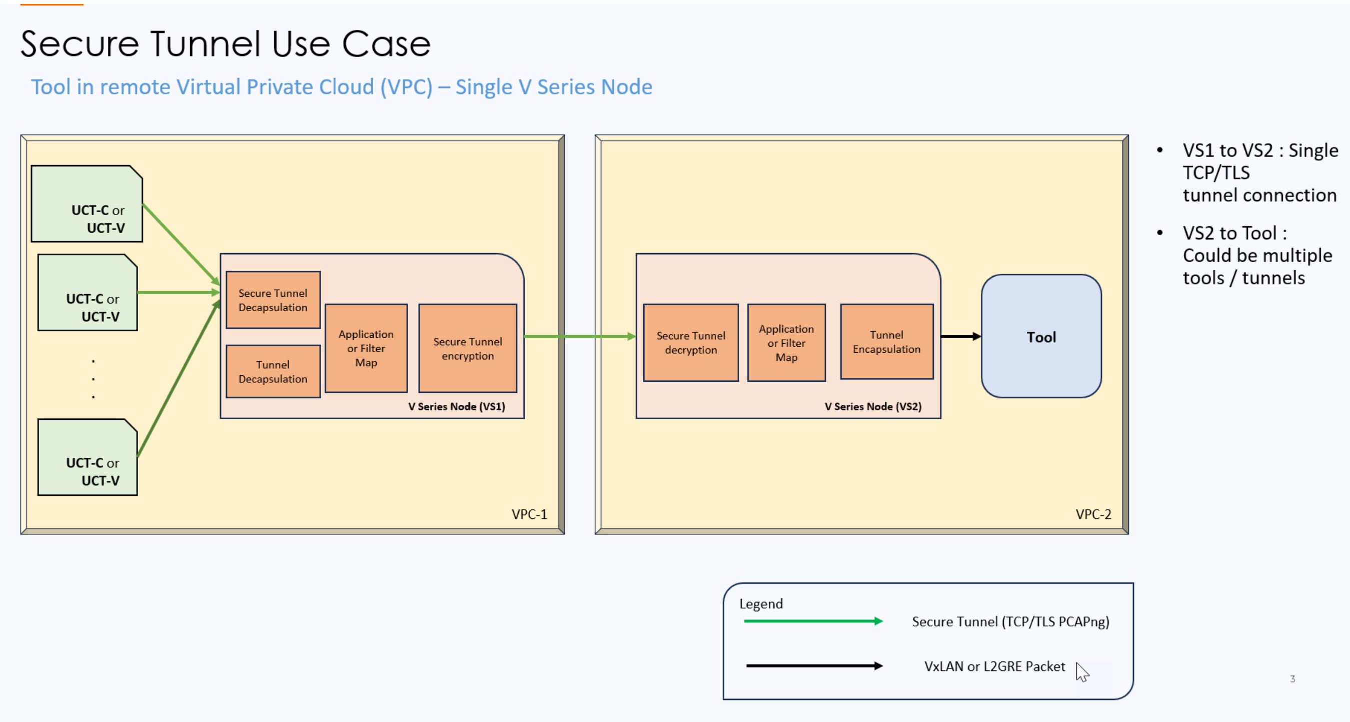
Secure Tunnel securely transfers the cloud captured packets on UCT-V and UCT-C to a GigaVUE V Series Node or Tool (only in case of UCT-C). The data from UCT-V and UCT-C are encapsulated in PCAPng format, and the encrypted data is sent over a TLS connection to a GigaVUE V Series Node.

Secure Tunnel can also transfer the cloud captured packets from a GigaVUE V Series Node to another GigaVUE V Series Node.

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

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

For more information about PCAPng, refer to PCAPng Application.



Secure Tunnel Use Case

Tool in remote Virtual Private Cloud (VPC) – Single V Series Node

- VS1 to VS2 : Single TCP/TLS tunnel connection
- VS2 to Tool : Could be multiple tools / tunnels

Supported Platforms

Secure tunnel is supported on:

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

For information about how to configure secure tunnels, refer to the section Configure Secure Tunnel.

Prefiltering

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

- Prefiltering
- AWS VPC Traffic Pre-filter

For more information on configuring a prefilter, refer to Create a Monitoring Session.

Prefiltering

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

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

Each monitoring session can have a maximum of 16 rules.

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

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

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

For more information on configuring a prefilter, refer to Create a Monitoring Session.

AWS VPC Traffic Pre-filter

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

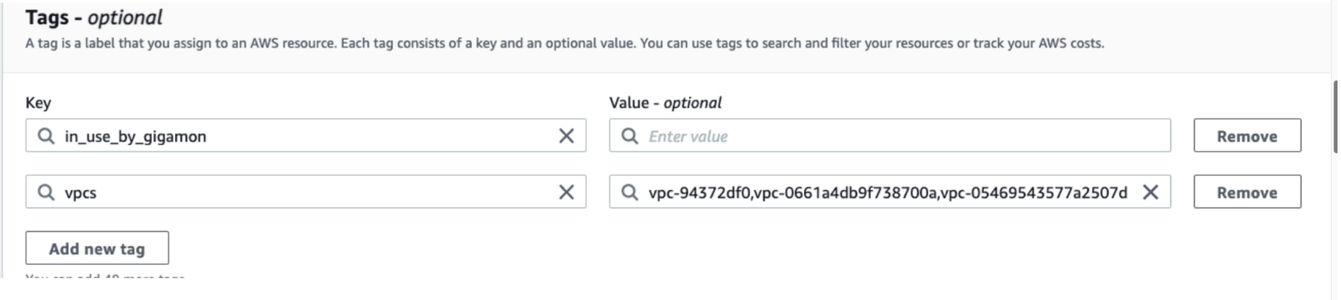
If you want to filter the traffic, then you can create a traffic mirror filter on AWS and add rules to determine the traffic that is mirrored. This traffic mirror filter acts as a pre-filter and pass only the filtered traffic to the GigaVUE V Series Nodes.

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

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

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

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



Tags - *optional*

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

Key	Value - *optional*
in_use_by_gigamon	*Enter value*
vpcs	vpc-94372df0,vpc-0661a4db9f738700a,vpc-05469543577a2507d

> **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 FM will pick a random filter and no error will be displayed.

For more information on creating a traffic mirror, refer to the AWS documentation.

Load Balancer

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

The following load balancers are supported:

- Elastic Load Balancer
- Gateway Load Balancer

Fabric Health Analytics for Virtual Resources

Fabric Health Analytics (FHA) in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using FHA[1] 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 FHA. Dashboards, Visualizations and Search Objects are called FHA objects. Refer to Fabric Health Analytics topic in *GigaVUE Fabric Management Guide* for more detailed information on Fabric Health 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 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

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

[1] FHA uses the Kibana front-end application to visualize and analyze the data in the Elasticsearch database of GigaVUE-FM. Kibana is an open source data visualization plugin for Elasticsearch.

Dashboard	Displays	*Visualizations*	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: ● Number of Monitoring Sessions ● Number of V Series Nodes ● Number of Connections ● Number of GCB Nodes You can filter the visualizations based on the following control filters: ● Platform ● Health Status	*V Series Node Status by Platform*	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		Monitoring Session Status by Platform	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		Connection Status by Platform	Number of healthy and unhealthy connections for each of the supported cloud platforms
		GCB Node Status by Platform	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*V Series Node Maximum CPU Usage Trend*	Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour. **NOTE:** The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V-series nodes do not have service cores, therefore the CPU usage is reported as 0.
		V Series Node with Most CPU Usage For Past 5 minutes	Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes. **NOTE:** You cannot use the time based filter

Dashboard	Displays	*Visualizations*	Displays
			options to filter and visualize the data.
		V Series Node Rx Trend	Receiving trend of the V Series node in 5 minutes interval, for the past one hour.
		V Series Network Interfaces with Most Rx for Past 5 mins	Total packets received by each of the V Series network interface for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.
		V Series Node Tunnel Rx Packets/Errors	Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation.
		V Series Node Tunnel Tx Packets/Errors	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: • Platform • Connection • VSeries Node	*Dedup Packets Detected/Dedup Packets Overload*	Statistics of the total dedup packets received (ipV4Dup, ipV6Dup and nonIPDup) against the dedup application overload.
		Dedup Packets Detected/Dedup Packets Overload Percentage	Percentage of the dedup packets received against the dedup application overload.
		Total Traffic In/Out Dedup	Total incoming traffic against total outgoing traffic

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

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

Dashboard	Displays	*Visualizations*	Displays
	You can select the following control filters, based on which the visualizations will get updated: • **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 Elasticsearch database, which are available only from software version 5.14.00 and beyond.

Traffic Health Monitoring

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

For more information on how to configure a traffic health monitor, refer to the topic Monitor Cloud Health.

Licensing GigaVUE Cloud Suite

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

- Purchase GigaVUE Cloud Suite using CPPO
- Volume Based License (VBL)

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

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 Consulting Partner Private Offers (CPPO) comes with a volume-based license.

The list of SKUs available on the AWS Marketplace through the Cloud Professional Partner Organization (CPPO) are:

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

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

Volume Based License (VBL)

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

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

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

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

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUEPlus

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

Bundle Replacement Policy

Refer to the following notes:

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

Add-on Packages

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

Rules for add-on packages:

- Add-on packages can only to be added when there is an active base bundle available in GigaVUE-FM.
- The base bundle limits the total volume usage of the add-on package.
- If your add-on package has volume allowance less than the base bundle, then your add-on package can only handle volume allocated for add-on package.
- When the life term of an add-on package extends beyond the base bundle, then when the base bundle expires, the volume allowance of the add-on package will be reduced to zero until a new base bundle is added.

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

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

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

How GigaVUE-FM Tracks Volume-Based License Usage

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

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

For releases prior to 6.4:

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

Manage Volume-based Licenses

To manage active Volume-based License:

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

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

Field	Description
SKUs	Unique identifier associated with the license
Bundles	Bundle to which the license belongs to
Volume	Total daily allowance volume
Starts	License start date
Ends	License end date
Type	Type of license (Commercial, Trial, Lab and other license types).
Activation ID	Activation ID
Entitlement ID	Entitlement ID

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

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

Field	Description
SKUs	Unique identifier associated with the license.
Bundles	Bundle to which the license belongs to.
Ends	License end date
Grace Period	Number of days the license is in grace period
Deactivation Date	Date the license got deactivated.
Revocation Code	License revocation code.
Status	License status.

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

Use the following buttons to manage your VBL.

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

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

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

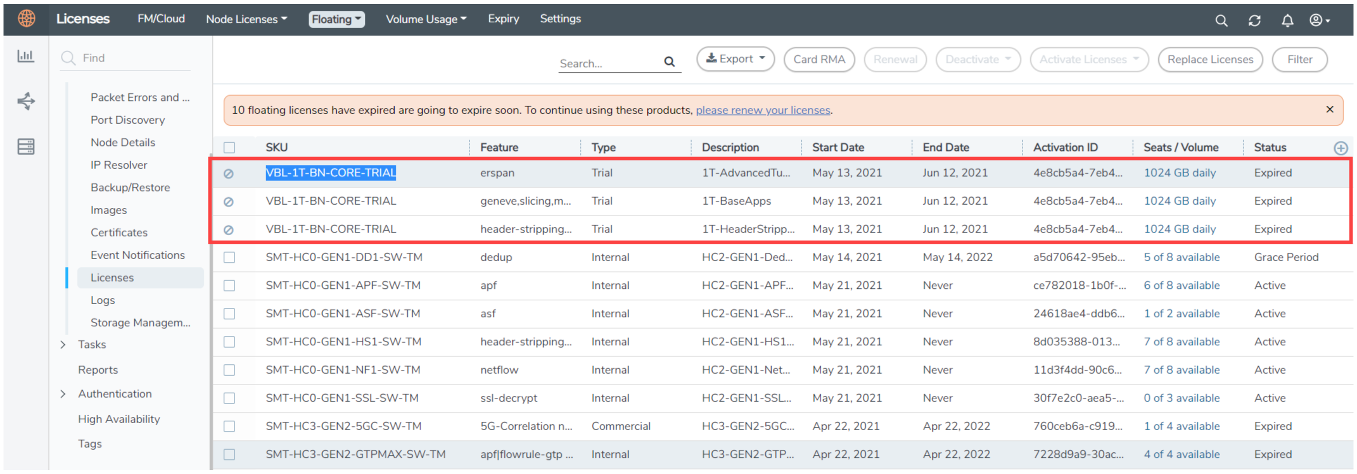
Activate Volume-based Licenses

To activate Volume-based licenses:

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

Default Trial Licenses

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



10 floating licenses have expired are going to expire soon. To continue using these products, please renew your licenses.

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

This license includes the following applications:

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

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

To deactivate the trial VBL refer to Delete Default Trial Licenses section for details.

Delete Default Trial Licenses

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

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

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

Prerequisites

Refer to the following topics for details:

- Subscribe to GigaVUE Cloud Suite Components
- AWS Security Credentials
- Amazon VPC
- Connect GigaVUE-FM to AWS
- Default Login Credentials

Subscribe to GigaVUE Cloud Suite Components

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

- GigaVUE V Series Node
- GigaVUE V Series Proxy
- GigaVUE V Series Controller
- GigaVUE-FM BYOL.

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

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 GigaVUE Cloud Suite version link from the list for Gigamon products.
5. Click **Continue to Subscribe**.

AWS Security Credentials

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

You need one of the following security credentials:

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

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

Amazon VPC

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

NOTE: To create a VPC, refer to Create a VPC topic in the AWS Documentation.

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

Subnet for VPC

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

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

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

Security Group

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

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

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

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
Inbound	● HTTPS ● SSH	TCP	● 443 ● 22	Administrator Subnet	Management connection to GigaVUE-FM
Inbound	Custom TCP Rule	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE V Series Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation UCT-V to send statistics to GigaVUE-FM
Outbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series node
UCT-V Controller					
Inbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with GigaVUE-FM
Inbound (This is the port used for Third Party Orchestration)	Custom TCP Rule	TCP(6)	8891	UCT-V or Subnet IP	Allows UCT-V Controller to communicate registration requests from UCT-V and forward the same to GigaVUE-FM
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
Outbound	Custom TCP Rule	TCP(6)	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate with UCT-Vs
UCT-V					
Inbound	Custom TCP Rule	TCP(6)	9901	UCT-V Controller IP	Allows UCT-Vs to communicate with UCT-V Controller
Outbound (This is the port used for Third Party	Custom TCP Rule	TCP(6)	8891	UCT-V or Subnet IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat

Direction	Type	Protocol	Port	CIDR	Purpose
Orchestration)					
Outbound	- UDP - IP	- UDP (VXLAN) - IP Protocol (L2GRE)	VXLAN (default 4789)	UCT-V or Subnet IP	Allows UCT-Vs to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Outbound	Custom TCP Rule	TCP	11443	UCT-V subnet	Allows UCT-V to securely transfer the traffic toGigaVUE V Series Node
GigaVUE V Series Proxy (optional)					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows V Series Proxy to communicate with V Series node
GigaVUE V Series Node					
Inbound	Custom TCP Rule	TCP	8889	- GigaVUE-FM IP - V Series Proxy IP	Allows V Series Proxy or GigaVUE-FM to communicate with V Series node
Inbound	- UDP - IP	- UDP (VXLAN) - IP Protocol (L2GRE)	- VXLAN (default 4789) - L2GRE	UCT-V or Subnet IP	Allows UCT-Vs to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM

Direction	Type	Protocol	Port	CIDR	Purpose
Outbound	Custom UDP Rule	● UDP (VXLAN) ● IP Protocol (L2GRE)	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound (optional)	ICMP	ICMP	● echo request ● echo reply	Tool IP	Allows V Series node to health check tunnel destination traffic
Bi-directional	Custom TCP Rule	TCP	11443	GigaVUE V Series Node subnet	Allows to securely transfer the traffic in between GigaVUE V Series Nodes.

Key Pair

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

To create a key pair, refer to Create a key pair using Amazon EC2 topic in the AWS Documentation.

Default Login Credentials

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

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

Points to Note

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

- It is recommended to deploy the GigaVUE-FM on the AWS to manage AWS workload.
- If the GigaVUE-FM is deployed outside of the AWS, then the GigaVUE-FM encrypts and stores the access key and the secret key in its database.
- Always attach an IAM role to the instance running GigaVUE-FM in AWS to connect it to your AWS account.
- If you are launching the GigaVUE-FM instance from the AWS Marketplace, you need to have only the IAM roles.
- Deployment of GigaVUE fabric components through a third-party orchestrator is supported on Linux and Windows platforms. Refer to Linux UCT-V Installation and Windows UCT-V Installation for detailed information.
- Fragmentation in the network should be avoided from UCT-V to GigaVUE V Series node and from GigaVUE V Series 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 fragments the packets. This results in packet loss, that is, all fragments over 200 packet per second gets dropped by ENA (Elastic Network Adapter) of AWS.

Deploy GigaVUE Cloud Suite for AWS

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

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

Refer to the following sections for details:

- Use Cases - Gigamon Validated Design
- Examples- Permissions
- Install GigaVUE-FM on AWS
- Create a Monitoring Domain
- Configure GigaVUE Fabric Components in GigaVUE-FM
- Configure Role-Based Access for Third Party Orchestration
- Configure GigaVUE Fabric Components in AWS
- Install UCT-V

Use Cases - Gigamon Validated Design

Gigamon Validated Designs (GVDs) are lab tested solutions that are intended to cater to network and security architects and/or administrators who would like to gain more insights and understand how these solutions can be deployed in their environments.

Each design provides:

- Design Overview
- Deployment Steps
- Verification Steps
- Validation Environment

It is recommended that you review the topic completely before starting the deployment steps.

Deploying GigaVUE Cloud Suite Across Multiple Accounts on AWS Cloud

Gigamon Cloud Suite has the Deep Visibility advantage that provides in-depth visibility data to the security and analytic tools from multiple Cloud accounts. By leveraging Gigamon Cloud Suite, you can reduce the operations cost and administrative overhead required to maintain separate tools for each account and also receive holistic insight into the data which is crucial especially in security installations.

Refer to the Gigamon Validated Design to see how GigaVUE-FM manages visibility across multiple AWS accounts by sharing Gigamon fabric nodes between them for obtaining visibility on the Cloud.

To learn more about this solution, read complete details on the Gigamon Community: Deploying GigaVUE Cloud Suite Across Multiple Accounts On AWS Cloud 5.16

AWS VPC Mirroring with Application Filter Intelligence and Slicing

The GigaVUE Cloud Suite supports VPC mirroring. GigaVUE Cloud Suite can now help you extend your security posture to AWS. With VPC mirroring, GigaVUE Cloud Suite can be configured to acquire mirrored traffic from AWS instances, optimize the traffic, and then distribute it to the relevant tools thereby improving the security in the AWS environment.

To learn more about this solution, read complete details on the Gigamon Community: AWS VPC Mirroring with Application Filter Intelligence and Slicing

Gigamon Precryption™ with Secure Tunnel to Gain Visibility into the Cloud (AWS) Environment

To achieve the goal of inspecting the encrypted traffic, Gigamon Precryption™ technology delivers plain text visibility of encrypted communications to the full security stack, without the traditional cost and complexity of decryption and thus redefines security for virtual, cloud, and containerized applications. To further secure the precrypted data flow from user workload to the Gigamon fabric, Gigamon has introduced secure tunnels feature that enables secure delivery of the precrypted data.

This GVD focuses on deploying the Gigamon cloud suite with Precryption™ and Secure Tunnel in AWS. It aims to deliver plain text visibility into encrypted traffic, secure the plain text traffic during transit from user workloads to Gigamon fabric, and subsequently forward it to the tools in an out-of-band fashion.

To learn more about this solution, read complete details on the Gigamon Community: Gigamon Precryption™ with Secure Tunnel to Gain Visibility into the Cloud (AWS) Environment

Examples- Permissions

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 FM instance running in AWS. If the FM is running outside the AWS, then you must use the access keys and secret keys.

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

- GigaVUE-FM Instance Multi Account Support Using Amazon STS
- Example: Traffic Acquisition using the UCT-V
- Example: Traffic Acquisition using the Customer Orchestrated Source
- Example: Traffic Acquisition using the Customer Orchestrated Source with GwLB
- Example: Traffic Acquisition using the Customer Orchestrated Source with NwLB
- Example: Traffic Acquisition using VPC Mirroring
- Example: Traffic Acquisition using VPC Mirroring with Network Load Balancer
- Example: Traffic Acquisition using VPC Mirroring and GwLB

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 IAM instance role for authentication:

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

   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"
   ```

   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.

Example: Traffic Acquisition using the UCT-V

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:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "ec2:RebootInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "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.

Example: Traffic Acquisition using the Customer Orchestrated Source

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: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",
                "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.

Example: Traffic Acquisition using the Customer Orchestrated Source with GwLB

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: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",
        "ram:CreateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:GetResourceShareInvitations",
        "ram:AcceptResourceShareInvitation",
        "ram:DisassociateResourceShare",
        "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.

Example: Traffic Acquisition using the Customer Orchestrated Source with NwLB

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:DescribeAddresses",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "ram:CreateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:GetResourceShareInvitations",
        "ram:AcceptResourceShareInvitation",
        "ram:DisassociateResourceShare",
        "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.

Example: Traffic Acquisition using VPC Mirroring

These are the minimum permissions that are required to acquire traffic using VPC 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: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",
                "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.

Example: Traffic Acquisition using VPC Mirroring with Network Load Balancer

These are the minimum permissions that are required to acquire traffic using VPC 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",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeInstances",
                "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",
                "ram:DeleteResourceShare",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",

                "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.

Example: Traffic Acquisition using VPC Mirroring and GwLB

This policy allows you to acquire traffic using VPC 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:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:CreateTrafficMirrorFilterRule",
                "ec2:CreateTrafficMirrorTarget",
                "ec2:CreateTrafficMirrorSession",
                "ec2:CreateTrafficMirrorFilter",
                "ec2:DeleteTrafficMirrorTarget",
                "ec2:DeleteTrafficMirrorSession",
                "ec2:DeleteTrafficMirrorFilter",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpoints",
                "ram:CreateResourceShare",
                "ram:DeleteResourceShare",
                "ram:GetResourceShareInvitations",
                "ram:AcceptResourceShareInvitation",
                "ram:DisassociateResourceShare",
                "ram:DeleteResourceShare",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "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.

Install GigaVUE-FM on AWS

You can launch GigaVUE-FM in AWS by subscribing it in the marketplace. For more information, see Launch GigaVUE-FM using CFT

Subscribe GigaVUE Products

You can deploy the GigaVUE Cloud Suite for AWS from the AWS Marketplace. The following GigaVUE Cloud Suite products are listed in the AWS Marketplace:

- GigaVUE V Series Node
- GigaVUE V Series Controller
- GigaVUE-FM

To subscribe to the GigaVUE products, 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 GigaVUE Cloud Suite version link from the list for Gigamon products.
5. Click **Continue to Subscribe**. The **Subscribe to this software** page is displayed, where the complete detail about the product is described.
6. Click **Continue to Configuration**. The **Configure this software** page is displayed.
7. In the Configure this software page, select the following:
    a. From the **Fulfillment option** drop-down list, select **Auto Deploy GigaVUE-FM using AWS CFT**.
    b. From the **Software version** drop-down list, select the latest version.
    c. From the **Region** drop-down list, select the appropriate region.
    d. Click **Continue to Launch**. The **Launch this Software** page is displayed.
8. In the Launch this Software page, from the **Choose Action** drop-down, select **Launch CloudFormation**.
9. Click **Launch**. The **Create Stack** page is displayed.

Related links:

Initial GigaVUE-FM Configuration

Initial GigaVUE-FM 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 launch GigaVUE-FM instance and expand the page in the **Descriptions** tab to view the instance information.
2. Copy and paste the Public IP address into a new browser window or tab.
3. Copy the Instance ID from the **Descriptions** tab.

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)**.

> 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.

Related links

Create a Monitoring Domain

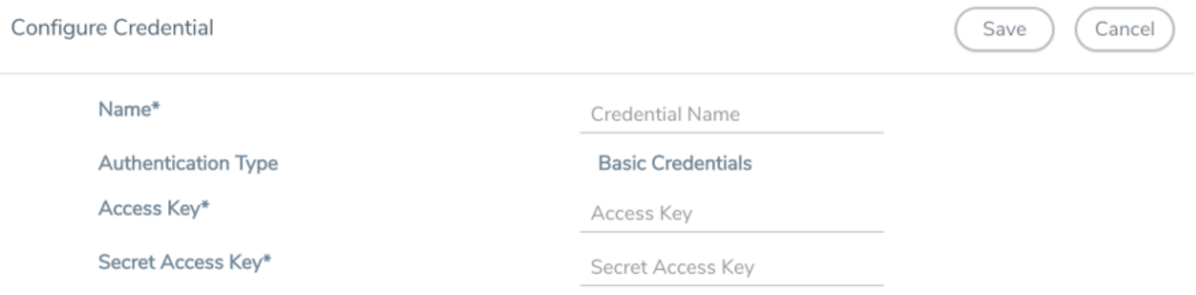
Create AWS Credentials

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 AWS 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 then you must add these to the GigaVUE-FM in the AWS Settings page, or in the Monitoring Domain creation page.

To create AWS credentials:

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



Configure Credential

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

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

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

4. Click **Save**. You can view the list of available credentials in the AWS Credential page.

Required Policies and Permissions

To add multiple AWS accounts in a monitoring domain, you must add the access and role name of all the additional accounts to your STS policy. Following is a sample STS policy where the *account2* and *account3* are the accesses added to the existing *account1* policy.

```
{
    "Version": "2012-10-17",
    "Statement": {
       "Effect": "Allow",
       "Action": "sts:*",
       "Resource": [
          "arn:aws:iam::account2:role/ROLE-NAME"
          "arn:aws:iam::account3:role/ROLE-NAME"
                   ]
                 }
}
```

For detailed information on the policies attached to GigaVUE-FM, refer to Examples-Permissions.

Following is the required IAM policy to exist in your remote networks:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Action": [
           "ec2:CreateTags",
           "ec2:DeleteTags",
           "ec2:Describe*",
           "ec2:*TrafficMirror*",
           "ram:GetResourceShareInvitations"
           ],

       "Resource": "*"
       "Effect": "Allow",
        }
               ]
}
```

Following is the required trust policy to set in your remote account:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Effect": "Allow",
           "Principal": {
               "Service": "ec2.amazonaws.com",
               "AWS": "arn:aws:iam::account:role/ROLE-NAME"
                       },
           "Action": "sts:AssumeRole"
         }
                ]
}
```

Install Custom Certificate

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

You can upload the custom certificate in two ways:

- Upload Custom Certificates using GigaVUE-FM
- Upload Custom Certificate using Third Party Orchestration

Upload Custom Certificates using GigaVUE-FM

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

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

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

4. Click **Save**.

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

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

Upload Custom Certificate using Third Party Orchestration

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

For integrated mode:

- Configure GigaVUE Fabric Components in AWS

For generic mode:

- Configure GigaVUE Fabric Components in AWS

Adding Certificate Authority

CA List

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

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

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

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

4. Click **Save**.

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 Cloud Suite for AWS 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 **Physical Device Infrastructure Management** category.

To create a Monitoring Domain:

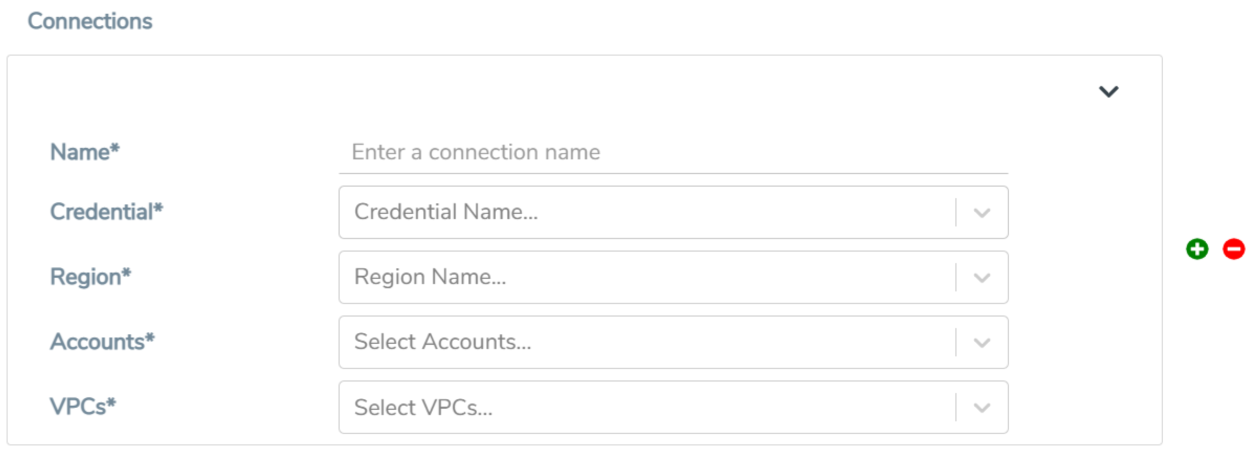
1. Go to **Inventory > VIRTUAL > AWS** , and then click **Monitoring Domain**.
2. On the Monitoring Domain page, click the **New** button. The Monitoring Domain

Configuration page appears.

3. Click **Check Permissions** and validate whether you have the required permissions.

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

Field	Action
Monitoring Domain	An alias used to identify the monitoring domain.
Use V Series 2	Select **Yes** to configure GigaVUE V Series 2 node.
Traffic Acquisition Method	Select a tapping method. The available options are: ▪ **UCT-V**: UCT-Vs are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series nodes. If you select UCT-V as the tapping method, you must configure the UCT-V Controller to communicate to the UCT-Vs from GigaVUE-FM. You can also configure the UCT-V Controller and UCT-Vs from your own orchestrator. Refer to Configure GigaVUE Fabric Components using AWS Orchestrator for detailed information. ▪ **VPC Traffic Mirroring**: If you select the VPC Traffic Mirroring option, the mirrored traffic from your workloads is directed directly to the GigaVUE V Series nodes, and you need not configure the UCT-Vs and UCT-V Controllers. For more information on VPC Peering, refer to VPC peering connections in the AWS Documentation. Peering is required to send mirrored traffic from other VPCs into a centralized GigaVUE V Series deployment. You can choose to use an external load balancer for VPC Traffic Mirroring. Select **Yes** to use load balancer. Refer to Configure an External Load Balancer for detailed information. • UCT-V Controller configuration is not applicable for VPC Traffic Mirroring. • VPC mirroring does not support cross-account solutions without a load balancer. • For VPC Traffic Mirroring option, additional permissions are required. Refer to the Permissions 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 use select **Customer Orchestrated Source** as the tapping method, you can use the Customer Orchestrated Source as a source option in the monitoring session, where the traffic is directly tunneled to the GigaVUE V Series nodes without deploying UCT-Vs and UCT-V Controllers. The user is responsible for creating this tunnel feed and pointing it to the GigaVUE V Series node(s). **NOTE:** When using Observability Gateway (AMX) application, select the **Traffic Acquisition Method** as **Customer Orchestrated Source**.
Traffic Acquisition Tunnel MTU	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. The UCT-V tunnel MTU should be 50 bytes less than the agent's destination interface MTU size.

Field	Action
Use FM to Launch Fabric	Select **Yes** to Configure GigaVUE Fabric Components in GigaVUE-FM or select **No** to Configure GigaVUE Fabric Components in AWS.
Connections  Connections Name* Enter a connection name Credential* Credential Name... Region* Region Name... Accounts* Select Accounts... VPCs* Select VPCs... **NOTE:** You can add multiple connections in a monitoring domain. Refer to Create AWS Credentials for more information on adding multiple AWS **Basic Credentials**.	
Name	An alias used to identify the connection.
Credential	Select an AWS credential. For detailed information, refer to Create AWS Credentials.
Region	AWS region for the monitoring domain. For example, US West.
Accounts	Select the AWS accounts
VPCs	Select the VPCs to monitor

5. Click **Save**. The **AWS Fabric Launch Configuration** page appears.

Related links:

Configure GigaVUE Fabric Components in GigaVUE-FM

Managing Monitoring Domain

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

- Monitoring Domain
- Connections Domain
- Connections Domain
- UCT-Vs

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

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

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

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

Monitoring Domain

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

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

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

Use the following buttons to manage your Monitoring Domain:

Button	Description
New	Use to create new connection
Actions	You can select a monitoring domain and then perform the following options: ● **Edit Monitoring Domain**- Select a monitoring domain and then click **Edit Monitoring domain** to update the configuration. ● **Delete Domain** - You can select a monitoring domain or multiple monitoring domains to delete them. ● **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 fabrics ● **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. ● **Delete Fabric**- You can delete all the fabrics associated with the monitoring domain of the selected Fabric. ● **Edit SSL Configuration** - You can use this option to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Filter	Filters the monitoring domain based on the list view options that are configured: ● **Tunnel MTU** ● **Acquisition Method** ● **Centralised Connection** ● **Management Subnet** 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.

Connections Domain

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

The list view shows the following details:

- Connections
- Monitoring Domain
- Status
- Fabric Nodes
- User Name
- Region

Fabric

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

The list view shows the following details:

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

UCT-Vs

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

The list view shows the following details:

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

.

Traffic Acquisition Methods

This section provides a 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 three 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. For information on the prerequisites and work flow refer the following topics:

- Traffic Acquisition Method as UCT-V
- Traffic Acquisition Method as VPC Mirroring
- Traffic Acquisition Method as Customer Orchestrated Source

Traffic Acquisition Method using UCT-V

This lightweight agent is 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. To acquire traffic using UCT-V, perform the following steps:

1. Install GigaVUE-FM on AWS.
2. Install UCT-V Agents
3. Create a Monitoring Domain.
    a. Select UCT-V as the Traffic Acquisition Method.
4. Configure GigaVUE Fabric Components.
5. Create and configure a Monitoring Session

Traffic Acquisition Method using VPC Mirroring

If you select the VPC Traffic Mirroring option, the mirrored traffic from your workloads is directed directly to the GigaVUE V Series nodes, and you need not configure the UCT-Vs and UCT-V Controller.

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

You can choose to use the AWS Network load balancer for a VPC Traffic Mirroring destination. Select **Yes** to use load balancer. Refer to Configure an External Load Balancer for detailed information.

To acquire traffic using VPC mirroring, perform the following steps:

1. Install GigaVUE-FM on AWS.
2. Create a Monitoring Domain.
    a. Select VPC Mirroring as the Traffic Acquisition Method.

       You can configure a prefilter and determine the VPC endpoint traffic that is mirrored. For more information on prefiltering, see Configure a Traffic Pre-filter.

> - UCT-V Controller configuration is not applicable for VPC Traffic Mirroring.
> - VPC mirroring does not support cross-account solutions without a load balancer.
> - For VPC Traffic Mirroring option, additional permissions are required. Refer to the Permissions 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.

3. Configure and Deploy GigaVUE Fabric Components in GigaVUE-FM
4. Create and configure a Monitoring Session

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

- AWS VPC Mirroring with Application Filter Intelligence and Slicing (6.3)

Traffic Acquisition Method using Customer Orchestrated Source

If you use select **Customer Orchestrated Source** as the tapping method, you can use the Customer Orchestrated Source as a source option in the monitoring session, where the traffic is directly tunneled to the GigaVUE V Series nodes without deploying UCT-Vs and UCT-V Controller. You must create this tunnel feed and point it to the GigaVUE V Series node (s). To acquire traffic using **Customer Orchestrated Source**, perform the following steps:

1. Install GigaVUE-FM on AWS.
2. Create a Monitoring Domain.
   a. Select **Customer Orchestrated Source** as the Traffic Acquisition Method.
3. Configure GigaVUE Fabric Components.
4. Create and configure a Monitoring Session

Configure GigaVUE Fabric Components in GigaVUE-FM

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

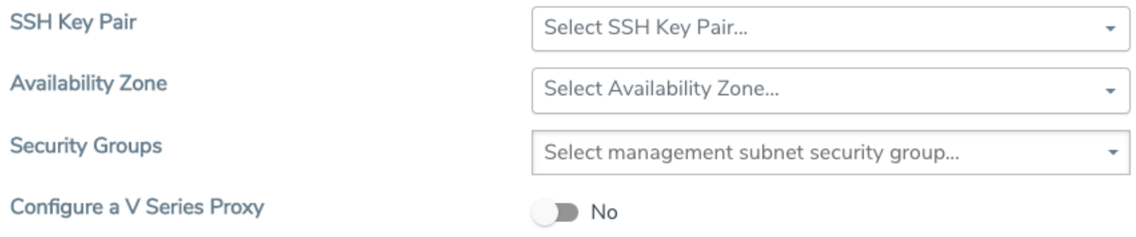
- Configure UCT-V Controller
- Configure GigaVUE V Series Proxy
- Configure GigaVUE V Series Node

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

Fields	Description
SSH Key Pair	The SSH key pair for the UCT-V Controller. For more information about SSH key pair, refer to Key Pairs.
Availability Zone	The distinct locations (zones) of the AWS region.

Fields	Description
Security Groups	The security group created for the UCT-V Controller. For more information, refer to Prerequisites.
Prefer IPv6	Enables IPv6 to deploy all the Fabric Controllers, and the tunnel between hypervisor to V Series node using IPv6 address. If the IPv6 address is unavailable, it uses an IPv4 address. This functionality is supported only in OVS Mirroring.
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs. **NOTE:** If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate.

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



SSH Key Pair: Select SSH Key Pair...

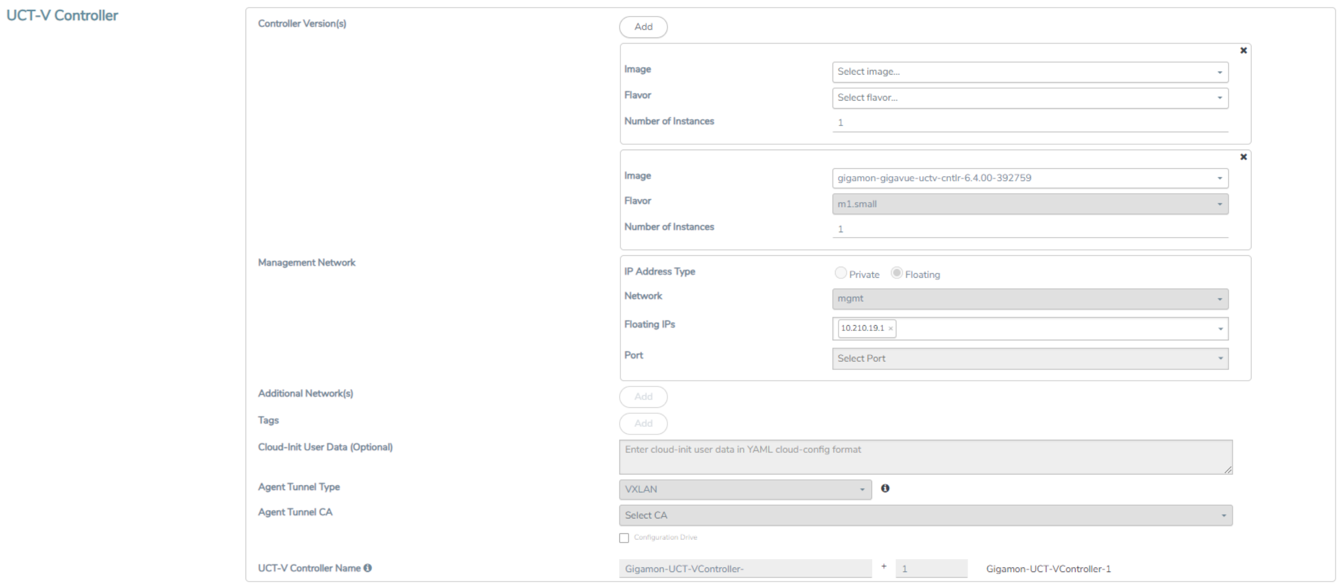
Availability Zone: Select Availability Zone...

Security Groups: Select management subnet security group...

Configure a V Series Proxy: No

Configure UCT-V Controller

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



UCT-V Controller

Controller Version(s) — Add

Image: Select image...
Flavor: Select flavor...
Number of Instances: 1

Image: gigamon-gigavue-uctv-cntlr-6.4.00-392759
Flavor: m1.small
Number of Instances: 1

Management Network
IP Address Type: ○ Private ● Floating
Network: mgmt
Floating IPs: 10.210.19.1
Port: Select Port

Additional Network(s) — Add

Tags — Add

Cloud-Init User Data (Optional): Enter cloud-init user data in YAML cloud-config format

Agent Tunnel Type: VXLAN

Agent Tunnel CA: Select CA

□ Configuration Drive

UCT-V Controller Name: Gigamon-UCT-VController- + 1 Gigamon-UCT-VController-1

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

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

Fields	Description
Controller Version(s)	The UCT-V Controller version that you configure must always have the same version number as the UCT-Vs deployed in the instances. For more detailed information refer GigaVUE-FM Version Compatibility Matrix. **NOTE:** If there is a version mismatch between the UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the agents in the instances. To add UCT-V Controllers: **a.** Under **Controller Versions**, click **Add**. **b.** From the **Image** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances. **c.** From the **Flavor** drop-down list, select a size for the UCT-V Controller. **d.** In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.
Management	This segment defines the management network that GigaVUE-FM

Fields	Description
Network	uses to communicate with UCT-V Controllers, GigaVUE V Series Proxy, and GigaVUE V Series Nodes. **Network** - Select the management network ID. **Ports** - Select a port, you can choose a port related to the selected management network ID. **IP Address Type** The type of IP address GigaVUE-FM needs to communicate with UCT-V Controllers: o **Private**—A private IP can be used when GigaVUE-FM, the UCT-V Controller, or the GigaVUE V Series Proxy reside inside the same project. o **Floating**—A floating IP is needed only if GigaVUE-FM is not in the same project in the cloud or is outside the cloud. GigaVUE-FM needs a floating IP to communicate with the controllers from an external network.
Additional Network(s)	(Optional) If there are UCT-Vs on networks that are not IP routable from the management network, additional networks or subnets must be specified so that the UCT-V Controller can communicate with all the UCT-Vs. Click **Add** to specify additional networks (subnets), if needed. Also, make sure that you specify a list of security groups for each additional network. **Ports**: Select a port associated with the network.
Tag(s)	(Optional) The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-uctv-controllers. There is a specific UCT-V Controller Version for OVS Mirroring and OVS Mirroring + DPDK. To add a tag: a. Click **Add**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-uctv-controllers.
Cloud-Init User Data (Optional)	Enter the cloud-init user data in cloud-config format.

Fields	Description
Agent Tunnel Type	The type of tunnel used for sending the traffic from UCT-Vs to GigaVUE V Series nodes. The options are GRE, VXLAN, and Secure tunnels (TLS-PCAPNG).
Agent Tunnel CA	The Certificate Authority (CA) that should be used in the UCT-V Controller for connecting the tunnel.
UCT-V Controller Name	(Optional) Enter the name of the UCT-V Controller. The UCT-V Controller name must meet the following criteria: o The entire name can be a minimum of 1 to a maximum of 128 characters. o The suffix must only be a numeral and it should range between 0 to 999999999. o When deploying multiple UCT-V Controllers, the suffix of the consecutive UCT-V Controller name is updated successively. E.g., 000, 001, 002, 003, etc..

Configure GigaVUE V Series Proxy

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

Configure GigaVUE V Series Node

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

Parameter	Description
Image	Select the GigaVUE V Series node AMI.
Flavor	Select the instance type of the GigaVUE V Series node. By default, C5n.large is selected.
Management Network	For the GigaVUE V Series Node, the Management Network is what is used by the GigaVUE V Series Proxy to communicate with the GigaVUE V Series Nodes. Select the management network ID. **Ports**— Select a port, you can choose a port related to the selected management network ID.
Data Network	Click **Add** to add additional networks. This is the network that the GigaVUE V Series node uses to tunnel the captured traffic to the monitoring tools. Multiple networks are supported. • **Tool Subnet**—Select a tool subnet, this is the default subnet that the GigaVUE-FM use to egress traffic to your tools. This subnet must have proper connectivity to your endpoint. • **Network 1**—Select a network type.

Parameter	Description
Tag(s)	(Optional) The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-uctv-controllers. To add a tag: a. Click **Add**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-uctv-controllers.
Cloud-Init User Data (Optional)	Enter the cloud-init user data in cloud-config format.
Min Instances	The minimum number of GigaVUE V Series nodes to be launched in AWS. The minimum number is 1. ● When you deploy a UCT-V based monitoring session, the V Series nodes will automatically be deployed based on the # of VMs being monitored and the instance per V Series node ratio defined in the AWS Setttings page. The ratio defined in Number of UCT-V agents per node. **NOTE:** GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.
Max Instances	The maximum number of GigaVUE V Series nodes that can be launched in AWS.
Tunnel MTU (Maximum Transmission Unit)	The Maximum Transmission Unit (MTU) is applied on the outgoing tunnel endpoints of the GigaVUE-FM V Series node when a monitoring session is deployed. The default value is 1450. The value must be 42 bytes less than the default MTU for GRE tunneling, or 50 bytes less than default MTU for VXLAN tunnels.

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

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

Configure Role-Based Access for Third Party Orchestration

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

Users

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

Add Users

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

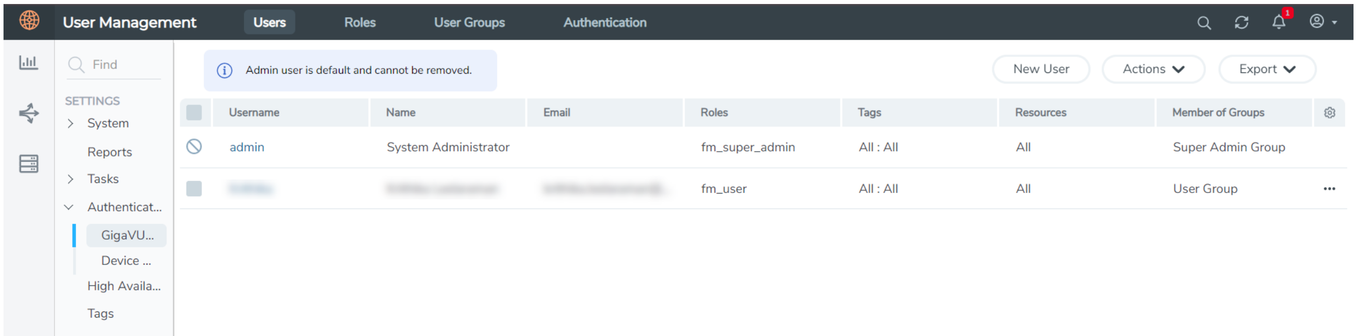
IMPORTANT: It is recommended to create users through GigaVUE-FM:

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

> **NOTE:** Monitor and operator users are not available in GigaVUE-FM. However, if you upgrade from a previous version in which monitor/operator users have been mapped in map default user, then after upgrade:
>
> - **In AAA:** Users authenticated through the external servers will be assigned the fm_user role.
> - **In LDAP:** Remote group based DN entry will not be migrated.

To add users perform the following steps:

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

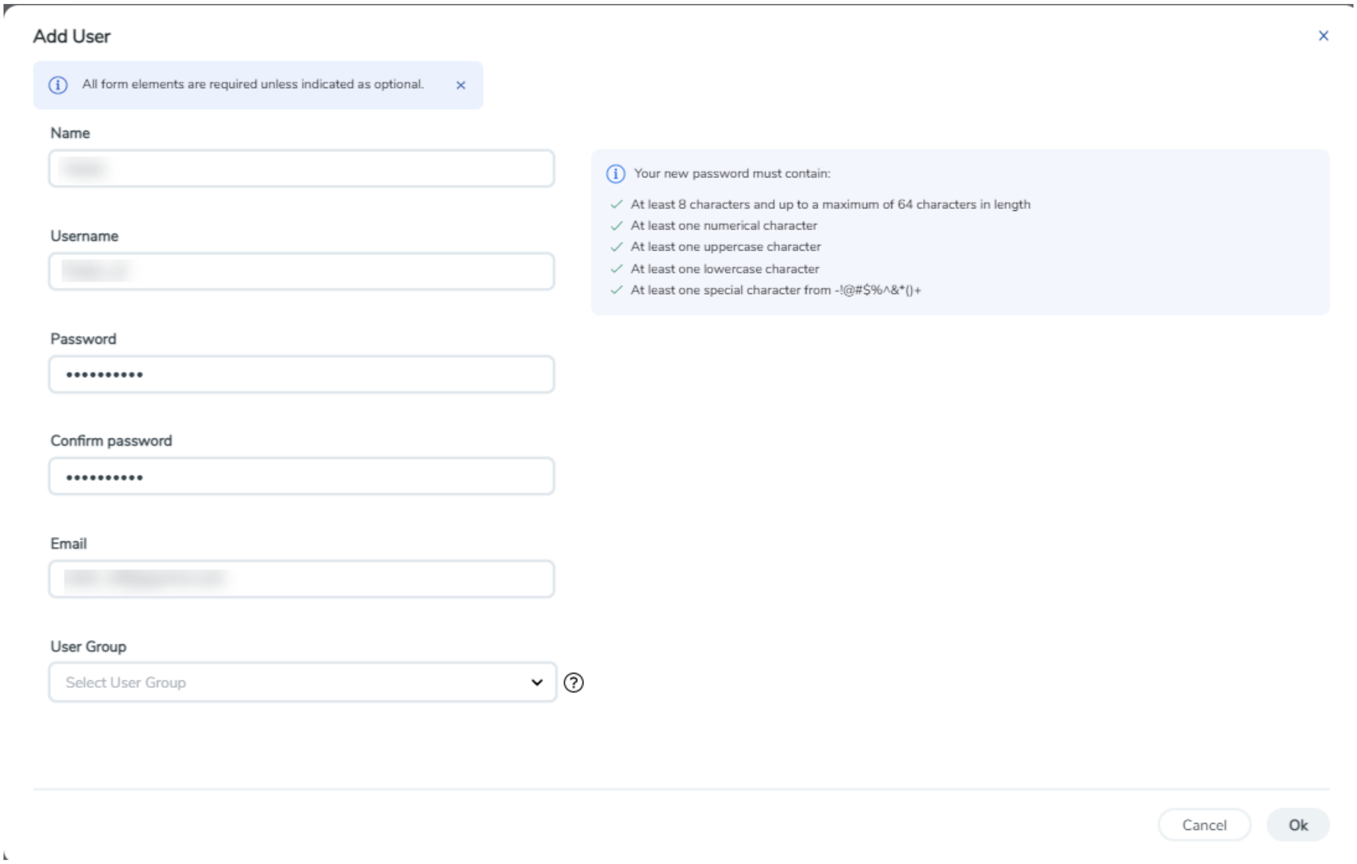


Admin user is default and cannot be removed.

Username	Name	Email	Roles	Tags	Resources	Member of Groups
admin	System Administrator		fm_super_admin	All : All	All	Super Admin Group
[redacted]	[redacted]	[redacted]	fm_user	All : All	All	User Group

Figure 1 *FM Users Page*

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



Add User ×

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

Name

[redacted]

Username

[redacted]

Password

••••••••••

Confirm password

••••••••••

Email

[redacted]

User Group

Select User Group ⌄ ?

ⓘ Your new password must contain:

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

Cancel Ok

Figure 2 *Create User*

a. In the Add User pop-up box, enter the following details:

- **Name:** Actual name of the user
- **Username**: User name configured in GigaVUE-FM
- **Email**: Email ID of the user
- **Password/Confirm Password**: Password for the user. Refer to the Change Your Password section.
- **User Group:** User group

NOTE: GigaVUE-FM will prompt for your password.

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

The new user is added to the summary list view.

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

- Create Roles
- Create Groups.

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

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

How to Unlock User Account

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

To unlock:

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

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

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

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

Create Roles

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

Create Roles

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

GigaVUE-FM has the following default roles:

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

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

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

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

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

Category	Associated Resources
All	Manages all resources ● A user with fm_super_admin role has both read and write access to all the resource categories. ● A user with fm_user role has only read access to all the resource categories.
Infrastructure Management	Manages resources such as devices, cards, ports and cloud resources. You can add or delete a device in GigaVUE-FM, enable or disable cards, modify port parameters, set leaf-spine topology. The following resources belong to this category: ● **Physical resources:** Chassis, slots, cards ports, port groups, port pairs, cluster config, nodes and so on ● **GigaVUE-FM inventory resources:** Nodes, node credentials ● **Device backup/restore:** Device and cluster configuration ● **Device license configuration:** Device/cluster licensing ● **Statistics:** Device, port ● **Tags**: Events, historical trending ● **Device security**: SystemTime, System EventNotification, SystemLocalUser, System Security Policy Settings, AAA Authentication Settings,Device User Roles, LDAP Servers, RADIUS Servers, TACACS+ Servers ● **Device maintenance**: Sys Dump, Syslog ● **Cloud Infrastructure resources**: Cloud Connections, Cloud Proxy Server, Cloud Fabric Deployment, Cloud Configurations, Sys Dump, Syslog, Cloud licenses, Cloud Inventory. **NOTE:** Cloud APIs are also RBAC enabled.
Traffic Control Management	Manages inline resources, flow maps, GigaSMART applications, second level maps, map chains, map groups. The following

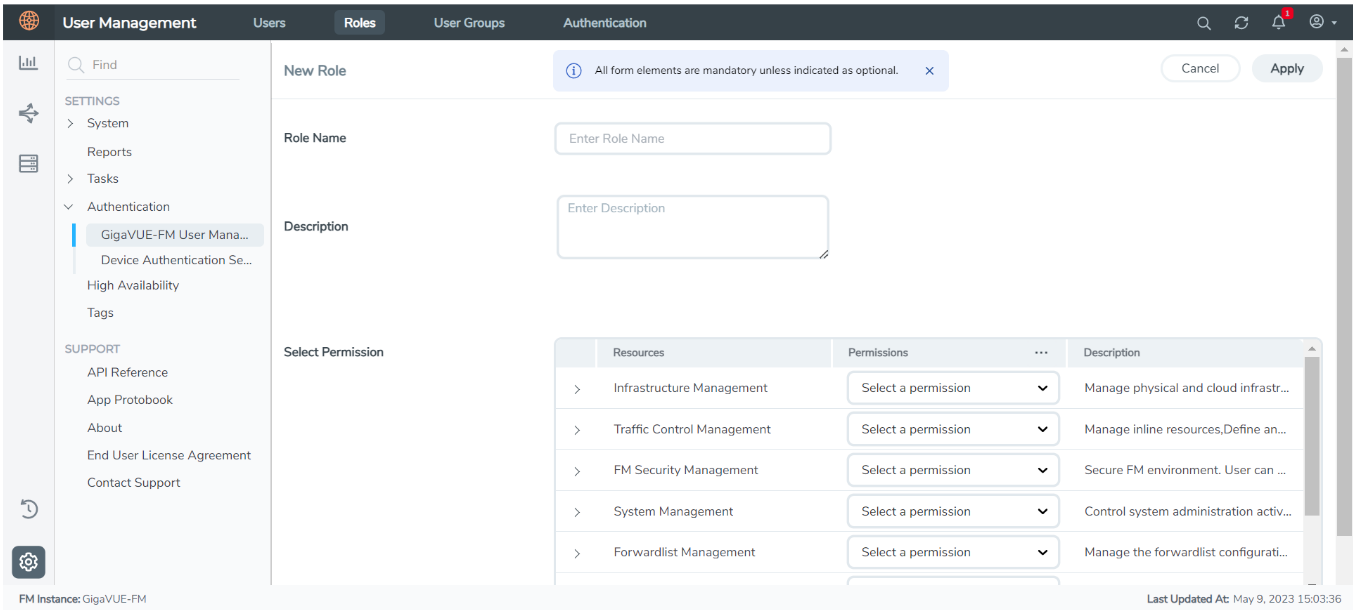
Category	Associated Resources
	resources belong to this category: ● **Infrastructure resources**: IP interfaces, circuit tunnels, tunnel endpoints, tunnel load balancing endpoints, ARP entries ● Intent Based Orchestration resources: Policies, rules ● **GigaSMART resources:** GigaSMART, GSgroups, vPorts, Netflow exporters ● **Map resources**: Fabric, fabric resources, flow maps, maps, map chains, map groups, map templates ● **Application intelligence resources**: Application visibility, Metadata, application filter resources ● **Tag**: Flow manipulation - Netflow operations, Statistics - device port ● Active visibility ● **Inline resources**: Inline networks, Inline network groups, Inline tools, Inline tool groups, Inline serial tools, Inline heartbeat profile ● **Cloud operation resources**: Monitoring session, stats, map library, tunnel library, tools library, inclusion/exclusion maps. **NOTE:** Cloud APIs are also RBAC enabled.
FM Security Management	Ensures secure GigaVUE-FM environment. Users in this category can manage user and roles, AAA services and other security operations.
System Management	Controls system administration activities of GigaVUE-FM. User in this category are allowed to perform operations such as backup/restore of GigaVUE-FM and devices, and upgrade of GigaVUE-FM. The following GigaVUE-FM resources belong to this category: ● Backup/restore ● Archive server ● License ● Storage management ● Image repo config ● Notification target/email
Forward list/CUPS Management	Manages the forward list configuration. The following resources belong to this category: ● GTP forward list ● SIP forward list
Third Party Orchestration	Used to deploy fabric components using external orchestrator.
Device Certificate Management	Manages device certificates.
Other Resource Management	Manages virtual and cloud resources

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

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

To create a role

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



New Role

All form elements are mandatory unless indicated as optional.

Role Name: Enter Role Name

Description: Enter Description

Select Permission

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

FM Instance: GigaVUE-FM

Last Updated At: May 9, 2023 15:03:36

3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: In the **Select Permission** table, select the required permission for the various resource categories.
4. Click **Apply** to save the configuration.

Create User Groups

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

Create User Groups

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

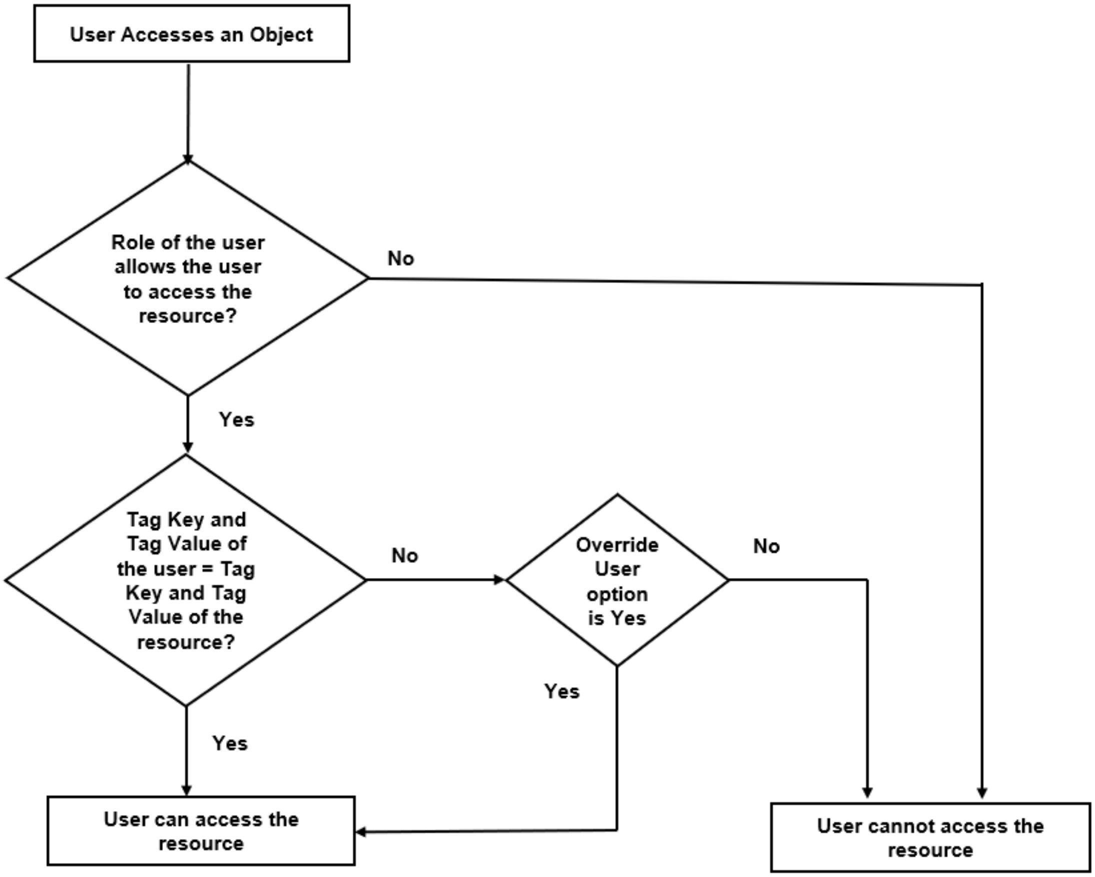
The following user groups are available by default in GigaVUE-FM. You will not be able to edit or change these groups in the system.

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

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

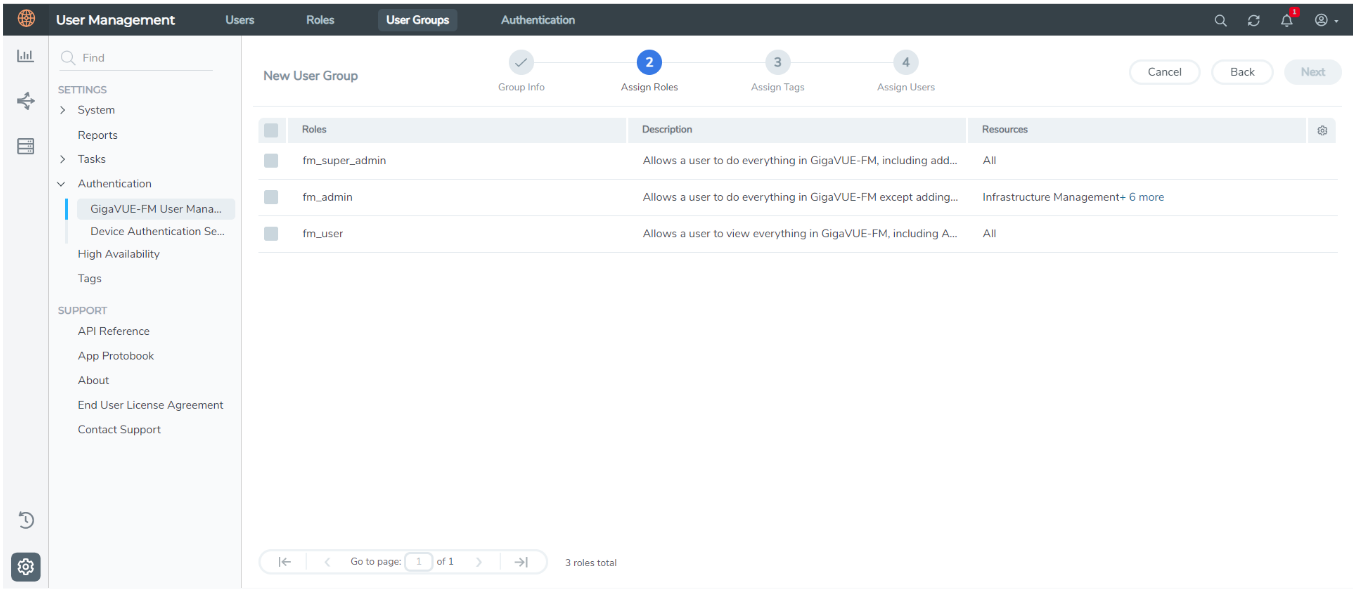
- The category of resources which the user can access, such as the clusters, ports, maps and so on. This is defined using the **Roles** option. Refer to the Roles section for more details.
- The physical and logical resources that the user can access, such as the ports in a cluster that belong to a specific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

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


User Accesses an Object
Role of the user allows the user to access the resource?
No
Yes
Tag Key and Tag Value of the user = Tag Key and Tag Value of the resource?
No
Override User option is Yes
No
Yes
Yes
User can access the resource
User cannot access the resource

To create a user group:

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



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

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

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

Click on the ellipses to perform the following operations:

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

Configure GigaVUE Fabric Components in AWS

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

You can also upload custom certificates to GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform when deploying the fabric components. Refer to Install Custom Certificate for more detailed information.

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

- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- You can use AWS as an Orchestrator for deploying GigaVUE fabric components only when using V Series 2 nodes.
- When using VPC 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 these interfaces when deploying the GigaVUE V Series Node in AWS. Refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation for more detailed information on how to add network interfaces when launching an instance.

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

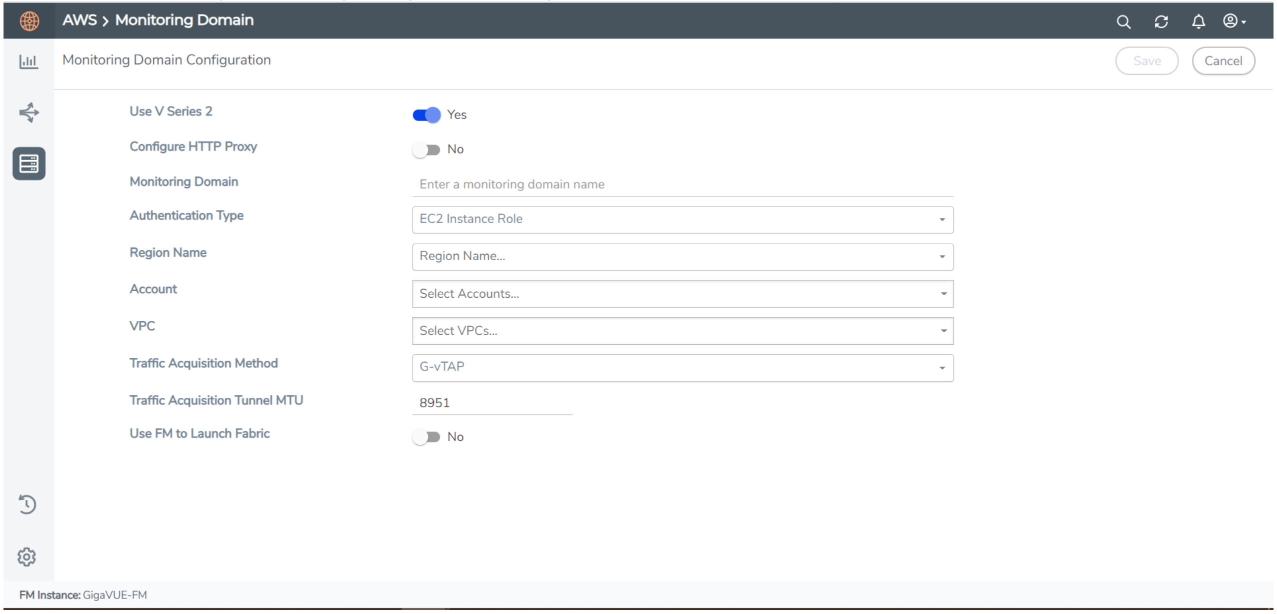
- Configure GigaVUE V Series Nodes and V Series Proxy in AWS
- Configure UCT-V Controller in AWS
- Configure UCT-V in AWS

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

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

1. Before configuring GigaVUE fabric components through AWS, you must create a monitoring domain in GigaVUE-FM. Refer to Create a Monitoring Domain for detailed instructions.

2. In the **Monitoring Domain Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you are going to configure the fabric components in AWS Orchestrator.



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

FM Instance: GigaVUE-FM

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

Register GigaVUE V Series Nodes or Proxy using User Data

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

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

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

<table>
<tr><th>Field</th><th>User Data</th></tr>
<tr><td>User data without custom certificate</td><td>

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <VPC Name>
        user: <Username>
        password: <Password>
        remoteIP: <IP address of the GigaVUE-FM> or <IP address of the Proxy>
        remotePort: 443
```

</td></tr>
<tr><td>User data with custom certificate</td><td>

```
#cloud-config
 write_files:
 - path: /etc/cntlr-cert.conf
   owner: root:root
   permissions: "0644"
   content: |
      -----BEGIN CERTIFICATE-----
      <certificate content>
      -----END CERTIFICATE-----
 - path: /etc/cntlr-key.conf
   owner: root:root
   permissions: "400"
   content: |
      -----BEGIN PRIVATE KEY-----
      <private key content>
      -----END PRIVATE KEY-----
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
         groupName: <Monitoring Domain Name>
         subGroupName: <VPC Name>
         user: <Username>
         password: <Password>
         remoteIP: <IP address of the GigaVUE-FM> or <IP address of the
Proxy>
         remotePort: 443
```

</td></tr>
</table>

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

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

Register GigaVUE V Series Node or Proxy using a configuration file

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

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

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

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

3. Restart theGigaVUE V Seriesproxy service.
   - V Series node:
     `$ sudo service vseries-node restart`
   - V Series proxy:
     `$ sudo service vps restart`

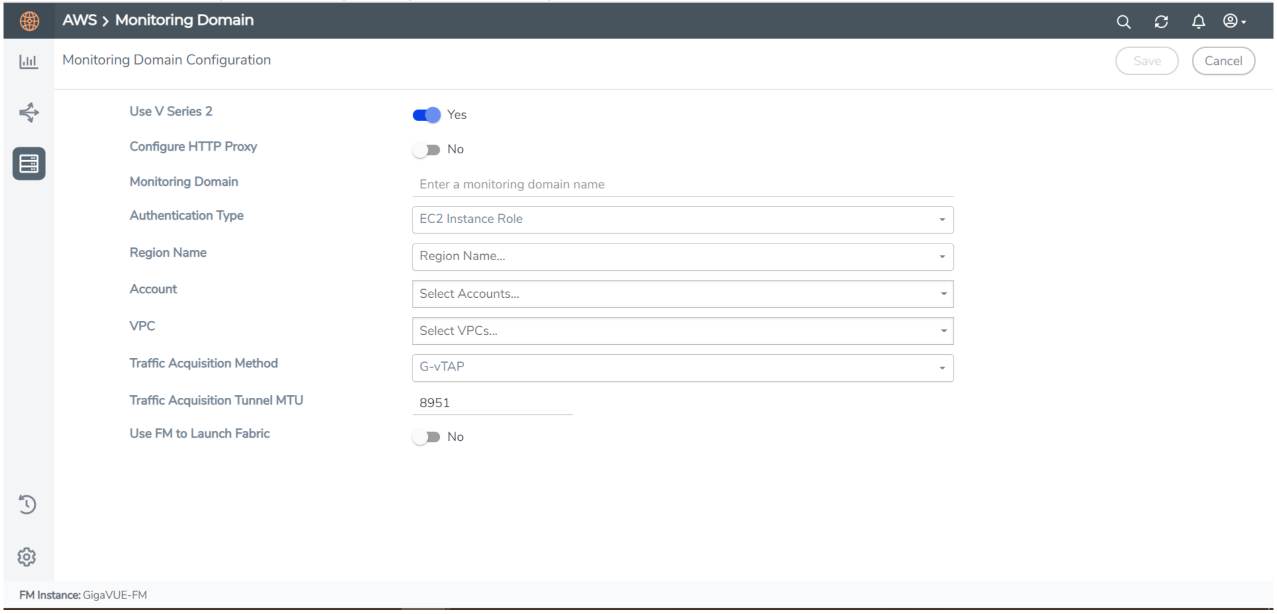
The deployed GigaVUE V Series node or proxy registers with the GigaVUE-FM. After successful registration theGigaVUE V Series node or proxy sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing ,the fabric node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the 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.

Configure UCT-V Controller in AWS

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

To configure UCT-V Controller in AWS platform:

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



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

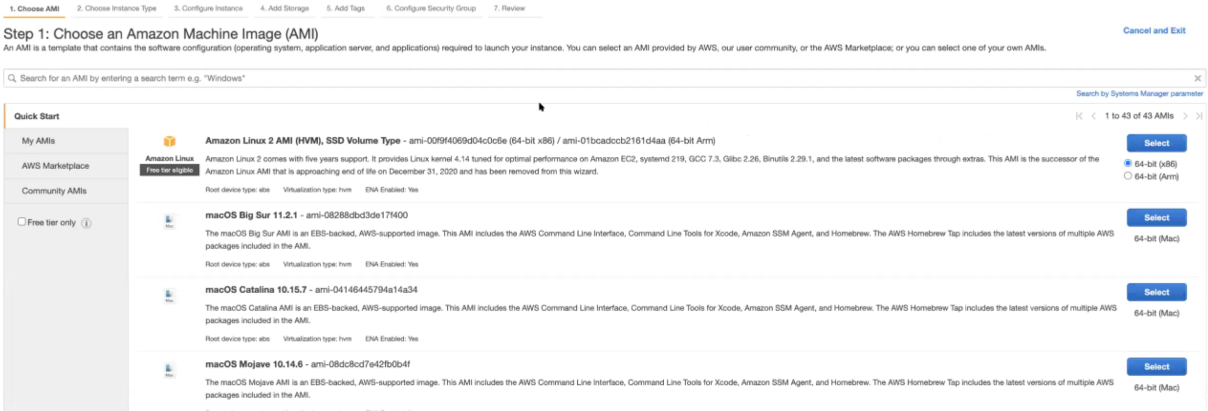
FM Instance: GigaVUE-FM

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

Register UCT-V Controller using User Data

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

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



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-00f9f4069d04c0c6e (64-bit x86) / ami-01bcadccb2161d4aa (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

● 64-bit (x86)
○ 64-bit (Arm)

macOS Big Sur 11.2.1 - ami-08288dbd3de17f400

The macOS Big Sur AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (Mac)

macOS Catalina 10.15.7 - ami-04146445794a14a34

The macOS Catalina AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (Mac)

macOS Mojave 10.14.6 - ami-08dc8cd7e42fb0b4f

The macOS Mojave AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

64-bit (Mac)

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

<table>
<tr><th>Field</th><th>User Data</th></tr>
<tr><td>User data without custom certificate</td><td>

```
#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
```

</td></tr>
<tr><td>User data with custom certificate</td><td>

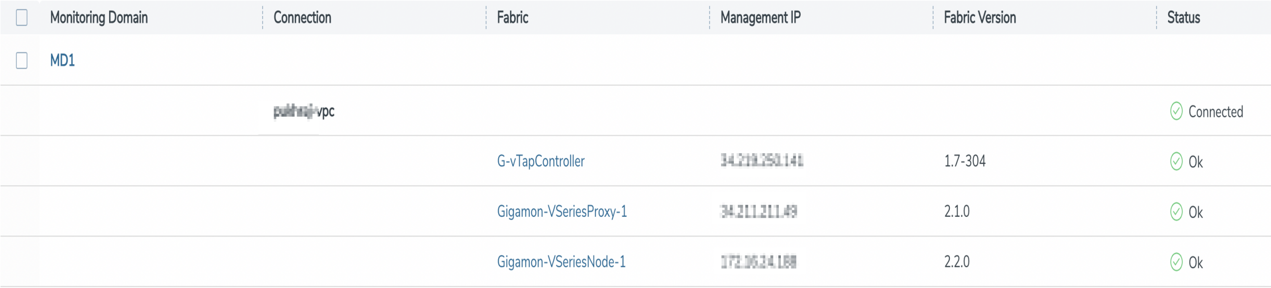
```
#cloud-config
 write_files:
 - path: /etc/cntlr-cert.conf
   owner: root:root
   permissions: "0644"
   content: |
      -----BEGIN CERTIFICATE-----
      <certificate content>
      -----END CERTIFICATE-----
 - path: /etc/cntlr-key.conf
   owner: root:root
   permissions: "400"
   content: |
      -----BEGIN PRIVATE KEY-----
      <private key content>
      -----END PRIVATE KEY-----
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
         groupName: <Monitoring Domain Name>
         subGroupName: <VPC Name>
         user: <Username>
         password: <Password>
         remoteIP: <IP address of the GigaVUE-FM>
         remotePort: 443
```

</td></tr>
</table>

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

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

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



□	Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
□	MD1					
		[redacted]				✓ Connected
			G-vTapController	[redacted]	1.7-304	✓ Ok
			Gigamon-VSeriesProxy-1	[redacted]	2.1.0	✓ Ok
			Gigamon-VSeriesNode-1	[redacted]	2.2.0	✓ Ok

Register UCT-V Controller using a configuration file

To register UCT-V Controller using a configuration file:

a. Log in to the UCT-V Controller.

b. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to UCT-V Controller, refer to the below table for details:

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

c. Restart the UCT-V Controller service.

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

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

Configure UCT-V in AWS

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

> **NOTE:** Deployment of UCT-Vs through a third-party orchestrator is supported on Linux and Windows platforms. 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. Edit the local configuration file and enter the following user data.

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

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

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

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

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

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

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

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

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

Install UCT-V

You can install UCT-V agent on Windows and Linux platforms to acquire traffic using UCT-V.

For more information on installing the agents, refer to the following topics:

- Install Linux UCT-V Agent
- Windows UCT-V Installation

Supported Operating Systems for UCT-V

Supported Operating System for UCT-V[1] is v6.4.00

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

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

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

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

Install Linux UCT-V Agent

You can install UCT-V agent on Ubuntu, SELinux on CentOS, Red Hat Enterprise Linux using Debian or RPM packages.

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

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

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

For more information on installing the agents, refer to the following topics:

- ENI Configurations
- Install UCT-V on Ubuntu using Debian Package
- Install UCT-V on Redhat and CentOS using RPM Package
- Install UCT-V on SELinux Enabled Red Hat and CentOS

ENI Configurations

Single ENI Configuration

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

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

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

Dual ENI Configuration

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

For example, assume that there is eth0 and eth1 in the monitoring instance. In the UCT-V configuration, eth0 can be configured as the source interface, ingress 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.

Install UCT-V on Ubuntu using Debian Package

This section provides instructions on how to UCT-V on Ubuntu using a Debian package.

To install UCT-V on Ubuntu using the debian package, perform the following steps:

1. Download theUCT-V**6.4.00** Debian (.deb) package from the Gigamon Customer Portal.
2. Copy the package to your instance. Install the package with root privileges,

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

3. After installing the UCT-V package, modify the file **/etc/uctv/uctv.conf** to configure and register the source and destination interfaces.

   > **NOTE:** If you make any changes to the uctvt config file after the initial setup, you need to restart the agent and refresh or synchronize the inventory from GigaVUE-FM to reflect the changes and start traffic mirroring again. However, if you have an ongoing monitoring session that is active and functioning well, modifying the UCT-V config file can cause traffic to be lost until GigaVUE-FM performs an automatic synchronization every 15 minutes.

   The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

   Example 1—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—Monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the migrnrbonred packets.

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

   Example 3—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
   ```

4. Save the file.
5. To enable the third-party orchestration, you must create **/etc/gigamon-cloud.conf** configuration file with the following contents:

   ```
   Registration:
           groupName: <Monitoring Domain Name>
           subGroupName: <Connection Name>
           user: <username>
           password: <password>
           remoteIP: <controller list IP addresses separated by comma>
   ```

```
                    remotePort: 8891
```

6. Reboot the instance.

If the The UCT-V is successfully installed, then the status will be displayed as running.

To check the status, run the following command:

```
sudo service uctv status
UCT-V is running
```

Install UCT-V on Redhat and CentOS using RPM Package

This section provides instructions on how to install UCT-V on Red Hat and CentOS using RPM package

To install UCT-V on Redhat, CentOS, or other RPM-based system using the RPM package, perform the following steps:

1. Download theUCT-V`6.4.00` RPM (.rpm) package from the Gigamon Customer Portal.
2. Copy this package to your instance. Install the package with root privileges, for example:

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

3. After installing the UCT-V package, modify the file **/etc/uctv/uctv.conf** to configure and register the source and destination interfaces.

   > **NOTE:** If you make any changes to the UCT-V config file after the initial setup, you need to restart the agent and refresh or synchronize the inventory from GigaVUE-FM to reflect the changes and start traffic mirroring again. However, if you have an ongoing monitoring session that is active and functioning well, modifying the UCT-V config file can cause traffic to be lost until GigaVUE-FM performs an automatic synchronization every 15 minutes.

   The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

   Example 1—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—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—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
   ```

4. Save the file.

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

   ```
   Registration:
           groupName: <Monitoring Domain Name>
           subGroupName: <Connection Name>
           user: <username>
           password: <password>
           remoteIP: <controller list IP addresses separated by comma>
           remotePort: 8891
   ```

6. Reboot the instance or restart the service by running the command `sudo service uctv start`

If the The UCT-V is successfully installed, then the status will be displayed as running.

To check the status, run the following command:

```
sudo systemctl status uctv
```

Install UCT-V on SELinux Enabled Red Hat and CentOS

This section provides instructions on how to install UCT-V on Red Hat and CentOS.

Prerequisites:

- For multiple NIC/ENI configuration, you might have to to modify the network configuration files to make sure that the extra NIC/ENI will initialize at boot time.
- Install the packages Python3 and Python modules such as netifaces, urllib3, and requests.
- The packages iproute-tc, tc is required for RHEL and CentOS VMs.
- You must have sudo/root access to edit the UCT-V configuration file.
- You must ensure that the port 9901 is allowed in the Firewall. This port is required for the communication between UCT-V and UCT-V Controller.

To install UCT-V on Redhat, CentOS, or other RPM-based system using the RPM package, perform the following steps:

1. Download the following packages from the Gigamon Customer Portal:
   - gigamon-gigavue_uctv_**6.4.00**_x86_64.rpm
2. Copy the downloaded UCT-V package files to UCT-V.
3. Install UCT-V package:
   ```
   sudo rpm -ivh gigamon-gigavue_uctv_6.4.00_x86_64.rpm
   ```
4. Edit the **uctv.conf** file to configure the required interface as source/destination for mirror:

   > **NOTE:** If you make any changes to the UCT-V agent config file after the initial setup, you need to restart the UCT-V and refresh or synchronize the inventory from GigaVUE-FM to reflect the changes and start traffic mirroring again. However, if you have an ongoing monitoring session that is active and functioning well, modifying the UCT-V config file can cause traffic to be lost until GigaVUE-FM performs an automatic synchronization every 15 minutes.

   ```
   # eth0 mirror-src-ingress mirror-src-egress mirror-dst
   # sudo systemctl status uctv
   ```
5. Reboot the instance.

Windows UCT-V Installation

You can install UCT-V on Windows by using MSI package or ZIP package.

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

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

For more information on installing the agents, refer to the following topics:

- Windows UCT-V Installation Using MSI Package
- Windows UCT-V Installation Using ZIP Package

Windows UCT-V Installation Using MSI Package

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

1. Download the Windows UCT-V `6.4.00` MSI package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator** and the UCT-V service starts automatically.
3. 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:** If you make any changes to the UCT-V config file after the initial setup, you need to restart the UCT-V and refresh or synchronize the inventory from GigaVUE-FM to reflect the changes and start traffic mirroring again. However, if you have an ongoing monitoring session that is active and functioning well, modifying the UCT-V config file can cause traffic to be lost until GigaVUE-FM performs an automatic synchronization 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 the interface does not have mirror-src permissions, then it will have both mirror-src-ingress and mirror-src-egress permissions..
   >   - 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 no interfaces have mirror-src permissions, all interfaces will have mirror-src-ingress and mirror-src-egress permissions.

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

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

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

   ```
   192.168.1.0/24   mirror-src-ingress mirror-src-egress
   192.168.2.0/24   mirror-dst
   ```
4. Save the file.

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

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

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

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

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

Windows UCT-V Installation Using ZIP Package

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

1. Download the Windows UCT-V `6.4.00` ZIP package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Extract the contents of the .zip file into a convenient location.
3. Run 'install.bat' as an **Administrator** and the UCT-V service starts automatically.
4. 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:** If you make any changes to the UCT-V config file after the initial setup, you need to restart the UCT-V and refresh or synchronize the inventory from GigaVUE-FM to reflect the changes and start traffic mirroring again. However, if you have an ongoing monitoring session that is active and functioning well, modifying the UCT-V config file can cause traffic to be lost until GigaVUE-FM performs an automatic synchronization 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 the interface does not have mirror-src permissions, then it will have both mirror-src-ingress and mirror-src-egress permissions..
   >   - 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 no interfaces have mirror-src permissions, all interfaces will have mirror-src-ingress and mirror-src-egress permissions.

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

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

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

   ```
   192.168.1.0/24   mirror-src-ingress mirror-src-egress
   192.168.2.0/24   mirror-dst
   ```
5. Save the file.

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

```
Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        user: <username>
        password: <password>
        remoteIP: <controller list IP addresses separated by comma>
        remotePort: 8891
```

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

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

> **NOTE:** You must edit the Windows Firewall settings to grant access to the uctv process. To do this, access the Windows Firewall settings and find "uctvd" in the list of apps and features. Select it to grant access. Be sure to select both Private and Public check boxes. If "uctvd" does not appear in the list, click **Add another app...** Browse your program files for the UCT-V application (uctvd.exe) and then click **Add**. (**Disclaimer:** These are general guidelines for changing Windows Firewall settings. See Microsoft Windows help for official instructions on Windows functionality.)

Create Images with Agent Installed

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**.

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
- Interface Mapping
- Create Ingress and Egress Tunnels
- Create Raw Endpoint
- Create a New Map
- Add Applications to Monitoring Session
- Deploy Monitoring Session
- View Monitoring Session Statistics
- Visualize the Network Topology

Create a Monitoring Session

You must create a monitoring domain before creating a monitoring session. Refer to Create Monitoring Domain for more detailed information on how to create a monitoring domain.

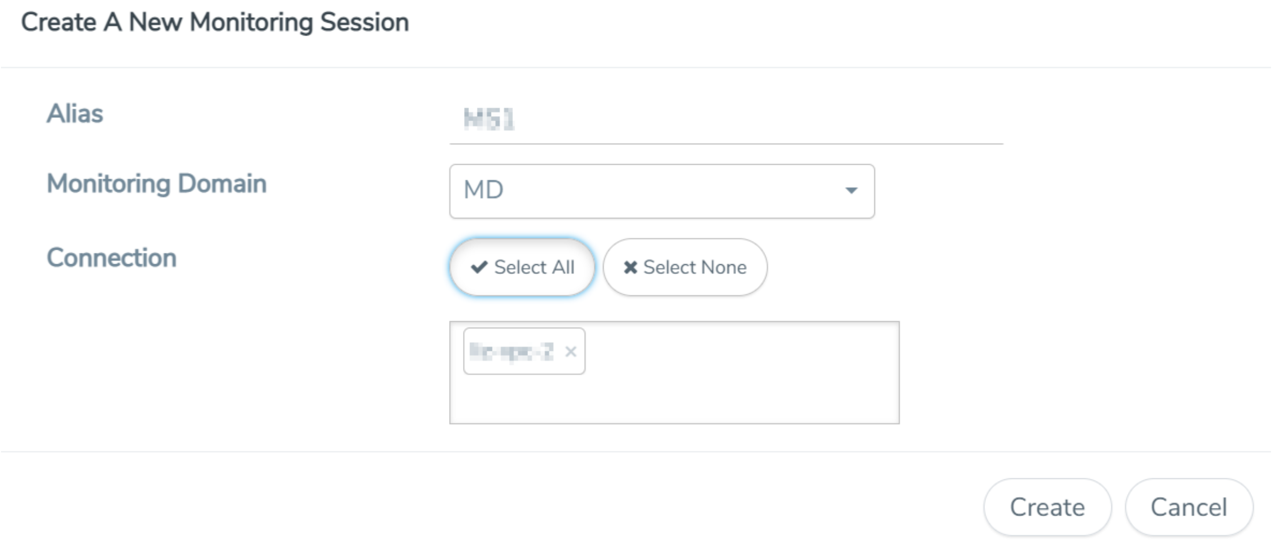
GigaVUE-FM automatically collects inventory data on all target instances available in your cloud environment. You can design your monitoring session to include or exclude the instances that you want to monitor. You can also choose to monitor egress, ingress, or all traffic. You can filter the traffic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

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

You can create multiple monitoring sessions per monitoring domain.

To create a new monitoring session:

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



Create A New Monitoring Session

Alias: [redacted]

Monitoring Domain: MD

Connection: [redacted]

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

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

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

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

Button	Description
Edit	Opens the Edit page for the selected monitoring session. **NOTE:** In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.
Delete	Deletes the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Deploy	Deploys the selected monitoring session.

Button	Description
Undeploy	Undeploys the selected monitoring session.
Apply Threshold	You can use this button to apply the threshold template created for monitoring cloud traffic health. Refer to Monitor Cloud Health for more detailed information on cloud traffic health, how to create threshold templates, and how to apply threshold templates.
Apply Policy	You can use this button to enable precyption, prefiltering, or Secure Tunnel. Refer to Enable Prefiltering, Precryption, and Secure Tunnel for more details.

Edit Monitoring Session

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

Refer to the following topics for detailed information:

- Create Ingress and Egress Tunnels
- Add Applications to Monitoring Session
- Create Raw Endpoint
- Create a New Map

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

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

Enable Prefiltering, Precryption, and Secure Tunnel

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

Enable Prefiltering

To enable Prefiltering, follow the steps given below:

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

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

Enable Precryption

To enable Precryption, follow the steps given below:

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

Enable Secure Tunnel

To enable Secure Tunnel, follow these steps:

1. In the Edit Monitoring Session page, click **Options**. The **Monitoring Session Options** page appears.
2. Enable the **Secure Tunnel** button. You can enable secure tunnel for both mirrored and precrypted traffic. For more information about Secure Tunnel, refer to

Prefiltering

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

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

Each monitoring session can have a maximum of 16 rules.

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

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

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

Create Prefiltering Policy Template

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

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

1. Go to **Resources** > **Prefiltering**, and then click **UCT-V**.

2. Click **New**.

3. Enter the name of the template in the **Template Name** field.

4. Enter the name of a rule in the **Rule Name** field.

5. Click any one of the following options:

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

6. Click any one of the following options as per the requirement:

   - Bi-Directional —- Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
   - Ingress — Filters the traffic that flows in.
   - Egress — Filters the traffic that flows out.

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

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

- L3
- L4

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

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

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

- Not Equal to
- Equal to

11. Enter the value for the given filter.

12. Click **Save**.

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

Interface Mapping

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

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select a Monitoring session from the list view and click **Actions > Edit**. The Edit Monitoring session page appears.
3. In the Edit Monitoring session canvas page, click on the **Interface Mapping** button.
4. The **Select nodes to deploy the Monitoring Session dialog box** appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.

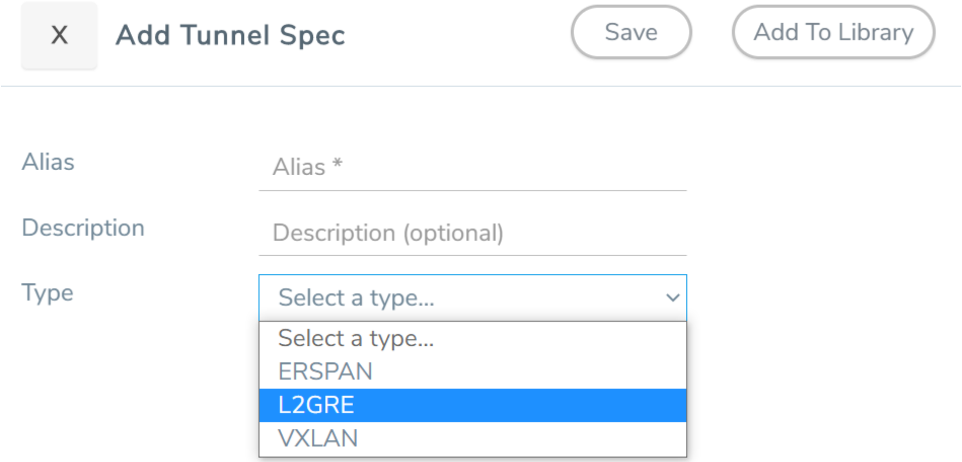
5. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual GigaVUE V Series Nodes. Then, click **Deploy**.

Create Ingress and Egress Tunnels

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

To create a new tunnel endpoint:

1. After creating a new monitoring session, or click **Actions > Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.


X
Add Tunnel Spec
Save
Add To Library
Alias
Alias *
Description
Description (optional)
Type
Select a type...
Select a type...
ERSPAN
L2GRE
VXLAN

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

Field	Description	
Alias	The name of the tunnel endpoint. **NOTE:** Do not enter spaces in the alias name.	
Description	The description of the tunnel endpoint.	
Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN, or UDPGRE to create a tunnel.	
VXLAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled

Field	Description	
		with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the	

Field	Description	
	GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295.
Out	Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295.
ERSPAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		

Field	Description	
In	**IP Version**	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	**IP Version**	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

Field	Description	
Out	**IP Version**	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

4. Click **Save**.

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

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

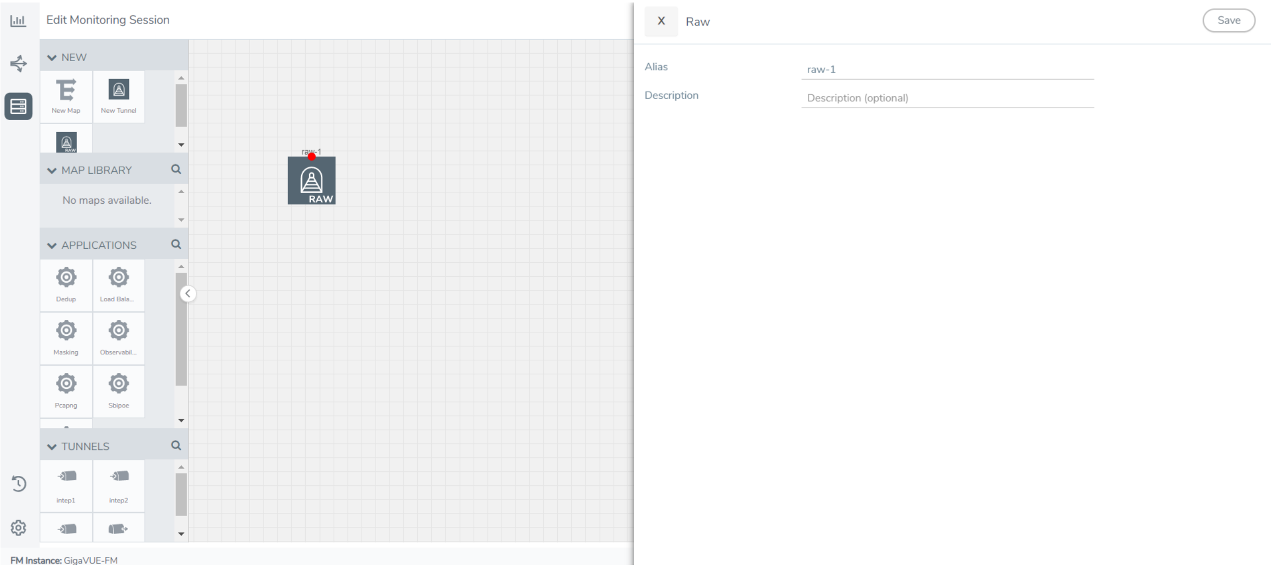
After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When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

Create Raw Endpoint

Raw End Point (REP) is used to pass traffic from an interface. 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** from **NEW** to the graphical workspace.
2. Click the **New RAW** icon and select **Details**. The **RAW** quick view page appears.
3. Enter the alias and description. In the **Alias** field, enter a name for the Raw End Point and click **Save**.



Alias raw-1

Description Description (optional)

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

Create a New Map

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

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

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

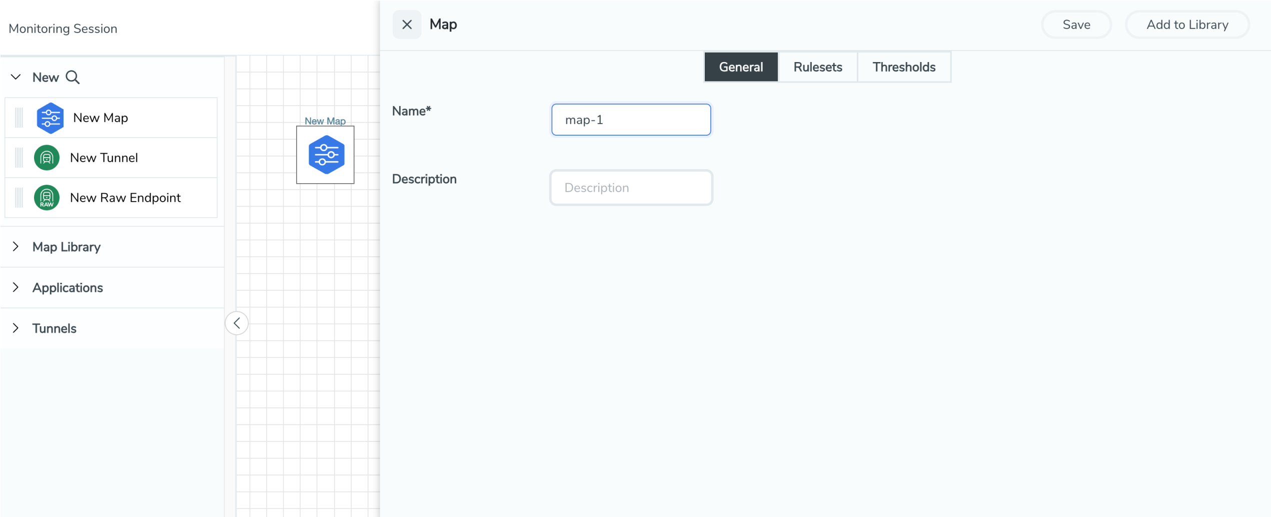
Keep in mind the following when creating a map:

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

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the monitoring session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps** Below are the filter rule types that work in ATS: ● mac Source ● mac Destination ● ipv4 Source ● ipv4 Destination ● ipv6 Source ● ipv6 Destination ● VM Name Destination ● VM Name Source ● VM Tag Destination - Not applicable to Nutanix. ● VM Tag Source - Not applicable to Nutanix. ● VM Category Source - Applicable only to Nutanix ● VM Category Destination - Applicable only to Nutanix. ● Host Name -Applicable only to Nutanix and VMware. The traffic direction is as follow: ● For any rule type as Source - the traffic direction is egress. ● For Destination rule type - the traffic direction is ingress. ● For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. **NOTE:** If no ATS rule filters listed above are used, all VMs and vNICS are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

To create a new map:

1. After creating a new monitoring session, or click **Actions > Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Map**, drag and drop a new map template to sthe workspace. The New Map quick view appears.



Name* map-1

Description Description

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

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

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

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

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

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

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

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

Rules and Notes:

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

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

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

Example- Create a New Map using Inclusion and Exclusion Maps

Consider a monitoring session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

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

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

Add Applications to Monitoring Session

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

- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- GENEVE Decap
- Header Stripping
- Application Metadata Exporter
- SSL Decrypt

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

You can also configure the following GigaSMART operations from the **Traffic > Solutions > Application Intelligence**:

- Application Metadata Intelligence
- Application Filtering Intelligence

For more information, refer to these GigaSMART Operations in the *GigaVUE Fabric Management Guide*.

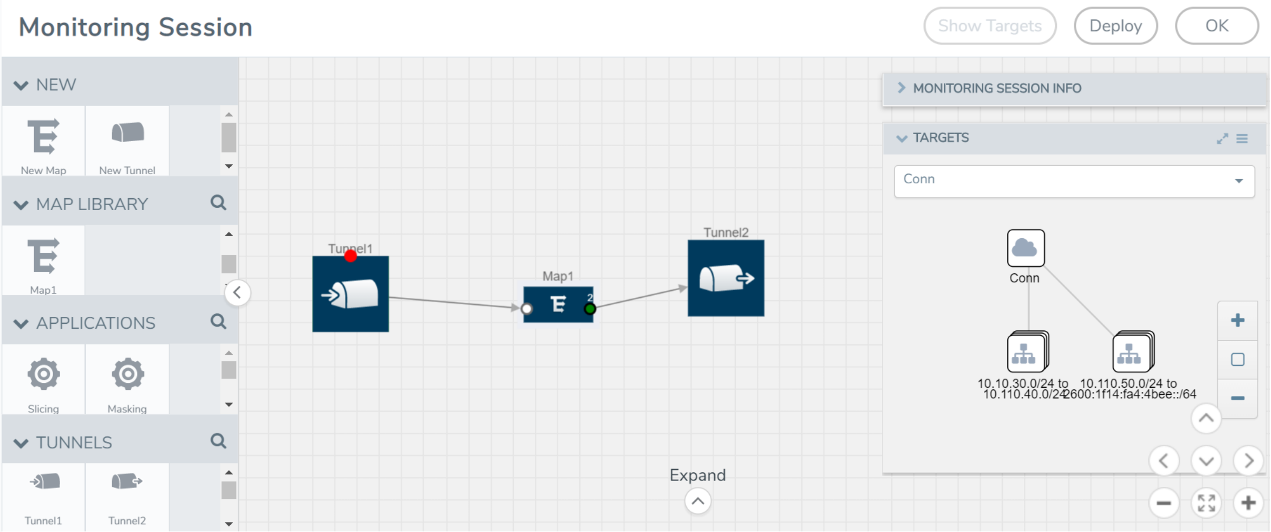
Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop the following items to the canvas as required:
   - Ingress tunnel (as a source) from the **NEW** section
   - Maps from the **MAP LIBRARY** section
   - Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
   - GigaSMART apps from the **APPLICATIONS** section
   - Egress tunnels from the **TUNNELS** section

2. After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

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



3. (Not applicable for Tunnel traffic acquisition method) Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.
4. Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series nodes. Click on the status link in the Status column on the Monitoring Session page to view the Monitoring Session Deployment Report. When you click on the Status link, the Deployment Report is displayed. If the monitoring session is not deployed properly, then one of the following errors is displayed in the Status column.
   - Partial Success—The session is not deployed on one or more instances due to V Series node failure.
   - Failure—The session is not deployed on any of the V Series nodes.

   The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

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

Button	Description
Undeploy	Undeploys the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Edit	Opens the Edit page for the selected monitoring session. **NOTE:** In case of an error while editing a monitoring session, undeploy and deploy the monitoring session

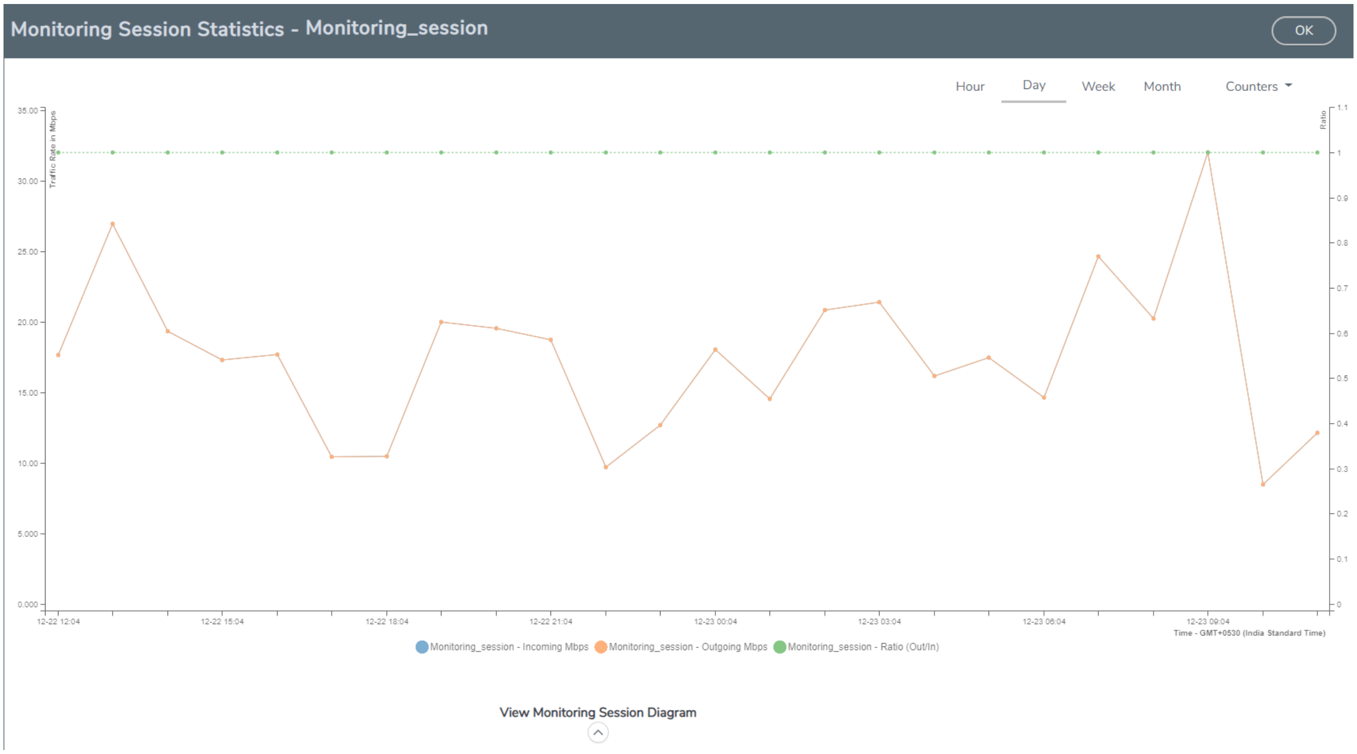
Button	Description
	again..
Delete	Deletes the selected monitoring session.

View Monitoring Session Statistics

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

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

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


Monitoring Session Statistics - Monitoring_session
OK
Hour
Day
Week
Month
Counters
Traffic Rate in Mbps
35.00
30.00
25.00
20.00
15.00
10.00
5.000
0.000
Ratio
1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
12-22 12:04
12-22 15:04
12-22 18:04
12-22 21:04
12-23 00:04
12-23 03:04
12-23 06:04
12-23 09:04
Time - GMT+0530 (India Standard Time)
● Monitoring_session - Incoming Mbps
● Monitoring_session - Outgoing Mbps
● Monitoring_session - Ratio (Out/In)
View Monitoring Session Diagram

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

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

View Health Status on the Monitoring Session Page

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

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

Health

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

V Series Node Health

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

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

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

Target Source Health

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

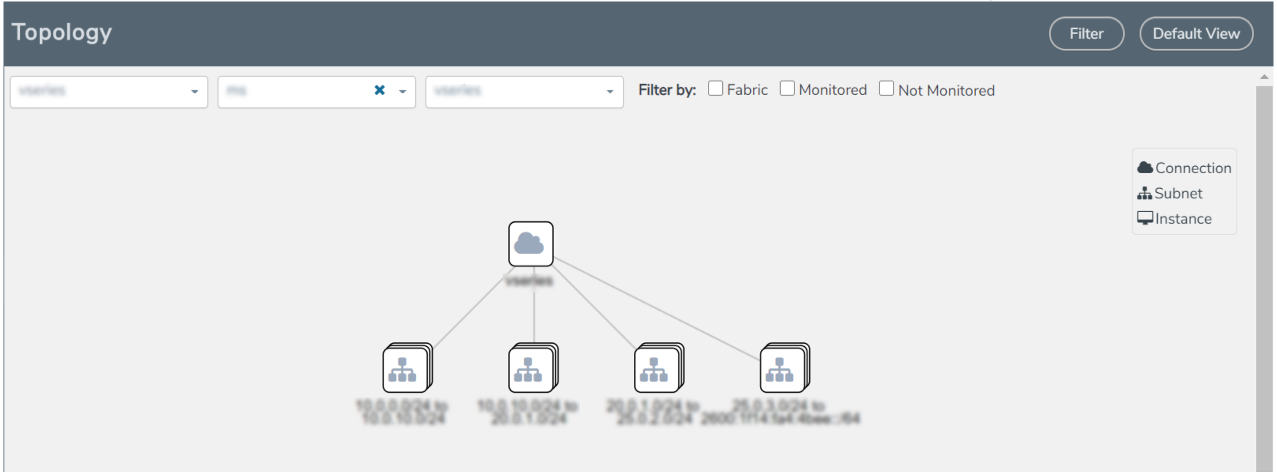
You can view the health status of the individual targets and also the error message associated with them, by clicking on the Target Source Health column.

Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

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



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

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

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

Configure Application Intelligence Solutions on GigaVUE V Series Nodes for AWS

To configure the Application Intelligence solution on the GigaVUE V Series Nodes, create a virtual environment with the required connections. After creating the connections, configure the sources and the required destinations for the traffic flow. Refer the following topics for step by step instructions on how to configure Application Intelligence solution for GigaVUE V Series Nodes:

- Configure Environment
- Create Credentials
- Connect to AWS
- Create Source Selectors
- Create Tunnel Specifications
- User Defined Application
- Slicing and Masking in Application Filtering Intelligence
- Application Metadata Intelligence
- Create NetFlow Session for Virtual Environment

Important Notes:

- You can deploy multiple GigaVUE V Series Nodes in a connection.
- When upgrading from any previous version to 6.4.00, you cannot enable secure tunnels. You will have to delete the Application Intelligence solution and deploy it again with secure tunnels.
- You cannot enable secure tunnels for an existing Application Intelligence Session, you must delete the Application Intelligence solution and deploy it again with secure tunnels.
- You can use GigaVUE V Series Proxy to scale and manage multiple V Series Nodes. Refer to the GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide for detailed information.

- You can use tool templates while creating an Application Metadata Intelligence session. To create a custom tool template for GigaVUE V Series Node, signature is required from the node. Refer to the Tool Templates section in the *GigaVUE Fabric Management Guide* for more detailed information.
- Prior to configuring the Application Intelligence solution, refer to the Prerequisites topic for the minimum requirements.
- When GigaVUE-FM and GigaVUE V Series Nodes are deployed in different cloud platforms, then the GigaVUE-FM public IP address must be added to the **Data Notification Interface** as the Target Address in the Event Notifications page. Refer to Configuration Settings section in the *GigaVUE Administration Guide* for configuration details.
- To delete a GigaVUE V Series Node deployed in a Application Intelligence solution, you must delete the resources in the following order:
    1. Delete the Application Intelligence solution.
    2. Delete the GigaVUE V series Node and Connection.
    3. Delete the Environment.

Configure Environment

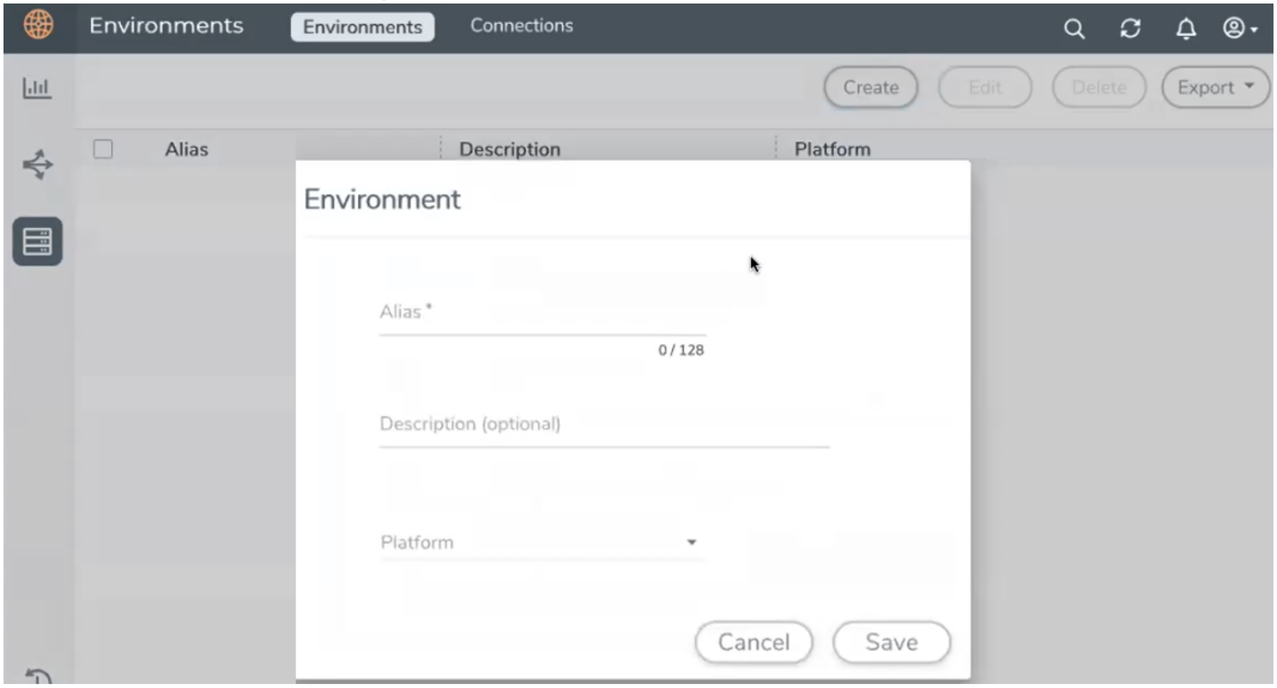
The Environments page allows you to create the following:

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

Create Environment

To configure the Environment:

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



3. Select or enter the following details:

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

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

Use the following buttons to manage your environment:

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

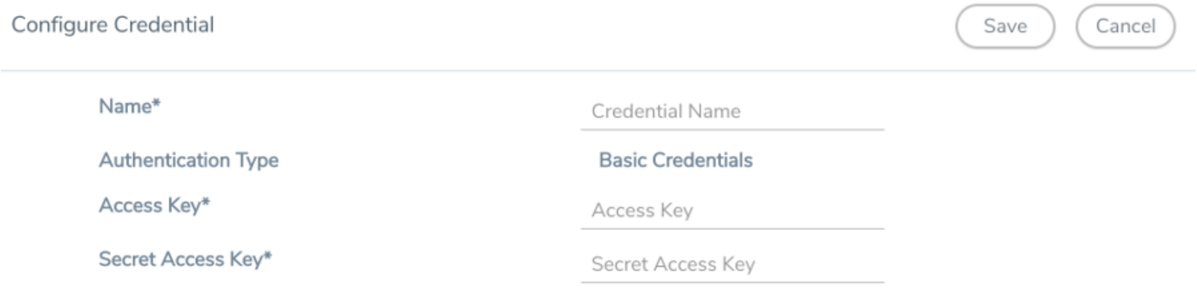
Create Credentials

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

Create AWS Credentials

To create AWS credentials:

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



Configure Credential

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

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

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

5. Click **Save**.

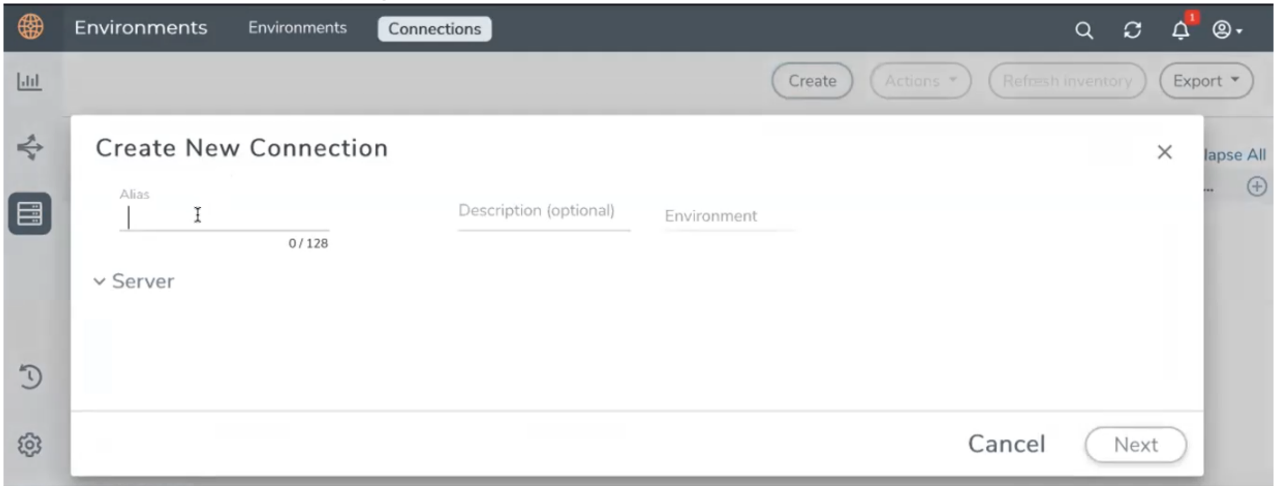
Connect to AWS

After creating a environment create a connection between the AWS and GigaVUE-FM. Refer to the following step given below for detailed information on how to create a new connection.

Create Connection

To create a new Connection:

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



3. The **Create New Connection** dialog box opens. Enter the details as mentioned in the below section.

> **NOTE:** When creating a connection in the connections page, the corresponding monitoring domain created for internal use in GigaVUE-FM will not be displayed in the Monitoring Domain list page.

> **NOTE:** For Application Intelligence solution, you must add the UDP port 2056 for GigaVUE-FM in your AWS security group.

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

Field	Description
Name	Name used to identify the connection.
Credential	Select your credentials from the drop-down menu. Refer Create Credentials for detailed information on how to create credentials.

Field	Description
Select Region	The AWS region for the connection. For example, EU (London). **NOTE:** If the region you want to choose is not available in the Region Name list, you can add a custom region. **Adding a Custom Region** To add a custom region: **a.** In the Region Name drop-down list, select **Custom Region**. **b.** In the Custom Region Name field, enter the name of the region that is not available in the list.
Select Account	Select the AWS account name/id.
Select VPCs	Select the VPC
Traffic Acquisition Method	Select a Tapping method. The available options are: ▪ **UCT-V**: If you select UCT-V as the tapping method, you must configure the UCT-V Controller to monitor the UCT-Vs. You can also configure the UCT-V Controller and UCT-Vs using your own orchestor. Refer to Configure GigaVUE Fabric Components using AWS Orchestrator for detailed information. ▪ **VPC Traffic Mirroring**: If you select VPC Traffic Mirroring option as tapping method, only nitro-based agent is support. If you wish to use an external load balancer (optional). Select **Yes** to use a load balancer. Refer to Configure an External Load Balancer and Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS for detailed information. UCT-V Controller configuration is not required for VPC Traffic Mirroring. ▪ **Tunnel**: If you use select Tunnel as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to GigaVUE V Series Nodes without deploying UCT-Vs or UCT-V Controllers.. **NOTE:** For VPC Traffic Mirroring option, additional permissions are required. Refer to the Permissions for details.
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. **NOTE:** The default MTU is 1450. You can edit the MTU value according to your requirements. The valid range is between 1450 to 9000.

In the AWS Virtual Node Deployment page, select or enter the following details and click **Next**:

Fields	Description
Centralized VPC	Alias of the centralized VPC in which the UCT-V Controllers, V Series Proxies and the GigaVUE V Series nodes are launched.
EBS Volume	The Elastic Block Store (EBS) volume that you can attach to the fabric components. The

Fields	Description
Type	available options are: ▪ gp2 (General Purpose SSD) ▪ io1 (Provisioned IOPS SSD) ▪ Standard (Magnetic).
SSH Key Pair	The SSH key pair for the GigaVUE fabric nodes.
Management Subnet	The subnet that is used for communication between the controllers and the nodes, as well as to communicate with GigaVUE-FM. This is a required field.
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs. **NOTE:** If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate.
Security Groups	The security group created for the GigaVUE fabric nodes.

Enable the **Configure a V Series Proxy** toggle button if you wish to deploy V Series nodes using a proxy. In the V Series Proxy section, select or enter the values for the fields as described in the below table.

Fields	Description
Version	GigaVUE V Series Proxy version.
Instance Type	Instance type for the GigaVUE V Series Proxy. The recommended minimum instance type is t2.micro. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
Number of Instances	Number of GigaVUE V Series Proxy to deploy in the monitoring domain.
Set Management Subnet	Use the toggle button to select a management subnet. • **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	Select one of the following IP address types: ▪ 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.

Fields	Description
	- Select **Public** if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. - Select **Elastic** if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. The elastic IP address does not change when you stop or start the instance.
Additional Subnets	(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. Click Add to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
Tags	(Optional) The key name and value that helps to identify the GigaVUE V Series Proxy instances in your AWS environment.

In the UCT-V Configuration section, select or enter the following details:

Fields	Description
Controller Version	The UCT-V Controller version. If there are multiple versions of UCT-Vs deployed in the EC2 instances, then you must configure multiple versions of UCT-V Controllers that matches the version numbers of the UCT-Vs. **NOTE:** If there is a version mismatch between UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the agents in the instances. Click **Add** to add multiple versions of UCT-V Controllers: An older version of UCT-V Controller can be deleted once all the UCT-Vs are upgraded to the latest version.
Instance Type	The instance type for the UCT-V Controller. The recommended minimum instance type is nitro-based starting from t2.micro. **NOTE:** GigaVUE V Series Node solution does not support non-nitro-based instance types.
Number of Instances	The number of UCT-V Controllers to deploy in the monitoring domain.
Agent Tunnel Type	The type of tunnel used for sending the traffic from UCT-Vs to GigaVUE V Series nodes. The options are GRE or VXLAN tunnels. If any Windows agents co-exist with Linux agents, VXLAN must be selected.
Agent Tunnel CA	The Certificate Authority (CA) that should be used in the UCT-V Controller for connecting the tunnel.
UCT-V MTU (Maximum Transmission Unit)	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. - In AWS, the default value is 9000. - For VXLAN, the default value is 8951. The UCT-V tunnel MTU must be at least 50 bytes less than the agent's destination interface MTU size.

Fields	Description
	- For GRE, the default MTU setting must be at least 42 bytes less than the default MTU. AWS Platform MTU is 9000 - With agent tunnel type L2GRE and 'Secure Mirror Traffic' option enabled, UCT-V Tunnel MTU should be set as (9000-42-53) = 8905. - With agent tunnel type L2GRE and 'Secure Mirror Traffic' option disabled, UCT-V Tunnel MTU should be configured as (9000-42) = 8958. - With agent tunnel type VXLAN and 'Secure Mirror Traffic' option enabled, UCT-V Tunnel MTU should be (9000-50-53) = 8897. - With agent tunnel type VXLAN and 'Secure Mirror Traffic' option disabled, UCT-V Tunnel MTU should be 8951.
IP Address Type	The IP address type. Select one of the following: - Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the UCT-V Controller and GigaVUE-FM. - Select **Public** if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. - Select **Elastic** if you want a static public IP address for your instance. Ensure to have the available elastic IP address in your VPC. **NOTE:** The elastic IP address does not change when you stop or start the instance.
Additional Subnet(s)	(Optional) If there are UCT-Vs on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the UCT-V Controller can communicate with all the UCT-Vs. Click **Add** to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
Tag(s)	(Optional) The key name and value that helps to identify the UCT-V Controller instances in your AWS environment. For example, you might have UCT-V Controllers deployed in a VPC. To identify the UCT-V Controllers you can provide a name that is easy to identify such as us-west-2-uctv-controllers. To add a tag, a. Click **Add tag**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-uctv-controllers.

In the V Series Node configuration section, select or enter the following:

Fields	Description
Version	GigaVUE V Series Node version.
Instance Type	The instance type for the GigaVUE V Series Node. The default instance type is

Fields	Description
	nitro-based t3a.xlarge. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
IP Address Type	Select one of the following IP address types: ▪ 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. The elastic IP address does not change when you stop or start the instance.
Min Number of Instances	The minimum number of GigaVUE V Series Nodes that must be deployed in the monitoring domain. The minimum number of instances must be 1. When 0 is entered, no GigaVUE V Series Node is launched. **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.
Max Number of Instances	The maximum number of GigaVUE V Series Nodes that can be deployed in the monitoring domain.
Tunnel MTU	The Maximum Transmission Unit (MTU) on the outgoing tunnel endpoints of the GigaVUE V Series Node when a monitoring session is deployed. The UCT-V and controller tunnel MTU should be 50 bytes less than the agent's destination interface MTU size. The default value is 9001.
Data Subnets	The subnet that receives the mirrored GRE or VXLAN tunnel traffic from the UCT-Vs. **NOTE:** Using the Tool Subnet checkbox you can indicate the subnets to be used by theGigaVUE V Series to egress the aggregated/manipulated traffic to the tools.

Use the following buttons to manage your AWS connections :

Button	Description
Create	Use to create new connection.
Actions	Provides the following options: • **Edit Connection** - Use to edit a connection. You can also use this option to deploy your node after creating the connection. • **Edit Node** - If you have already deployed your node, then use this option to edit your node. You can also use this option to add more nodes into your existing connection. • **Delete Connection** - Use to delete a connection.

Button	Description
	• **Delete Node** - Use to delete a node. • **Force Delete** - This option is enabled when an upgrade fails due to infrastructure issues. Use this option to force delete the connection. • **Upgrade Fabric** - Use to upgrade your fabric components.
Refresh Inventory	Use to refresh the entire connections page.
Export	Use to export the details from the Connections page into an XLS or a CSV file.

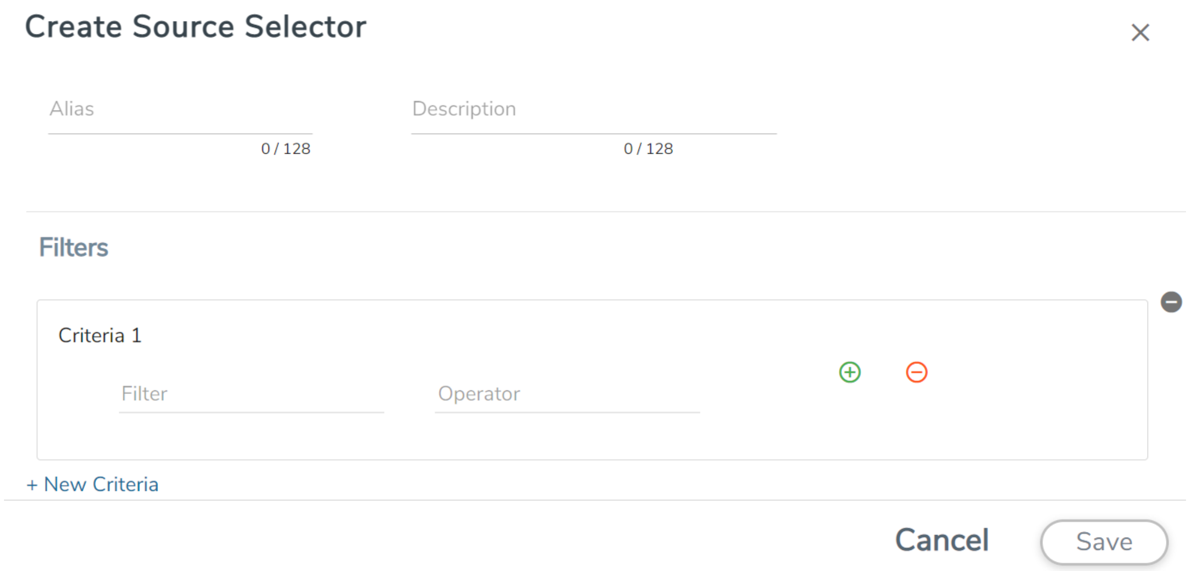
Create Source Selectors

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

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

To configure the Source Selectors:

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



3. Enter or select the required information:

Field	Description
Alias	Name of the source
Description	Description of the source
Filters	You can create a filter template from the Filters option
Criteria 1	Criteria to filter the traffic source. **NOTE:** You can create multiple criteria.
Filter	The criteria based on which the traffic is filtered. Select from the list of available filters. **NOTE:** Ensure that the registered traffic agents match the filter criteria.
Operator	Select the required operator based on the filter selected. Options are: • Starts with • Ends with • excludes • equals • between
Values	The values for the filter.

4. Click Save to save the source selector.

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

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

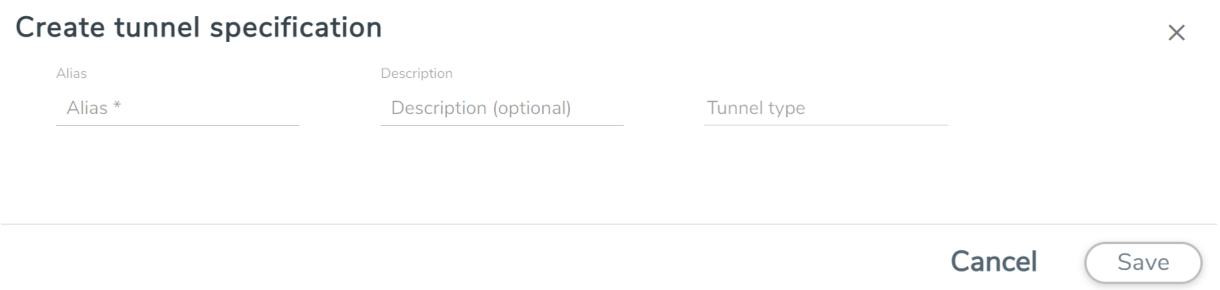
Create Tunnel Specifications

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

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

To configure the tunnels:

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



3. Enter or select the following information:

Field	Description
Alias	The name of the tunnel endpoint. **NOTE:** Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint.
Tunnel Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN to create a tunnel. Do not select UDPGRE tunnel type. **NOTE:** VXLAN is the only supported tunnel type for Azure.
Traffic Direction	The direction of the traffic flowing through the V Series node. • Choose **In** (Decapsulation) for creating an Ingress tunnel, Tunnel Spec for the Source should always have the Traffic Direction as IN, signifying an ingress tunnel. Enter values for the Key. • Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint. Select or enter values for MTU, Time to Live, DSCP, PREC, Flow Label, and Key. • ERSPAN, L2GRE, and VXLAN are the supported **Ingress tunnel** types. You can configure Tunnel Endpoint as your first level entity in Monitoring Session. • L2GRE and VXLAN are the supported **Egress tunnel** types. • For Azure connection, VXLAN is the supported Ingress and Egress tunnel type.
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.

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

User Defined Application

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

To configure User Defined Application signatures :

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

Create Rules under User Defined Application

1. Click **Inventory**.

2. Click **User Defined Applications** to create rules based on a set of **Supported Protocols and Attributes**. For information on **Supported protocols and Attributes** refer **User Defined Application** topic. This helps the physical or virtual node to classify the traffic based on the protocols and attributes selected in the created rule.

3. Click **New** in the **User Defined Applications** screen to create a new rule.

4. Enter **Application Name**.

5. Enter **Priority**. The value must be between 1 and 120.

Note: The least value will have the highest priority.

6. In the created rule:

   a. Choose the **Protocol** from the list of protocols.

   b. Choose the **Attributes** from the list of attributes.

   c. Choose the **Values** from the list of values.

7. Click **Apply**. The rule is now created. For information on the limitations for creating rules refer Configuration Limitations section.

8. Click the application listed under the **Applications** column.

9. Click the **Rule** tab.

10. Select a rule to view its protocol details.

Supported Protocols and Attributes

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

For supported Regex patterns, refer Supported RegExp Syntax

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

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

	subject_alt_name	t Alt Name(s)	host names which belong to the same certificate	to Client Only		
rtmp	cts-page_url	Page URL	URL of the webpage where the audio/video content is streamed	Client to Server Only	REGEXP	http:\/\/www.music.tv\/recorded\/1234567
tcp	stream	Payload Data	Data payload for a packet, excluding the header.		REGEXP	.*GIGAMON.* mindata = 70 Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
udp	stream	Payload Data	Data payload for a packet, excluding the header		REGEXP	.*GIGAMON.* mindata = 100 Refer Mindata
	port	Server Port	Server (listen)		UINT16 RANGE	80-4350

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

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

Mindata

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

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

Supported RegExp Syntax

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

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

Limitations

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

Slicing and Masking in Application Filtering Intelligence

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

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

Configuring Application Filtering Intelligence with Slicing

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

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

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

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

Configuring Application Filtering Intelligence with Masking

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

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

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

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

Configuring Application Filtering Intelligence with Slicing and Masking

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

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

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

Configure Application Intelligence Session

Application Intelligence provides a comprehensive solution that:

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

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

- **Application Visualization (earlier known as Application Monitoring)** - Identifies and monitors all applications contributing to the network traffic, and reports on the total applications and the total bandwidth they consume over a select period. Able to identify more than 3,200 applications. It displays the traffic statistics in bytes, packet and flows.
- **Application Filtering Intelligence**- Enables traffic filtering by layer 7 applications, which means you can filter out high-volume, low-risk traffic from reaching the tools and distribute high-risk network traffic of interest to the right tool at the right time.
- **Application Metadata Intelligence** - Supports exporting over 5000 attributes of metadata that provide relevant usage context on over 3,200 applications, thus enabling you to rapidly identify indicators of compromise (IoC) for security analytics and forensics tools.

Prerequisites

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

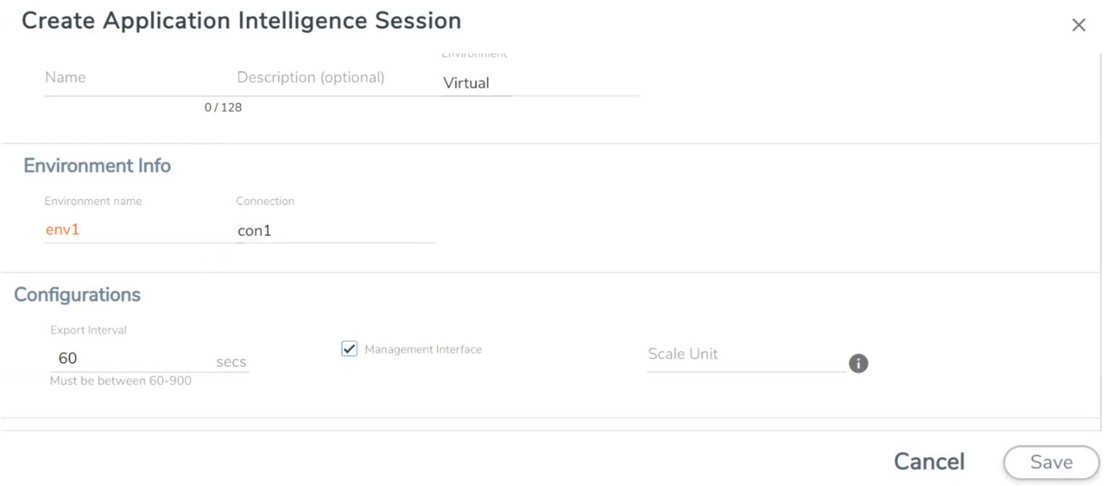
> **NOTE:** For Application Visualization and Application Metadata Intelligence, the destination(s) are defined internally by the solution.

Create an Application Intelligence Session in Virtual Environment

To create an Application Intelligence Session:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**.

2. Click **Create New**. The **Create Application Intelligence Session** page appears.



Create Application Intelligence Session

Name

Description (optional) 0 / 128

Environment: Virtual

Environment Info

Environment name: env1

Connection: con1

Configurations

Export Interval: 60 secs

Must be between 60-900

☑ Management Interface

Scale Unit

3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created:

   - Virtual- connects to the specific environment.

4. In the Environment section, select the **Environment Name**, and the **Connection Name.** To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides..

5. In the **Configurations** section, complete the following:

   a. Select an **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization. The valid range is 60–900 seconds.

   b. Select the required interface. By default, **Management Interface** is enabled. To export the data through tunnel interface, uncheck the Management Interface check box.

   c. Enter a value for the **Scale Unit**. The scale unit represents the number of flows supported by the application. If the scale unit value is 1, the maximum active flow limit will be 100k.
   Refer to the following table for the maximum scale unit supported for VMware, AWS Nutanix, and Azure platforms.

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

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

6. In the **Source Traffic** section, select anyone of the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

You can also filter the traffic based on the applications. For more information, see Create Application Filtering Intelligence.

Application Metadata Intelligence

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

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

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

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

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

Refer to Create Application Metadata Intelligence Session for Virtual Environment topic for step-by-step instructions on how to configure Application Metadata Intelligence on Virtual Environment.

Create Application Metadata Intelligence Session for Virtual Environment

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

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

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

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

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

Field	Description
Tool Name	Enter the tool Name
Tool IP Address	Enter the tool IP address
Template	Select the tool template. Refer to Tool Templates for more details on what are tool templates and to create custom tool templates.
L4 Source Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
L4 Destination Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
APPLICATION ID	Enable to export the data with Application Id.
Format	Select NetFlow or CEF
NetFlow: Select this option to use Netflow	
Record / Template type	● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds
CEF: Select this option to use CEF	
Record / Template type	● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.

   b. Click **App Editor**, to select the applications and its attributes. You can select a maximum of 64 attributes for each of the application. (Not applicable when using NetFLow V5 Template in the above **Template** drop-down menu.) The Application Editor screen appears as shown:

c. Select an **Application Family** and the **Applications** that needs to be filtered from the traffic. You can also select **Add All Applications in Family** or **Delete All Applications in Family**. The selected applications and their families appear in the **Selected Applications** section.

> **NOTE:** You can select the required applications without selecting the application family.

5. In the **Advanced Settings** > **Collects** section, you can select the following packet attributes:
   - Counter - Select the Bytes, and Packets.
   - IPv4 - Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.
   - IPv6 - Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
   - Transport -Select the required attributes. By default, Source Port, Destination Port are enabled.

   a. By default, the above collect types are displayed. Click ⊕ to add the following collect types:
      - Data Link - Select any one of the parameters such as Source Mac, Destination Mac and VLAN.
      - Timestamp - Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
      - Flow - Select the parameter as End Reason if required.
      - Interface - Select any one of the parameter such as Input Physical, Output Physical and Input Name.

6. In the **Application Metadata Settings** section:
   a. Select the Flow Behavior as any one of the following:
      - Uni-Directional
      - Bi-Directional. The default value is Bi-Directional.

   b. Enter the Timeout and Cache Size.

   c. You can enable or disable the **Multi-Collect** option to perform the following:
      - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
      - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.

   d. You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

NOTE: You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

e. You can enable or disable the **Advance Hash** option to perform the following:
   - **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
   - **Disable** — Disables the metadata cache advance-hash for flows.

f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.

g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.

7. Click **Save**.

The metrics of the Application Metadata traffic appear on the dashboard.

Create NetFlow Session for Virtual Environment

Note: This configuration is applicable only when using NetVUE Base Bundle.

NetFlow Generation is a simple and effective way to increase visibility into traffic flows and usage patterns across systems. The flow-generated data can be used to build relationships and usage patterns between nodes on the network.

To create an NetFlow session, follow these steps:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**.
2. Click **Create** . The **Create Application Intelligence Session** page appears.
3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created.
4. In the Environment section, select the **Environment Name**, and the **Connection Name.** To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides.
5. In the **Configurations** section, complete the following:
   a. The **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization is 5 seconds
   b. By default, **Management Interface** is enabled.

6. In the **Source Traffic** section, select anyone of the following:
   a. **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to Create Source Selectors

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

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

   > **NOTE:** Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration. Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel. For Azure Connection, VXLAN is the only supported Tunnel Type.

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

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

7. Click on the **Application Metadata** tab.

8. In the **Destination Traffic** section, click **+ Add New** to create an exporter to receive application-specific traffic. You can only create a maximum of 5 exporters. Enter the following details:

Field	Description
Tool Name	Enter the tool name.
Tool IP Address	Enter the tool IP address.
Template	Select the tool template. Refer to Tool Templates for more details on what tool templates are and to create custom tool templates.
L4 Source Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
L4 Destination Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
APPLICATION ID	Enable to export the data with Application Id.
Format	NetFlow
Record / Template type	● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds.

9. In the **Advanced Settings** > **Collects** section, the following details are already configured.

> **NOTE:** When the template is NetFlow v5 or when the format is NetFlow and the version as V5 you cannot modify the **Collects**.

- TimeStamp
- Counter
- Interface
- IPv4
- Transport

10. In the **Application Metadata Settings** section:
    a. Select the Flow Behavior as any one of the following:
    - Uni-Directional
    - Bi-Directional. The default value is Bi-Directional.

    b. Enter the Timeout and Cache Size.

    c. You can enable or disable the **Multi-Collect** option to perform the following:
    - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
    - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.

    d. You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

NOTE: You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

e. You can enable or disable the **Advance Hash** option to perform the following:
   - **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
   - **Disable** — Disables the metadata cache advance-hash for flows.

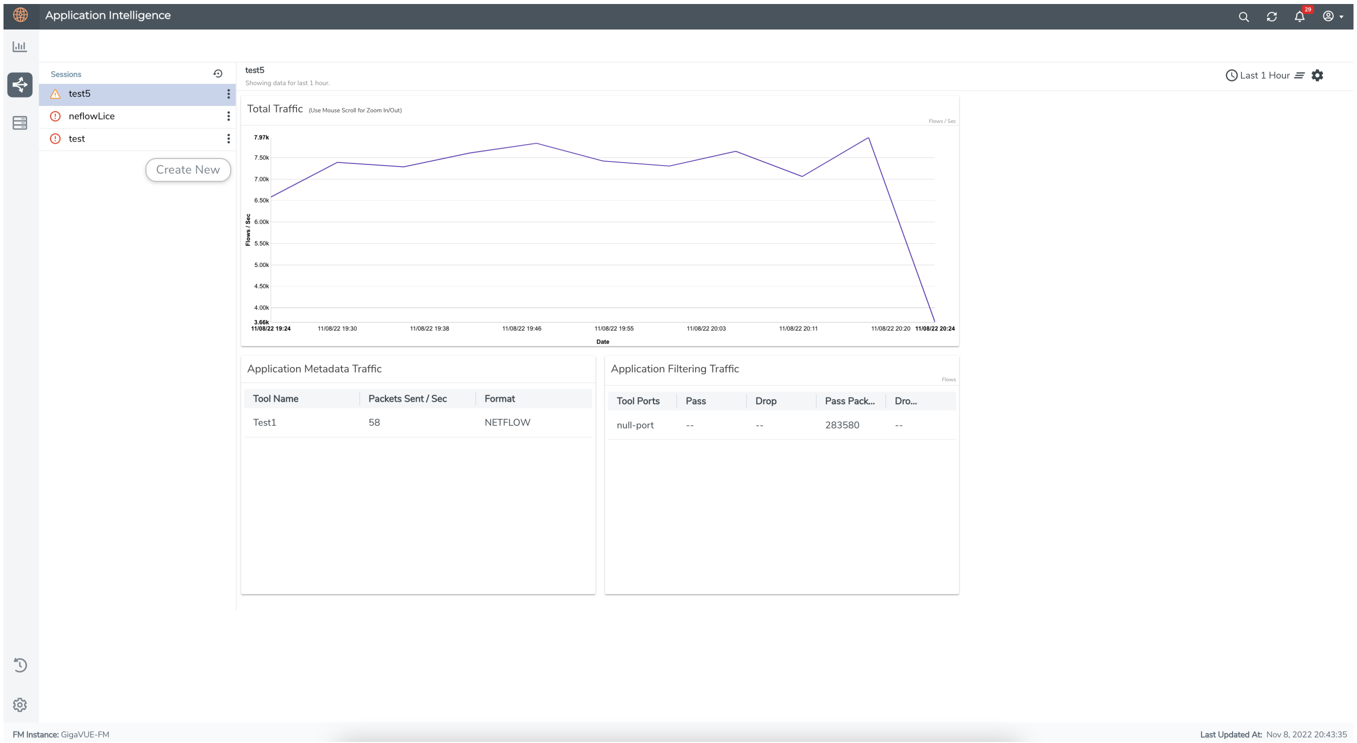
f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.

g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.

11. Click **Save**.

NetFlow Dashboard

In Appviz, only the traffic statistics are displayed as applications cannot be configured and used in the NetFlow configuration



Application Metadata Traffic

Tool Name	Packets Sent / Sec	Format
Test1	58	NETFLOW

Application Filtering Traffic

Tool Ports	Pass	Drop	Pass Pack...	Dro...
null-port	--	--	283580	--

FM Instance: GigaVUE-FM

Last Updated At: Nov 8, 2022 20:43:35

Configure a Load Balancer

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

The following load balancers are supported:

- AWS Network Load Balancer on GigaVUE Cloud Suite
- Gateway Load Balancer

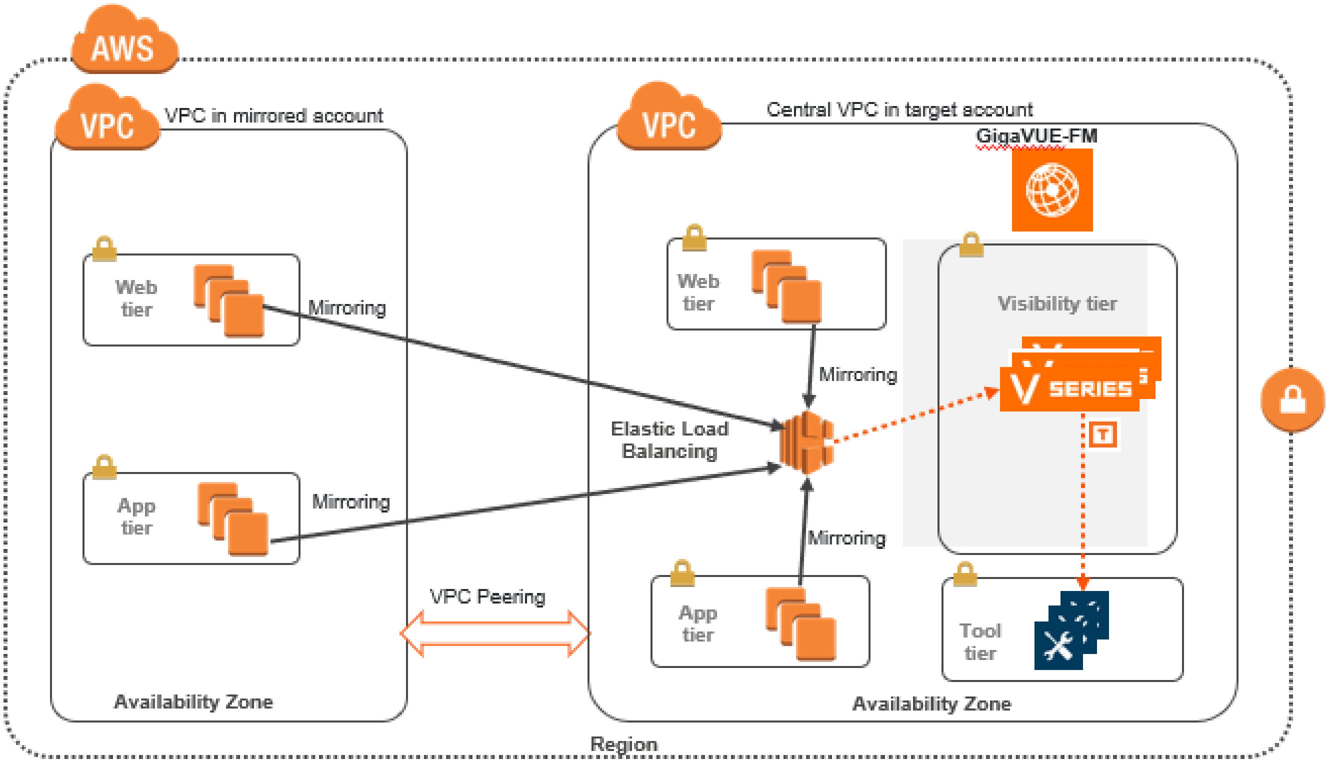
AWS Network Load Balancer on GigaVUE Cloud Suite

You can use a load balancer to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series Nodes. The load balancer distributes the traffic to the GigaVUE V Series Nodes and the AWS platofrm auto-scales the GigaVUE V Series Nodes based on the traffic by using the AWS autoscaling group. GigaVUE-FM creates a traffic mirror from the target VMs to the load balancer that all the targets must have the same traffic load balancer destination. Load balancer forwards the traffic to the GigaVUE V Series nodes and the AWS Auto Scaling group monitors the load of all GigaVUE V Series nodes. AWS Auto Scaling group can add or remove nodes if the traffic load is heavy or low.

Refer to the following topics for detailed information.

- Architecture of an External Load Balancer
- Configure a Network Load Balancer in AWS
- Deploy GigaVUE V Series Solution Network Load Balancing

Architecture of an External Load Balancer



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 VPC 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 (Fabric Manager)
- GigaVUE V Series Node
- AWS Network Load Balancer (uniformly distributes traffic from AWS target VMs to GigaVUE V Series nodes)

Configure a Network Load Balancer in AWS

Prerequisites

- Create or update Security Group polices of GigaVUE Cloud Suite components. Refer to 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. Refer to Amazon VPC for more information.

  > **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 AMI and Permissions section for detailed information.

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

1. In the **Target Groups** page, click **Create target group** and the Create target group wizard appears. Enter or select the following values and create the target group.
   a. Select **IP addresses** as the target type.
   b. Enter a name for the target group.
   c. Select the **UDP** as the Protocol and **4789** as the port number.
   d. Select the VPC of your target group where the targets are registered.
   e. Select **TCP** as the Health check protocol in port number **8889** with **10 seconds** health check interval.

   > **NOTE:** For detailed instructions, refer to Create a target group for your Network Load Balancer topic in the AWS Elastic Load Balancing document.

2. Navigate to the **Load Balancer** page and click **Create Load Balancer** the Create elastic load balancer wizard appears. Enter or select the following values and create the load balancer.
   a. Select **Network Load Balancer** as the load balancer type and click **Create**.
   b. Enter a name for the Network Load Balancer.
   c. Select **Internal** load balancer as the Scheme.
   d. Select the **VPC** for your targets (GigaVUE V Series Nodes).
   e. Select the regions/zones and the corresponding subnets.
   f. Select **UDP** as the Listener Protocol with Port number **4789**.

   > **NOTE:** For detailed instructions, refer to Create a Network Load Balancer topic in the AWS Elastic Load Balancing document.

3. Navigate to the **Launch Templates** page and click **Create launch template** the Create launch template wizard appears. Enter or select the following values and create the launch template.
   a. Enter a name for the launch template.
   b. Select the AMI of the GigaVUE V Series node.
   c. Select **t3a.xlarge** as the instance type.
   d. Select a Key pair for the instance.
   e. Select **VPC** as the Networking platform and don't specify the security group.
   f. Add 2 Network Interfaces for the GigaVUE V Series Node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces, select the appropriate security group.

   > **NOTE:** For detailed instructions, refer to Creating a launch template for an Auto Scaling group topic in the AWS EC2 Auto Scaling document.

4. Navigate to the **Auto Scaling groups** page, and click **Create an Auto Scaling group** the Create Auto Scaling group wizard appears. Enter or select the following values and create the Auto Scaling group.
   a. Enter a name for the Auto Scaling group.
   b. Select an existing launch template.
   c. Select the VPC and subnet.
   d. In the Group size section, enter the value for minimum and maximum capacity.
   e. In the Scaling policies section, select **Target tracking scaling policy** and choose Average network in (bytes) for the Metric type with **1000000000 (bytes)** as target value and **300** seconds warm up value.
   f. (optional) Add **Tags** to the instances.

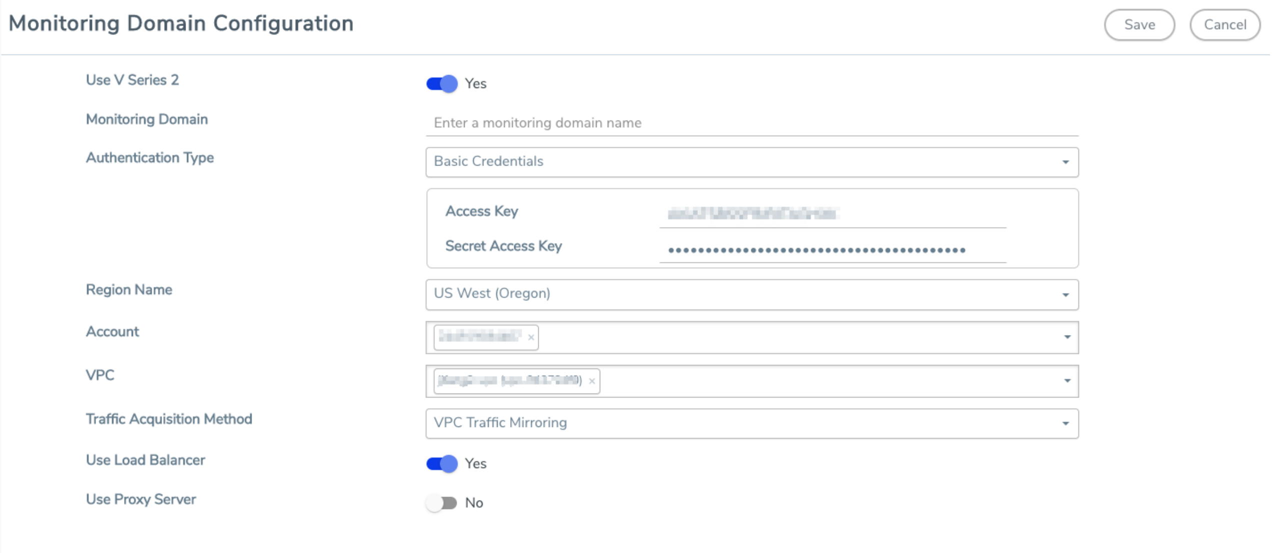
   > **NOTE:** For detailed instructions, refer to Creating an Auto Scaling group using a launch template topic in the AWS EC2 Auto Scaling document.

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

Deploy GigaVUE V Series Solution Network Load Balancing

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

1. In the **Monitoring Domain Configuration** page, select **VPC Traffic Mirroring** as the Traffic Acquisition method. Refer to Create a Monitoring Domain for detailed information.



Monitoring Domain Configuration

Use V Series 2: Yes

Monitoring Domain: Enter a monitoring domain name

Authentication Type: Basic Credentials

Access Key: [redacted]

Secret Access Key: ••

Region Name: US West (Oregon)

Account: [redacted]

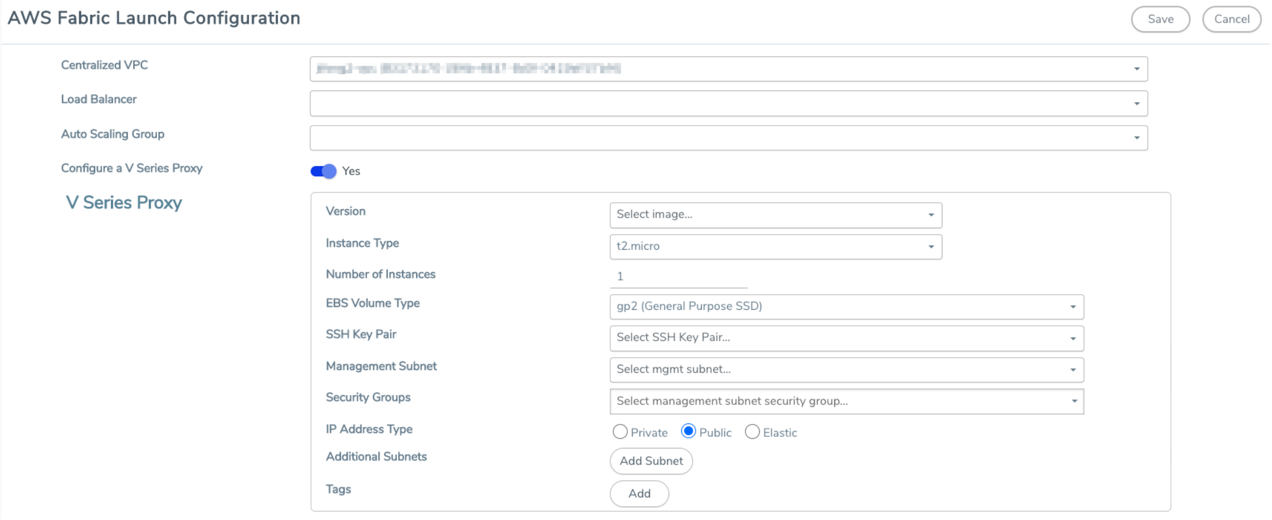
VPC: [redacted]

Traffic Acquisition Method: VPC Traffic Mirroring

Use Load Balancer: Yes

Use Proxy Server: No

2. For the **Use Load Balancer** field, select **Yes**.
3. Click **Save** and the AWS Fabric Launch Configuration page appears.



AWS Fabric Launch Configuration

Centralized VPC: [redacted]

Load Balancer:

Auto Scaling Group:

Configure a V Series Proxy: Yes

V Series Proxy

Version: Select image...

Instance Type: t2.micro

Number of Instances: 1

EBS Volume Type: gp2 (General Purpose SSD)

SSH Key Pair: Select SSH Key Pair...

Management Subnet: Select mgmt subnet...

Security Groups: Select management subnet security group...

IP Address Type: ○ Private ● Public ○ Elastic

Additional Subnets: Add Subnet

Tags: Add

4. In the AWS Fabric Launch Configuration page, select the following for the load balancer.
   - Select the Load Balancer configured in AWS
   - Select the Auto Scaling Group configured in AWS

   For the remaining field description, refer to Configure GigaVUE Fabric Components in GigaVUE-FM.
5. Click **Save** to save the configuration.

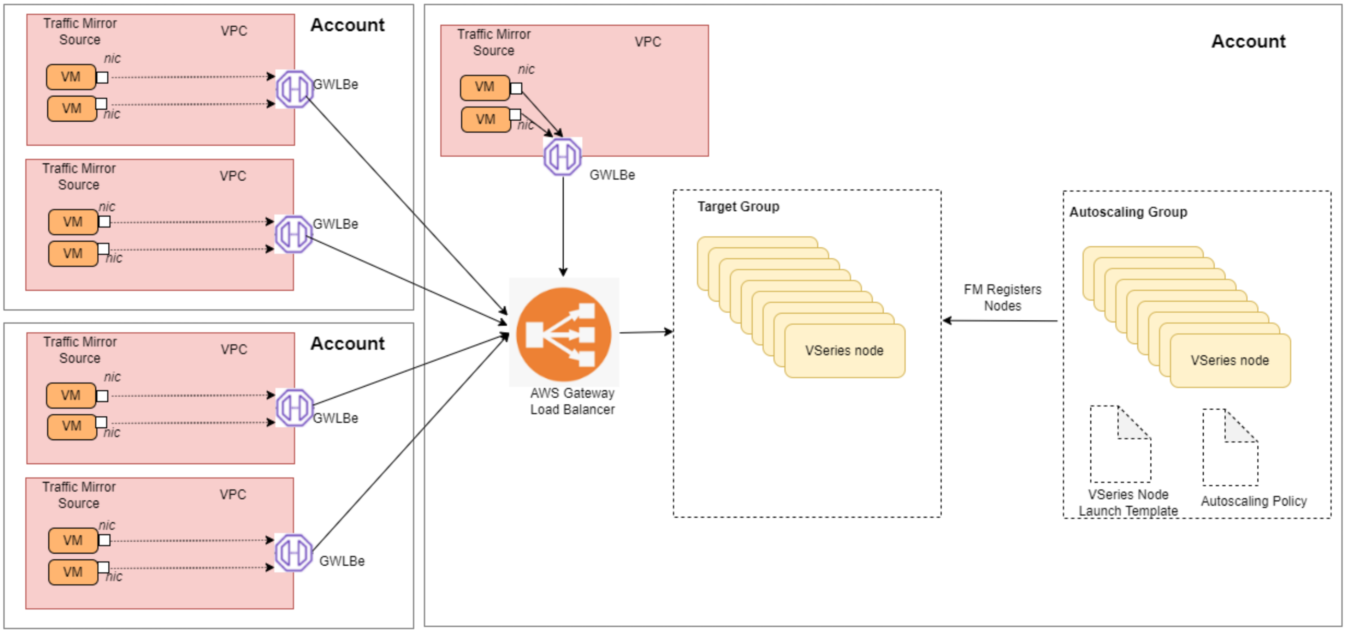
Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS

The gateway load balancer (GWLB) uses the gateway load balancer end points as a destination for VPC Traffic mirror. You can monitor network traffic across multiple VPCs and accounts, with centralized traffic inspection in a single VPC across their entire organization.

Refer to the following topics for detailed information.

- Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS
- Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS
- Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS
- Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS

Architecture



Configure a Gateway Load Balancer in AWS

Prerequisites

- 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 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 AMI and Permissions section for detailed information.
- 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.

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

1. In the **Target Groups** page, click **Create target group** and the Create target group wizard appears. Enter or select the following values and create the target group.
   a. Select **IP addresses** as the target type.
   b. Enter a name for the target group..
   c. Select the VPC of your target group where the targets are registered.
   d. Select **TCP** as the Health check protocol in port number **8889** with **10 seconds** health check interval.

   > **NOTE:** You must select GENEVE protocol and port 6081 while creating the targets groups. For detailed instructions, refer to Target groups for your Gateway Load Balancers.

2. Navigate to the **Load Balancer** page and click **Create Load Balancer** the Create elastic load balancer wizard appears. Enter or select the following values and create the load balancer.
   a. Select **Gateway Load Balancer** as the load balancer type and click **Create**.
   b. Enter a name for the Gateway Load Balancer.
   c. Select the **VPC** for your targets (GigaVUE V Series Nodes).
   d. Select the regions/zones and the corresponding subnets.
   e. Associate the load balancer to the target group.
   f. By default, **GENEVE** as the Listener Protocol with Port number **6081** is selected.

   > **NOTE:** For detailed instructions, refer to Create a Gateway Load Balancer topic in the AWS Elastic Load Balancing document

3. Navigate to the **Launch Templates** page and click **Create launch template** the Create launch template wizard appears. Enter or select the following values and create the launch template.
   a. Enter a name for the launch template.
   b. Select the AMI of the GigaVUE V Series node.
   c. Select **c5n.xlarge** as the instance type.
   d. Select a Key pair for the instance.
   e. Select **VPC** as the Networking platform and don't specify the security group.
   f. Add 2 Network Interfaces for the GigaVUE V Series node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces, select the appropriate security group.

   > **NOTE:** For detailed instructions, refer to Creating a launch template for an Auto Scaling group topic in the AWS EC2 Auto Scaling document.

4. Navigate to the **Auto Scaling groups** page, and click **Create an Auto Scaling group** the Create Auto Scaling group wizard appears. Enter or select the following values and create the Auto Scaling group.
   a. Enter a name for the Auto Scaling group.
   b. Select an existing launch template.
   c. Select the VPC and subnet.
   d. In the Group size section, enter the value for minimum and maximum capacity.
   e. In the Scaling policies section, select **Target tracking scaling policy** and choose Average network in (bytes) for the Metric type with **1000000000 (bytes)** as target value and **300** seconds warm up value.
   f. (optional) Add **Tags** to the instances.

   > **NOTE:** For detailed instructions, refer to Creating an Auto Scaling group using a launch template topic in the AWS EC2 Auto Scaling document.

In the Instances page, you can view the GigaVUE V Series Node instance launched by the auto scaling group.

Deploy GigaVUE V Series Solution with Gateway Load Balancer

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

1. In the **Monitoring Domain Configuration** page, select **VPC Traffic Mirroring** as the Traffic Acquisition method. Refer to Create a Monitoring Domain for detailed information.
2. For the **Use Load Balancer** field, select **Yes**.
3. Click **Save** and the AWS Fabric Launch Configuration page appears.
4. In the AWS Fabric Launch Configuration page, select the following for the load balancer.
   - Select the Load Balancer configured in AWS
   - Select the Auto Scaling Group configured in AWS

   For the remaining field description, refer to Configure GigaVUE Fabric Components in GigaVUE-FM.
5. Click **Save** to save the configuration.

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 Precryption in UCT-V

GigaVUE-FM allows you to enable or disable the Precryption feature for a monitoring session.

To enable or disable the Precryption feature in UCT-V, refer to Create monitoring session.

To create a new monitoring session with Precryption, follow these steps:

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

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

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

4. Click **Next**. The **Edit Monitoring Session** page appears with the new canvas.
5. Click **Options** button. The Monitoring Session Options appears.
6. Enable **Precryption**.
7. Click **Save**. The **Edit Monitoring Session** page appears. You can proceed to create map, tunnels, and adding applications.

> **NOTE:** It is recommended to enable the secure tunnel feature whenever the Precryption feature is enabled. Secure tunnel helps to securely transfer the cloud captured packets or precrypted data to a GigaVUE V Series Node. For more information, refer to Secure Tunnel .

Validate Precryption connection

To validate the Precryption connection, follow the steps:

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

Rules and Notes

- To avoid packet fragmentation, you should change the option precryption-path-mtu in UCT-V configuration file (**/etc/uctv/uctv.conf**) within the range 1400-9000 based on the platform path MTU.

To know more, refer to Precryption™.

Configure Secure Tunnel

Secure tunnel can be configured on:

- Precrypted Traffic
- Mirrored Traffic

Precrypted Traffic

You can send the precrypted traffic through secure tunnel. When secure tunnel for precryption is enabled, packets are framed and sent to the TLS socket. PCAPng format is used to send the packet.

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

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

For more information about PCAPng, refer to PCAPng Application.

Mirrored Traffic

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

Refer to the following sections for Secure Tunnel Configuration:

- Configure Secure Tunnel from UCT-V to GigaVUE V Series Node in UCT-V
- Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2

Prerequisites

- Port 11443 should be enabled in security group settings.
- While creating Secure Tunnel, you must provide the following details:
    - SSH key pair
    - CA certificate

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

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

<table>
<thead>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Upload a Custom Authority Certificate (CA)</td>
<td>
<p>)You must upload a Custom Certificate to UCT-V Controller for establishing a connection with the GigaVUE V Series node.</p>
<p>To upload the CA using GigaVUE-FM follow the steps given below:</p>
<ol>
<li>Go to <b>Inventory > Resources > Security > CA List</b>.</li>
<li>Click <b>New</b>, to add a new Custom Authority. The <b>Add Custom Authority</b> page appears.</li>
<li>Enter or select the following information.
<table>
<thead><tr><th>Field</th><th>Action</th></tr></thead>
<tbody>
<tr><td>Alias</td><td>Alias name of the CA.</td></tr>
<tr><td>File Upload</td><td>Choose the certificate from the desired location.</td></tr>
</tbody>
</table>
</li>
<li>Click <b>Save</b>.</li>
</ol>
<p>For more information, refer to the section Adding Certificate Authority</p>
</td>
</tr>
<tr>
<td>2.</td>
<td>Upload a SSL Key</td>
<td>You must add a SSL key to GigaVUE V Series node. To add SSL Key, follow the steps in the section SSL Decrypt.</td>
</tr>
</tbody>
</table>

S. No	Task	Refer to
3	Enable the secure tunnel	You should enable the secure tunnel feature to establish a connection between the UCT-Vand GigaVUE V Series node. To enable the secure tunnel feature follow these steps: **1.** In the Edit Monitoring Session page, click **Options**. The **Monitoring Session Options** page appears. **2.** Enable the **Secure Tunnel** button. You can enable secure tunnel for both mirrored and precrypted traffic.
4.	Select the SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM.	You must select the added SSL Key in GigaVUE V Series node Key while creating a monitoring domain configuring the fabric components in GigaVUE-FM. To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM. If the existing monitoring domain does not have a SSL key, you can add it by following the given steps: **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.	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

Configure Secure Tunnel from GigaVUE V Series Node 1 to GigaVUE V Series Node 2

You can create secure tunnel in the following ways:

- Between GigaVUE V Series Node 1 to GigaVUE V Series Node 2
- From GigaVUE V Series Node 1 to multiple GigaVUE V Series nodes.

You must have the following details before you start the configuration of secure tunnel from GigaVUE V Series Node 1 toGigaVUE V Series Node 2:

- IP address of the tunnel destination endpoint (GigaVUE V Series Node 2).
- SSH key pair (pem file).

To configure secure tunnel from GigaVUE V Series Node 1 toGigaVUE V Series Node 2, refer to the following steps:

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td>1.</td><td>Upload a Certificate Authority (CA) Certificate</td><td>You must upload a Custom Certificate to UCT-V Controller for establishing a connection between the GigaVUE V Series node.
To upload the CA using GigaVUE-FM follow the steps given below:
1. Go to <b>Inventory > Resources > Security > CA List</b>.
2. Click <b>Add</b>, to add a new Certificate Authority. The <b>Add Certificate Authority</b> page appears.
3. 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>
4. Click <b>Save</b>.
5. Click <b>Deploy All</b>.
For more information, refer to the section Adding Certificate Authority</td></tr>
<tr><td>2.</td><td>Upload a SSL Key</td><td>You must add a SSL key to GigaVUE V Series node.</td></tr>
<tr><td>3</td><td>Creating a secure tunnel between UCT-Vand GigaVUE Cloud Suite V Series Node 1.</td><td>You should enable the secure tunnel feature to establish a connection between the UCT-Vand GigaVUE Cloud Suite V Series node 1. To enable the secure tunnel feature follow these steps:
<b>1.</b> In the Edit Monitoring Session page, click <b>Options</b>. The <b>Monitoring Session option</b> page appears.
<b>2.</b> Enable the <b>Secure Tunnel</b> button. You can enable secure tunnel for both mirrored and precrypted traffic.</td></tr>
<tr><td>4.</td><td>Select the added SSL Key while creating a monitoring domain.</td><td>Select the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in GigaVUE V Series Node 1.
You must select the added SSL Key in GigaVUE V Series Node 1.
To select the SSL key, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM.</td></tr>
<tr><td>5.</td><td>Select the added CA certificate while creating the monitoring domain</td><td>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</td></tr>
<tr><td>6</td><td>Create an Egress tunnel from GigaVUE</td><td>You must create a tunnel for traffic to flow out from GigaVUE</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td>V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session.</td><td>
<p>V Series Node 1 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>
<li>After creating a new monitoring session, or click <b>Actions</b> &gt; <b>Edit</b> on an existing monitoring session, the GigaVUE-FM canvas appears.</li>
<li>In the canvas, select <b>New</b> &gt; <b>New Tunnel</b>, drag and drop a new tunnel template to the workspace. The <b>Add</b> Tunnel Spec quick view appears.</li>
<li>On the New Tunnel quick view, enter or select the required information as described in the following table:</li>
</ol>
<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>
<tr><td>Traffic Direction</td><td>
<p>Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:</p>
<ul>
<li>MTU- The default value is 1500.</li>
<li>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.</li>
<li>DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li>
<li>Flow Label - Enter the Flow Label value.</li>
<li>Source L4 Port- Enter the Souce L4 Port value</li>
<li>Destination L4 Port - Enter the Destination L4 Port value.</li>
<li>Flow Label</li>
<li>Cipher- Only SHA 256 is supported.</li>
<li>TLS Version - Select TLS Version1.3.</li>
<li>Selective Acknowledgments - Choose <b>Enable</b> to turn on the TCP selective acknowledgments.</li>
</ul>
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td></td><td>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 <b>Enable</b> to turn on delayed acknowledgments.</td></tr>
<tr><td>IP Version</td><td>The version of the Internet Protocol. Only IPv4 is supported.</td></tr>
<tr><td>Remote Tunnel IP</td><td>Enter the interface IP address of the GigaVUE V Series Node 2 (Destination IP).</td></tr>
</table>
<b>4.</b> Click <b>Save</b>.
</td></tr>
<tr><td>7.</td><td>Select the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in GigaVUE V Series Node 2</td><td>You must select the added SSL Key in GigaVUE V Series Node.</td></tr>
<tr><td>8</td><td>Create an ingress tunnel in the GigaVUE node 2 with tunnel type as TLS-PCAPNG while creating the monitoring session for GigaVUE node 2.</td><td>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.

To create the ingress tunnel, follow these steps:
<b>1.</b> After creating a new monitoring session, or click <b>Actions</b> &gt; <b>Edit</b> on an existing monitoring session, the GigaVUE-FM canvas appears.
<b>2.</b> In the canvas, select <b>New</b> &gt; <b>New Tunnel</b>, drag and drop a new tunnel template to the workspace. The <b>Add</b> Tunnel Spec quick view appears.
<b>3.</b> 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>
</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td>Traffic Direction</td><td>Choose <b>in</b> (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6:</td></tr>
<tr><td>IP Version</td><td>The version of the Internet Protocol. Only IPv4 is supported.</td></tr>
<tr><td>Remote Tunnel IP</td><td>Enter the interface IP address of the GigaVUE V Series Node 1 (Destination IP).</td></tr>
</table>
<b>4.</b> Click <b>Save</b>.
</td></tr>
</table>

For more information, refer to Secure Tunnels.

Viewing Status of Secure Tunnel

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

To verify the status of secure tunnel, go to **UCT-C** > **Monitoring Damain**. In the monitoring domain page, **Tunnel status** column shows the status of the tunnel. The green color represents that the tunnel is connected and the red represents that the tunnel is not connected.

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

Uninstall UCT-V

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

Uninstall Linux UCT-V

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

Stop the UCT-V service using the following commands:

For Ubuntu/Debian Package:

```
sudo service uctv stop
```

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

```
sudo systemctl stop uctv
```

Uninstall the UCT-V using the following:

For Ubuntu/Debian Package:

```
sudo dpkg -r uctv
```

For RPM package:

```
sudo rpm -e uctv
```

For Red Hat Enterprise Linux and CentOS with Selinux Enabled:

```
sudo rpm -e uctv
```

Uninstall Windows UCT-V

To uninstall Windows UCT-V:

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

Upgrade or Reinstall UCT-V

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

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

Refer to Uninstall UCT-V for more detailed information on how to uninstall UCT-V.

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

- Linux UCT-V Installation
- Windows UCT-V Installation

Monitor Cloud Health

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

- Configuration Health Monitoring
- Traffic Health Monitoring
- View Health Status

Configuration Health Monitoring

The configuration health status provides us detailed information about the configuration and deployment status of the deployed monitoring session.

This feature is supported for the following fabric components and features on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Nutanix

For UCT-Vs:

- AWS
- Azure
- OpenStack

For VPC Mirroring:

- AWS

For OVS Mirroring and VLAN Trunk Port:

- OpenStack

To view the configuration health status, refer to the Configuration Health Monitoring section.

Traffic Health Monitoring

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

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

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

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware

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

- Create Threshold Template
- Apply Threshold Template
- Edit Threshold Template
- Clear Thresholds
- Supported Resources and Metrics

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

- By default Threshold Template is not configured to any monitoring session. If you wish to monitor the traffic health status, then create and apply threshold template to the monitoring session.
- Editing or redeploying the monitoring session will reapply all the threshold policies associated with that monitoring session.
- Deleting or undeploying the monitoring session will clear all the threshold policies associated with that monitoring session.
- After applying threshold template to a particular application, you need not deploy the monitoring session again.

Create Threshold Template

To create threshold templates:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Then, click on the **Threshold Template** tab in the top navigation bar.
2. The **Threshold Template** page appears. Click **Create** to open the **New Threshold Template** page.
3. Enter the appropriate information for the threshold template as described in the following table.

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

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

Apply Threshold Template

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

Apply Threshold Template to Monitoring Session

To apply the threshold template across a monitoring session, follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.

3. The **Apply Thresholds** page appears. To apply a threshold template across a monitoring session, select the template you wish to apply across the monitoring session from the Threshold Template drop-down menu or enter the threshold values manually.
4. Click **Done**.

Apply Threshold Template to Applications

To apply the threshold template to a particular application in the monitoring session follow the steps given below:

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

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

Edit Threshold Template

To edit a particular threshold template follow the steps given below:

1. On the Threshold Template page, Click **Edit**. The **Edit Threshold Template** page appear.
2. The existing threshold templates will be listed here. Edit the templates you wish to modify.
3. Click **Save**.

> **NOTE:** Editing a threshold template does not automatically apply the template to monitoring session. You must apply the edited template to monitoring session for the changes to take effect.

Clear Thresholds

You can clear the thresholds across the entire monitoring session and also to a particular application.

Clear Thresholds for Applications

To clear the thresholds of a particular application in the monitoring session follow the steps given below:

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

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a monitoring session follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds page appears**. Click **Clear**.

> **NOTE:** Clearing thresholds at monitoring session level does not clear the thresholds that were applied specifically at the application level. To clear thresholds for a particular application refer to Clear Thresholds for Applications

Supported Resources and Metrics

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

Resource	Metrics	Threshold types	Trigger Condition
Tunnel End Point	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	1. Difference 2. Derivative	1. Over 2. Under

	5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors		
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	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

View Health Status

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

View Health Status of the Entire Monitoring Session

To view the health status of a monitoring session:

1. On the Monitoring Session details page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed, click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

This displays the configuration health and traffic health of the monitoring session and also the thresholds applied to that monitoring session.

View Health Status of an Application

To view the health status of an application across an entire monitoring session:

1. On the Monitoring Session page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed.
3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **Status** tab.

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

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

View Health Status for Individual V Series Nodes

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

1. On the Monitoring Session page, click on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu and then click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

View Application Health Status for Individual V Series Nodes

To view the application configuration and traffic health status of the GigaVUE V Series Nodes:

1. On the Monitoring Session page, click on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu.
3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **Status** tab.

The subsession toggle button available in the top-left corner of the canvas allows you to view the statistics of individual paths in the monitoring session. If the traffic health is not configured for monitoring session or a particular application, the traffic health is displayed as **Not Applicable**.

You can also view the cloud health Status in the Monitoring Session Page, refer to View Health Status on the Monitoring Session Page topic for more detailed information on how to view cloud health status in the Monitoring Session page.

Administer GigaVUE Cloud Suite for AWS

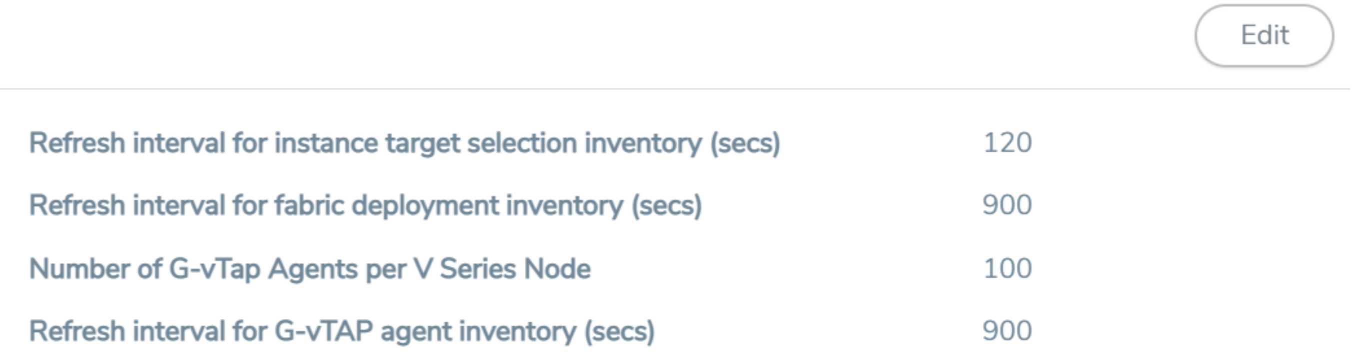
You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for AWS:

- Configure AWS Settings
- Configure Proxy Server
- Role Based Access Control
- About Events
- About Audit Logs

Configure AWS Settings

This section provides information on how to configure the maximum number of connections, refresh intervals for instance and non-instance inventory, and maximum batch size for monitoring session updates.

Go to **Inventory > VIRTUAL > AWS** and then click **Settings**.



Refresh interval for instance target selection inventory (secs)	120
Refresh interval for fabric deployment inventory (secs)	900
Number of G-vTap Agents per V Series Node	100
Refresh interval for G-vTAP agent inventory (secs)	900

In the Settings page, select **Advanced** tab to edit these AWS settings.

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.

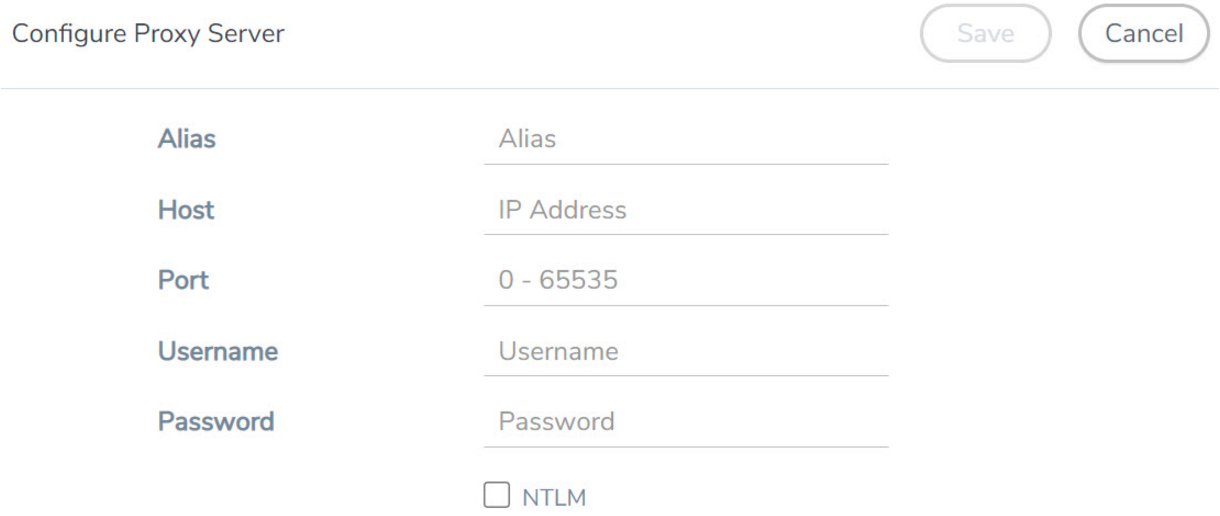
Configure Proxy Server

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 **Physical Device Infrastructure Management** category.

To create a proxy server:

1. Go to **Inventory > VIRTUAL > AWS and** then click **Settings**. In the Settings page, select **Proxy Server Configuration** tab to edit these AWS settings.
2. Click **Add**. The Add Proxy Server page is displayed.



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

Field	Description
Alias	The name of the proxy server.
Host	The host name or the IP address of the proxy server.
Port	The port number used by the proxy server for connecting to the Internet.
Username	(Optional) The username of the proxy server.
Password	The password of the proxy server.
NTLM	(Optional) The type of the proxy server used to connect to the VPC. On enabling NTML, enter the following information: • **Domain**—domain name of the client accessing the proxy server. • **Workstation**—name of the workstation or the computer accessing the proxy server.

4. 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.

Role Based Access Control

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

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

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

Resource Category	Cloud Configuration Task
Physical Device Infrastructure Management: This includes the following cloud infrastructure resources: • Cloud Connections • Cloud Proxy Server • Cloud Fabric Deployment • Cloud Configurations • Sys Dump • Syslog • Cloud licenses • Cloud Inventory	• Configure GigaVUE Cloud Components • Create Monitoring Domain and Launch Visibility Fabric • Configure Proxy Server
Traffic Control Management: This includes the following traffic control resources: • Monitoring session • Threshold Template • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps	• Create, Clone, and Deploy Monitoring Session • Create and Apply Threshold Template • Add Applications to Monitoring Session • Create Maps • View Statistics • Create Tunnel End Points

NOTE: Cloud APIs are also RBAC enabled.

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

About Events

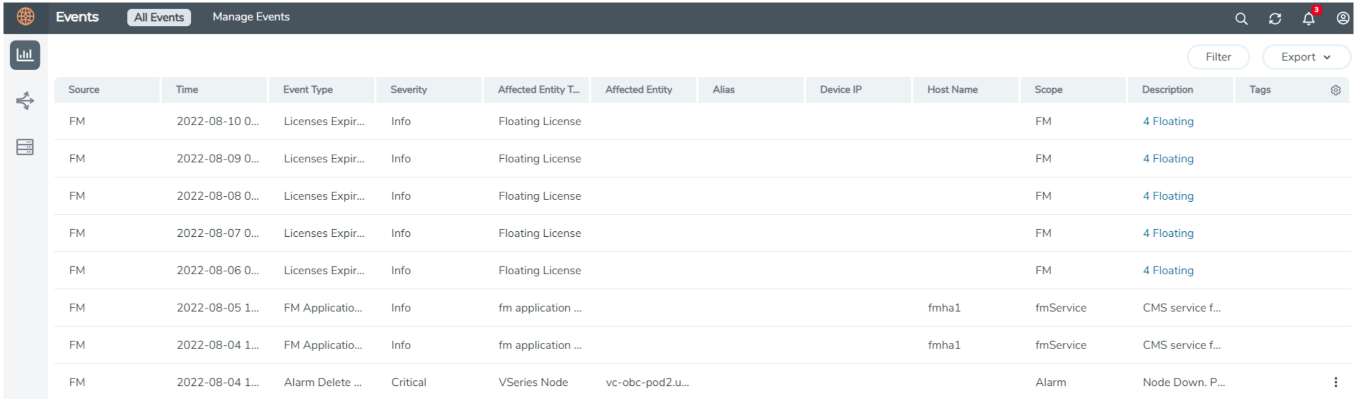
The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- 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: ▪ FM - indicates the event was flagged by the Fabric Manager. ▪ IP address - is the address of the GigaVUE HC Series or GigaVUE Cloud Suite G Series node that detected the event. For a node to be able to send notifications to the Fabric Manager, the SNMP_TRAP must be configured with the Fabric Manager’s IP address specified as a host. Refer to the GigaVUE Administration Guide for instructions on adding a destination for SNMP traps. ▪ 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.
Time	The timestamp when the event occurred. **IMPORTANT:**Timestamps 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.
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 statistics, and so on.
Severity	The severity is one of Critical, Major, Minor, or Info. Info is informational messages. For example, when power status change notification is displayed, then the message is displayed as Info.
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.
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.
Alias	Event Alias
Device IP	The IP address of the device.
Host Name	The host name of the device.
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.

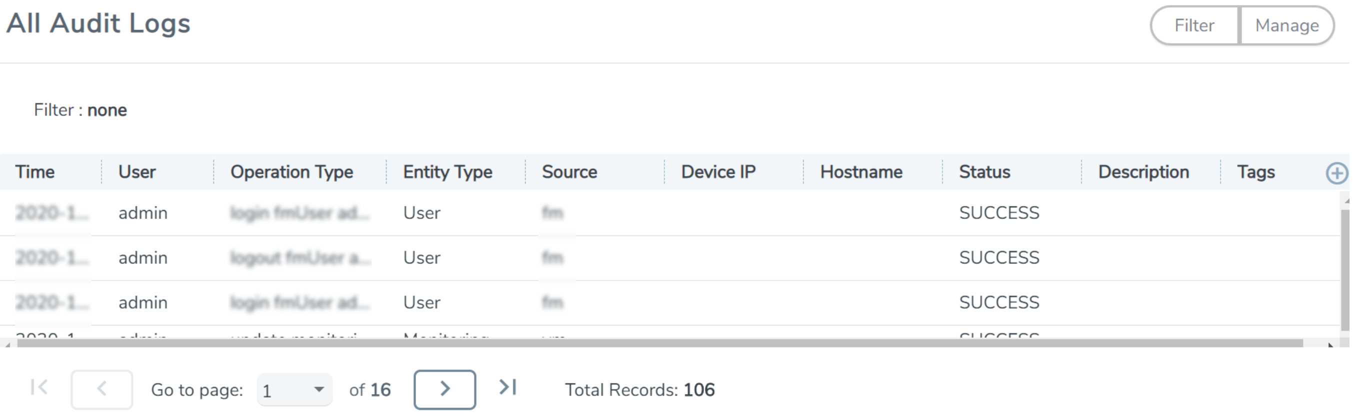
To filter the alarms and event:

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.



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		

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: ▪ 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 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 FM or device. Select **All Systems** apply both 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.

GigaVUE-FM Version Compatibility Matrix

The following tables list the different versions of GigaVUE Cloud Suite Cloud Suite fabric components available for the different versions of GigaVUE-FM.

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

GigaVUE-FM Version Compatibility

The following fabric components are renamed as follows:

- G-vTAP Agents - UCT-V
- Next Generation G-vTAP Agents - Next Generation UCT-V
- G-vTAP Controller - UCT-V Controller

GigaVUE-FM	UCT-V Version	Next Generation UCT-V Version	UCT-V Controller Version	GigaVUE V Series Proxy	GigaVUE V Series Nodes
6.4.00	v6.4.00	v6.4.00	v6.4.00	v6.4.00	v6.4.00

GigaVUE-FM	G-vTAP Agent Version	Next GenerationG-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Proxy	GigaVUE V Series Nodes
6.3.00	v6.3.00	v6.3.00	v6.3.00	v6.3.00	v6.3.00
6.2.00	v6.2.00	v6.2.00	v6.2.00	v6.2.00	v6.2.00
6.1.00	v6.1.00	N/A	v6.1.00	v6.1.00	v6.1.00
6.0.00	v1.8-7	N/A	v1.8-7	v2.7.0	v2.7.0
5.16.00	v1.8-5	N/A	v1.8-5	v2.6.0	v2.6.0
5.15.00	v1.8-5	N/A	v1.8-5	v2.5.0	v2.5.0

GigaVUE-FM	G-vTAP Agent Version	Next GenerationG-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Proxy	GigaVUE V Series Nodes
5.14.00	v1.8-4	N/A	v1.8-4	v2.4.0	v2.4.0
5.13.01	v1.8-3	N/A	v1.8-3	v2.3.3	v2.3.3
5.13.00	v1.8-2	N/A	v1.8-2	v2.3.0	v2.3.0
5.12.01	v1.8-1	N/A	v1.8-1	v2.2.0	v2.2.0
5.12.00	v1.7-1	N/A	v1.7-1	v2.1.0	v2.1.0

Glossary

This appendix lists the AWS terminologies used in this document. To find a brief definition of these terms, refer to AWS Glossary.

- Access Key
- Access key ID
- Amazon API Gateway
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon VPC
- AMI
- AWS
- AWS Identity and Access Management (IAM)
- CIDR block
- EC2 Instances
- Elastic IP address
- Endpoint
- Instance
- Instance type
- Internet gateway
- Key pair
- Secret access key
- Subnet
- Tag
- Target Instance
- Tunnel

Additional Sources of Information

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

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The VÜE Community

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.4 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide

GigaVUE Cloud Suite 6.4 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud Tap - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite 6.4 Hardware and Software Guides
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to My Gigamon. Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to My Gigamon
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

> **Note:** My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to: documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	
For Online Topics	**Online doc link**	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The VÜE Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)